Anusandhanvallari
Vol 2026, No.1
June 2026
ISSN 2229-3388

Comparative Governance and Regulatory Approaches Towards Generative Artificial Intelligence

Yoshita Sharma
BBA LLB (Hons.) - NMIMS, Indore
E-mail address: Yoshita1500@gmail.com

Introduction

Generative Artificial Intelligence (GenAI) use is not restricted to ordinary data processing and this is why it has become a key issue in the business landscape related to Corporate Governance and Technology Law. Content generation, impact on organizational decisions, legal, financial and reputational consequences are all areas where GenAI systems can impact. The risk of misinformation, copyright problems, data security and algorithmic bias and insufficient regulation have thus given rise to the need for good corporate governance structures. However, there are distinct jurisdictions' methods of control of such risks. The European Union has a comprehensive and risk-based approach, while the United Kingdom is moving towards a principles-based and sector-led approach; the United States has a primarily fragmented and enforcement-based approach; India has an approach driven by innovation and adaptation; and China has a compliance-based and state-led approach.

European Union: Risk-Based Governance

One of the most comprehensive proposals to regulate AI is Regulation (EU) 2024/1689, known as the Artificial Intelligence Act, for the EU. The EU framework is based on the risk-based approach where the risks that AI systems may pose are classified. This is crucial because it aims to differentiate between all AI systems and to align legal obligations with the scope of impact of a given AI system. High-risk AI systems are subject to strict governance, documentation, monitoring and compliance testing and practices that are considered to involve unacceptable risks are banned. High-risk applications include sectors like employment, creditworthiness, healthcare, law enforcement and critical infrastructure, where the inappropriate or inaccurate results of AI can have a serious impact on people and society.

For Generative Artificial Intelligence (GenAI), the consequences of an AI system are dependent to a large extent on the context in which it is used, which is why the risk-based structure is of importance (Balkin *et al.*,2020). A generative system, where administrative support is regular, can have comparatively low risks, whereas an AI system assisting in the recruitment process, credit approval, healthcare or other critical decision-making processes can have serious consequences on individuals. Thus the EU approach tries to lay a proportionality guideline between technological risk and the responsibility of the regulation. The framework does not impose the same duty on organisations to comply when they are using AI applications to which the same duty is not applied – it intends to make them as responsible as they can be when they are using an application that poses a higher risk.

A second key aspect of the European approach is that AI governance should not be suspended when the final product of an AI application is deployed. The AI Act proposes the following conditions for risk management, data governance, technical documentation, transparency, human oversight and cyber security. The above requirements contribute to ensuring that organisations are aware of potential risks associated with AI, not just when harm is already done. In this respect, the European way moves towards a preventive corporate governance and the identification and mitigation of risk becomes part of the organizational collective decision making process.

Another important aspect of the EU framework is its focus on general-purpose AI (GPAI) models. These models can be used for a range of downstream applications and may be a threat in various sectors (Bamberger *et al.*,2011). The obligations on the regulatory regime include those concerning the technical documentation, copyright and systemic-risk management of the relevant GPAI models. Adversarial testing, incident reporting and other requirements are important when models entail systemic risks. This is because AI governance is not only about the end user in the company but risks can be present at various points in the AI value chain.

The European approach is also international in its scope because of its extraterritorial scope. The obligations may be applicable to non-EU based organisations where their AI system affects individuals in the EU. In practice, it is not always feasible to distinguish the European element of the multinational company's AI use from the company's overall governance system. The EU framework might therefore become part of the encouragement of organisations operating in various countries to establish common internal standards, which comply with more stringent European standards.

Another fundamental element of the EU corporate governance model is the involvement of humans. High-risk AI applications will require leaders to be competent and empowered to understand the outputs of AI tools and what to do when needed. It is a particularly important one in board-level governance because it makes the point that there is a need for effective human control over significant corporate decisions. Organisations are thus not responsible for making decisions for AI systems.

The EU model, therefore, establishes a solid governance structure that encompasses risk classification, corporate compliance, data governance, transparency, human control and continuous monitoring. An important thing about it is that it tries to internalise the risks of AI before it becomes a serious problem for the organisation and causes damage. The framework is all-encompassing, but that may lead to high compliance expenses, particularly for smaller companies (Bello y Villarino *et al.*,2024). Uncertainty in the transition can also stem from implementing various provisions over time, and evolving requirements around general purpose AI.

To sum up, the EU's risk-based approach is a significant shift from the former reactive strategies and a move towards proactive and systematic management of AI. The EU is trying to provide a venue for technological innovation that is accountable, transparent and controlled by humans, by grounding the regulations on the amount of risk, and by granting more accountability to organisations developing or using AI systems. This is because the EU approach is a blueprint for evaluating other regulatory approaches, and can also be used as a basis to design strong governance mechanisms for Generative Artificial Intelligence.

One of the key aspects of the EU framework is its approach to general-purpose AI (GPAI) models. These models can be linked to multiple projects and applications in the downstream and hence have a risk that extend beyond one project or use case. The AI Act establishes specific obligations regarding the technical documentation, copyright issues regarding training data and the management of systemic risk. Systemic risks models may also be the subject of measures such as incident reporting and adversarial testing. By adopting this method, the organization that is ultimately responsible for deploying an AI application is not the only space that governance will need to focus on; there may be risks that emerge at the level of the underlying model and model development processes.

The extraterritorial application of the AI Act reinforces the significance of the European approach on a global scale. Applying to organisations outside the European Union, the requirements can still apply if they are used by the systems in the EU. EU's regulation is not geographically limited and therefore can reach multinational enterprises (MNEs) which provide or utilize AI systems in different regions (Calo *et al.*,2017). This is a push for companies from outside of the EU to integrate EU-level compliance principles across their corporate AI governance frameworks.

It is at the core of the EU framework of corporate governance. Particular emphasis is given to the responsibilities of organisations involved in deploying high-risk AI systems, such as the need for meaningful human oversight, in Article 26. People responsible for overseeing AI systems need to have the necessary expertise and authority to understand and rectify AI-generated content when necessary. In terms of corporate governance, this provision could help to prevent the human element from being completely taken off the hook when it comes to decisions made by AI systems, and to make sure that human decision-makers are held responsible when the decisions taken are based on AI.

The framework also stipulates that organisations ensure that the use of an AI system is consistent with the instructions relevant to the system and monitor its performance throughout the entire AI lifecycle, maintain the appropriate documentation and report any serious incident and inform relevant persons if the system is used if it affected the person (Chauhan *et al.*,2025). Furthermore, AI literacy is a key aspect of the AI Act, emphasizing the need for everyone involved in AI systems' use to be informed of their capabilities and risks. The requirement has significant implications for good corporate governance because it is not sufficient to have a formal, assigned role to ensure that the business is run effectively, that role must be held by someone with the requisite skill in order to achieve this.

Moreover, high-risk AI governance includes aspects of risk-management systems, data governance, technical documentation, transparency, human oversight and cyber security. The requirements effectively integrate AI risks into current enterprise risk management and compliance processes. In the EU model, AI governance is an ongoing organisational responsibility and not a project of the end of the year.

This is a major transformation from liability to risk-based governance in the EU model. The framework is designed to go beyond addressing potential risks to proactively manage and mitigate risks when developing and deploying AI systems. However, it is not without its difficulties in this all-encompassing strategy. Compliance requirements can be expensive and onerous for companies, particularly smaller companies. In addition, with several provisions being phased-in and the regulatory environment changing, it may bring some confusion in the process.

The European Union's approach, overall, demonstrates how the EU's approach to regulation of AI is embedded in the corporate governance. The EU would like to develop a “preventative governance architecture” that would integrate the four components of risk classification, human control, data governance, transparency, documentation and enforcement, which corporations need to accept for identifying and managing risks in AI before it can do harm. It is a key touchpoint to consider alongside and a potential example to consider as an example of good practice when drafting and developing a jurisdiction's own Governance Framework for Generative AI.

United Kingdom: Principles-Based and Sector-Led Governance

In comparison to the European Union's comprehensive statutory approach, the United Kingdom has a more fundamentally different regulatory outlook on Generative Artificial Intelligence (GenAI). The UK has no single, broad-based AI law, but a principles-based and sector-led approach to make sure existing laws and institutions are aligned with new AI technologies (Chen *et al.*,2025). This approach was clearly outlined in the UK Government's A Pro-Innovation Approach to AI Regulation, which highlights principles including safety, transparency, fairness, accountability and contestability. Responsibility for the governance of AI is spread across the current regulatory institutions, according to their competence, without establishing a new regulatory framework.

The UK system is mainly intended to balance the need for new technologies with the need for accountability. The idea is that by introducing the legislation too early, they risk it becoming redundant because of the fast development of the technologies behind AI. A flexible approach will enable regulators to adjust existing regulations and principles to new AI forms without having to re-issue laws. This can have the effect of fostering innovation, by limiting the compliance demands and offering organisations more leeway in managing new

technologies. Yet, the lack of a single statute for AI can also lead to fragmentation and uncertainty, especially if GenAI systems are used in various sectors.

There are a number of significant institutions in the UK regulatory structure. The Information Commissioner's Office (ICO) plays a key part in data protection and privacy, the Financial Conduct Authority (FCA) is the financial sector's regulator and the Competition and Markets Authority (CMA) takes care of issues on competition (Edwards *et al.*,2019). Such a decentralised arrangement enables the regulators to take into account the specific risks of AI in their respective fields. It can also output different results, as one GenAI system could be applied across multiple sectors, with different regulations.

The corporate governance's role is very important in this context. Given the lack of specific AI laws, directors are tasked with applying current corporate law principles to their decision making on the adoption and deployment of AI. Section 174 of the Companies Act 2006 outlines the duties of the directors, namely to exercise reasonable care, skill and diligence. This duty is technology agnostic and could have a direct impact on governance of GenAI. A director's actions may not be sufficient for a reasonably diligent director if it is approved for deployment of an AI system without proper risk assessment, monitoring, internal controls or appropriate safeguards.

This is even more crucial when GenAI is implemented for activities that involve risk or have commercial value. Just because it's a software developer's or third party technology provider's issue, does not mean a director can say it. If AI is taking a pivotal role in corporate decision-making, directors must be aware of the potential material risks of employing AI and make sure appropriate governance is put in place (Eroğlu *et al.*,2022). Thus, the UK approach does not create a new category of 'AI fiduciary duties'; it rather ensures that AI governance is in line with previously known principles of fiduciary duty, responsibility and corporate diligence.

The role of the businesses may be even more extensive for regulated industries. The Senior Managers and Certification Regime (SM&CR) in the financial sector sets out the responsibility for operational and technological risks by designating certain senior people. This can lead to stronger personal responsibility and will have particular significance in the event the monetary establishment is utilizing AI for credit scoring, fraud detection, buyer service, investments or other delicate processes.

Another crucial aspect of UK AI governance is data protection. The UK GDPR and Data Protection Act 2018 have provisions regarding fairness, transparency and accountability in the context of automated decision-making and AI processing. ICO guidance on AI and Data protection also emphasises the need for Data Protection Impact Assessments if there is significant risk to data protection in processing with AI tools (Ge *et al.*,2024). On top of this, some restrictions on the use of automated decisions with legal and/or important consequences further underscore the importance of meaningful human involvement in meaningful decisions.

The UK framework is also a derivative governance model for AI because the roles are being defined in current corporate, financial, data protection and consumer-protection laws, not with a new statute. Its greatest asset is its flexibility, which allows regulators and courts to draw on past cases and precedents to deal with new technological advances. This flexibility can also have an adverse effect, however, in terms of legal uncertainty, regulatory fragmentation and differing enforcement practices. As such, the effectiveness of the UK approach will depend on how well existing regulators are able to coordinate and if traditional standards of care, diligence and accountability are adequate to control the emerging risks of GenAI.

The UK approach is flatter, but is also flexible. The standards for GenAI systems could overlap between sectors and dimensions, depending on the different kinds of regulators that may have a focus on different aspects of AI (Hartzog *et al.*,2020). The focus is on directors (and what their responsibilities are and their compliance with the organisations) and not so much on the detail of the legislation relating to AI.

United States: Fragmented and Enforcement-Based Governance

The U.S. has a more decentralised AI governance strategy. The regulatory regime is not a single uniform national law on AI, rather it is a collection of sector-specific legislation, the policies of regulatory agencies and the enforcement of those policies, and common-law principles. At first Executive Order 14,110 established a significant federal policy framework, but was later rescinded in January 2025, thus reducing the federal coordination. There are agencies such as the Federal Trade Commission, Equal Employment Opportunity Commission and Consumer Financial Protection Bureau that are still looking into risks associated with using AI in their respective areas of work.

Corporate governance therefore relies heavily on internal organisation controls to a large extent, and on the voluntary frameworks. The NIST AI Risk Management Framework and the NIST voluntary commitments have helped shape responsible AI governance, although they are not binding, so they are not as effective at governance as a binding regulation. The issue of civil liability is not clear, and can be based on the doctrine of negligence, product liability, or fraud depending on the facts. There has also been State legislation that has increased the overall regulatory complexity.

The biggest strength of the U.S. model is its flexibility and ability to stimulate technological innovation (Hashmi *et al.*,2025). However, its decentralized structure brings with it accountability concerns, particularly for multi-industry general-purpose AIs. The lack of uniformity in the ex ante conformity requirements also allows the potential for the deployment of harmful AI systems before regulation is in place.

India: Adaptive and Innovation-First Governance

India has adopted an innovation-first, adaptive and relatively non-prescriptive approach towards the governance of Generative Artificial Intelligence (GenAI). Unlike the European Union, which has established a comprehensive AI-specific statutory framework, India has not introduced a dedicated and comprehensive AI legislation. Instead, the Indian regulatory approach relies on a combination of existing legal frameworks, governmental policies, regulatory initiatives and non-binding guidance. This approach reflects an intention to encourage technological development while gradually developing appropriate governance mechanisms as AI technologies and their associated risks evolve (Huang *et al.*,2025). The India AI Governance Guidelines emphasise important principles including trust, fairness, accountability, transparency, safety and innovation. However, because these guidelines are primarily normative and non-binding in character, their ability to impose direct legal obligations or penalties remains limited.

The innovation-first approach is partly influenced by India's distinctive socio-economic and technological environment. India has a large and diverse population, rapidly expanding digital infrastructure and significant differences in technological access and capability. Consequently, a rigid and uniform regulatory framework may create difficulties for businesses, technology developers and public institutions operating in different contexts. The Indian model instead favours incremental and context-sensitive regulation, allowing legal and policy mechanisms to develop alongside technological change. This provides organisations with greater flexibility to experiment with AI applications while allowing policymakers to observe emerging risks before introducing more prescriptive requirements.

In the absence of a dedicated AI statute, corporate governance responsibilities arise primarily through existing legislation. One of the most important frameworks is the Digital Personal Data Protection Act, 2023 (DPDPA). The Act establishes obligations for data fiduciaries concerning consent, purpose limitation, data minimisation and accountability. These principles become particularly relevant to GenAI systems because such systems may process substantial quantities of personal information for activities including profiling, automated decision-making and personalised services. Organisations deploying GenAI must therefore consider whether their collection, processing and use of personal data comply with applicable data-protection requirements.

The DPDPA also provides for greater responsibilities in relation to Significant Data Fiduciaries, including enhanced governance requirements such as data protection impact assessments, external audits and the appointment of Data Protection Officers. Where corporations deploy GenAI systems involving sensitive or large-scale data processing, these requirements can increase the importance of internal compliance mechanisms and senior-level oversight. Consequently, although India does not currently rely upon a comprehensive AI-specific corporate governance statute, existing data protection obligations can indirectly establish significant governance responsibilities for organisations using GenAI.

The Information Technology Act, 2000, together with the applicable Intermediary Guidelines and Digital Media Ethics Code Rules, also contributes to India's AI governance structure. Section 79 provides intermediary safe-harbour protection subject to compliance with applicable due-diligence requirements (Janssen *et al.*,2025). This becomes relevant where AI-generated content is harmful, unlawful or misleading and is distributed through online platforms. The principles established in *Shreya Singhal v. Union of India* concerning intermediary liability and due diligence provide an important legal context for assessing how platforms may be expected to respond to unlawful content generated or disseminated through AI systems.

The Consumer Protection Act, 2019 provides another important source of corporate accountability. AI-generated content may create consumer-protection concerns where businesses use artificial endorsements, misleading advertising, fabricated reviews or other deceptive representations. Consequently, corporations cannot assume that the use of an automated system removes responsibility for the accuracy and legality of information communicated to consumers. Existing consumer-protection principles may therefore operate as an indirect mechanism for regulating the consequences of GenAI deployment.

India's approach nevertheless faces important governance limitations. The absence of binding AI-specific legislation creates uncertainty concerning accountability, enforcement and the allocation of responsibility between developers, vendors, deployers and users. Regulatory responsibilities are also distributed among institutions such as the Ministry of Electronics and Information Technology, sectoral regulators and other governmental bodies, without a single comprehensive AI regulatory authority. This decentralised structure may create overlapping responsibilities and inconsistent regulatory expectations.

The emerging Indian legal position also demonstrates uncertainty in areas such as intellectual property and AI-generated content. The *ANI Media Pvt. Ltd. v. OpenAI Inc.* dispute raises questions concerning the use of copyrighted material for AI training, the application of copyright exceptions and the jurisdiction of Indian courts over foreign AI providers. In the absence of extensive AI-specific jurisprudence, Indian courts are likely to rely substantially on existing principles of copyright, intermediary liability, consumer protection and data governance.

Overall, India's model can be understood as a hybrid form of adaptive governance that seeks to balance technological innovation with incremental regulatory intervention. Its flexibility may support India's rapidly developing AI ecosystem, but this flexibility comes at the cost of legal predictability and enforceability. For corporations, the resulting environment requires AI risks to be incorporated into existing compliance and corporate governance structures. Until a more coherent statutory framework develops, effective GenAI governance in India will depend substantially on organisational accountability, risk management and the careful application of existing legal principles.

The emerging Indian jurisprudence demonstrates significant uncertainty. In *ANI Media Pvt. Ltd. v. OpenAI Inc.*, issues concerning AI training, copyright and jurisdiction illustrate the difficulty of applying existing legal principles to novel AI disputes (Okuno *et al.*,2025). The absence of AI-specific jurisprudence means courts are likely to rely on existing copyright, intermediary liability and consumer protection principles.

India's principal weakness is therefore the absence of a coherent and enforceable AI-specific framework. Regulatory decentralisation, limited enforcement infrastructure and uncertainty surrounding intellectual property create substantial compliance risks for corporations.

China: State-Directed and Compliance-Intensive Governance

China follows a state-directed, interventionist and compliance-intensive approach to the governance of Generative Artificial Intelligence (GenAI). Unlike the relatively flexible and innovation-oriented approach adopted by India or the principles-based approach followed by the United Kingdom, China has developed a more prescriptive regulatory structure in which AI development and deployment are closely connected with national security, public order, data governance and content control (Papagiannidis *et al.*,2025). Rather than relying upon a single comprehensive AI statute, China has established a layered framework consisting of the Interim Measures for the Management of Generative Artificial Intelligence Services (2023), together with the Cybersecurity Law 2017, Data Security Law 2021 and Personal Information Protection Law 2021. These instruments collectively establish governance requirements that operate throughout the AI lifecycle, from data collection and model training to deployment, monitoring and generation of outputs.

A distinctive characteristic of the Chinese approach is its emphasis on preventive and ex ante regulation. The regulatory framework does not merely respond to harmful consequences after they occur; instead, organisations are expected to identify and control risks before and during the deployment of GenAI systems. AI systems possessing public-opinion attributes or social mobilisation capabilities may be subject to security assessment and regulatory filing requirements. This demonstrates China's broader regulatory philosophy of anticipating systemic risks and establishing controls before AI systems are widely deployed.

Corporate compliance forms a central component of this regulatory structure. Organisations providing GenAI services are required to establish mechanisms capable of identifying and managing unlawful or harmful content (Passador *et al.*,2026). This includes real-time content moderation, supported by automated filtering mechanisms and human supervision. The emphasis on continuous monitoring means that corporations cannot regard compliance as a one-time exercise undertaken before an AI system is introduced. Instead, governance responsibilities continue throughout the operational life of the system. Corporations are expected to monitor outputs and take corrective measures where inappropriate or unlawful content is generated.

Data governance represents another important element of China's regulatory model. The Interim Measures require training data to be obtained lawfully and to respect intellectual property rights. In addition, the Personal Information Protection Law establishes requirements concerning the lawful collection and processing of personal information. Consequently, corporations developing or deploying GenAI must consider not only the performance of their models but also the legality, provenance and quality of the data used to train and operate them. This approach creates a direct relationship between data governance and corporate accountability.

Chinese regulation also places significant emphasis on internal governance, risk management, traceability and auditability. Corporations are expected to establish compliance policies and operational controls, monitor AI system activities and maintain mechanisms through which AI-related processes can be traced and audited. These requirements are particularly important from a corporate governance perspective because they enable organisations and regulators to identify how AI systems operate, determine responsibility for particular decisions and investigate potential violations. Consequently, the Chinese framework attempts to reduce the attribution problems that can arise when AI systems involve multiple developers, vendors and corporate users.

Transparency is reinforced through mandatory labelling of AI-generated and synthesised content. China's Measures for Labelling of AI-Generated Synthetic Content establish explicit and implicit labelling requirements for AI-generated material. Such requirements are particularly significant in addressing misinformation, deepfakes

and other forms of synthetic media (Petrin *et al.*,2019). By requiring users and audiences to know when content has been generated or synthesised through AI, the framework seeks to improve transparency and reduce the possibility of deception.

The Chinese approach is further distinguished by its integration of legal requirements with technical standards. Technical specifications concerning generative AI security, training-data management and system integrity provide practical mechanisms through which broader regulatory objectives can be implemented. This combination of legislation, regulatory requirements and technical standards demonstrates China's attempt to create governance controls that operate at both the legal and engineering levels.

Enforcement under the Chinese model can involve administrative, civil and criminal liability, while responsible executives may also face personal consequences. The framework therefore places significant responsibility not only upon corporate entities but also upon individuals involved in AI governance and management. Judicial developments discussed in the dissertation further indicate that corporations may not simply transfer responsibility to third-party AI vendors where harmful or infringing outputs result from their deployment of AI systems.

Overall, China's GenAI governance framework demonstrates a strong preventive and compliance-oriented model in which corporate responsibility extends across the entire AI lifecycle. Its major strength lies in its detailed operational requirements, strong enforcement mechanisms and integration of legal, technical and organisational controls. However, the highly interventionist nature of the system may create substantial compliance burdens and potentially constrain innovation (Bello y Villarino *et al.*,2024). From a corporate governance perspective, China nevertheless provides an important example of how AI responsibility can be embedded directly into organisational systems, requiring corporations to address data governance, content moderation, risk management, human supervision, traceability and accountability before and throughout the deployment of Generative Artificial Intelligence

China also provides significant enforcement mechanisms, including administrative, civil and criminal liability. Judicial developments have demonstrated that companies cannot necessarily shift responsibility to third-party AI providers, while emerging criminal cases indicate that liability may arise from deliberate system design and configuration decisions.

Comparative Synthesis and Conclusion

The comparative analysis of the European Union, United Kingdom, United States, India and China demonstrates that, despite significant differences in regulatory philosophy, institutional design and enforcement mechanisms, there is an emerging degree of convergence concerning the fundamental principles of Generative Artificial Intelligence (GenAI) governance. Across the five jurisdictions, corporate accountability, transparency, data governance, risk management and human oversight have increasingly become central components of responsible AI regulation. This convergence is particularly important because GenAI systems are increasingly integrated into corporate decision-making, customer services, employment processes, financial activities and other areas in which AI-generated outcomes can create significant legal and commercial consequences (Calo *et al.*,2017). The comparative analysis therefore indicates that, although jurisdictions disagree on how AI should be regulated, they increasingly recognise that corporations cannot treat GenAI as an entirely autonomous technology beyond the scope of organisational responsibility.

A significant area of convergence concerns the responsibility of the corporation deploying AI. In the European Union, the AI Act establishes specific obligations for organisations deploying high-risk systems, including requirements concerning human oversight, risk management, monitoring and record keeping. In the United Kingdom, corporate responsibility is derived from existing duties of directors, particularly the obligation to exercise reasonable care, skill and diligence. In the United States, responsibility is distributed through regulatory

enforcement, consumer protection, employment law and other sector-specific mechanisms. India similarly places responsibility upon organisations through data protection, intermediary and consumer protection laws, while China's framework imposes extensive compliance responsibilities upon AI providers and deployers. Thus, despite differences in legal form, the five jurisdictions increasingly recognise that corporations using GenAI cannot simply transfer responsibility to the technology provider or treat AI-generated outcomes as independent events.

Data governance represents another major point of convergence. The EU incorporates data governance requirements within its AI Act, while the UK relies significantly upon the UK GDPR and Data Protection Act 2018. The United States addresses data-related risks through existing privacy, consumer protection and sectoral enforcement mechanisms. India uses the Digital Personal Data Protection Act 2023 to establish obligations for data fiduciaries, while China combines its Personal Information Protection Law with its broader cybersecurity and data-security framework (Chauhan *et al.*,2025). This comparative similarity demonstrates that control over data is one of the most important regulatory entry points for AI governance. Since GenAI systems depend heavily on large volumes of training and operational data, the legality, quality, security and provenance of that data have become central elements of corporate accountability.

Transparency and explainability also represent increasingly common governance principles. The EU imposes detailed transparency requirements, while China has introduced mandatory labelling requirements for AI-generated and synthesised content. The United States addresses deceptive or misleading AI outputs through enforcement mechanisms, whereas the UK and India incorporate transparency through broader principles of accountability, fairness and data protection. Transparency is therefore not simply a mechanism for informing users about how AI operates. It also facilitates regulatory oversight, assists affected individuals in understanding AI-supported decisions and helps determine responsibility when AI systems produce harmful outcomes.

Similarly, the principle of human oversight has become an important common feature. The EU expressly establishes human oversight obligations for high-risk AI systems, while China integrates human supervision into operational compliance requirements. The UK, United States and India approach the issue more indirectly through existing principles of due diligence, fairness, accountability and responsible decision-making. This indicates a broader international recognition that consequential corporate decisions should not be treated as entirely autonomous simply because they involve AI. Human actors remain necessary for interpreting outputs, identifying errors and taking corrective action.

Despite these areas of convergence, substantial divergences in regulatory design remain. The European Union has adopted a comprehensive, ex ante and risk-based statutory model in which obligations increase according to the level of risk presented by an AI system (Chen *et al.*,2025). China follows a state-directed and compliance-intensive approach that combines AI governance with content regulation, data sovereignty and national-security considerations. The United Kingdom has chosen a principles-based and sector-led structure, relying upon existing regulators and legal principles rather than a comprehensive AI statute. The United States follows a fragmented and enforcement-driven model in which AI governance develops through agency action, litigation and sector-specific rules. India occupies a comparatively flexible position, adopting a policy-led and innovation-first framework with relatively limited binding force.

These differences have significant consequences for enforcement intensity and legal certainty. The EU and China have developed relatively strong compliance and enforcement mechanisms, whereas the United States depends substantially upon regulatory agencies and litigation. The UK applies AI governance through existing areas such as data protection and financial regulation, while India's framework remains comparatively less prescriptive and more dependent upon existing legislation and governmental guidance. Consequently, multinational corporations operating across these jurisdictions may face different compliance expectations for substantially similar AI activities.

The comparison therefore demonstrates the emergence of regulatory pluralism in GenAI governance. There is no single global model capable of completely resolving the legal and governance challenges created by AI (Edwards *et al.*,2019). Nevertheless, the shared emphasis on accountability, transparency, data governance, risk management and human oversight provides a potential foundation for developing common corporate governance standards. For multinational corporations, the most effective approach may therefore be to establish internal AI governance mechanisms capable of satisfying the highest commonly applicable standards across jurisdictions. Such an approach can reduce regulatory uncertainty, strengthen board-level accountability and minimise legal, operational and reputational risks arising from the rapidly expanding use of Generative Artificial Intelligence.

The most significant unresolved issue is the attribution of liability across the AI value chain involving developers, providers, deployers and users. No jurisdiction has yet established a universally applicable mechanism for distributing liability among these actors. Furthermore, even jurisdictions with developed regulatory systems face challenges concerning the practical capacity to monitor increasingly complex AI systems.

Overall, the comparative analysis demonstrates that GenAI governance has entered a period of regulatory pluralism. Multinational corporations must therefore operate across different and sometimes competing legal standards (Frankel *et al.*,1983). In the absence of globally harmonised AI regulation, corporations would benefit from establishing internal governance standards capable of satisfying the most demanding applicable regulatory requirements. Such an approach can strengthen accountability, reduce legal uncertainty and provide more effective protection against the growing corporate risks associated with Generative Artificial Intelligence

Reference list

[1] Balkin, Jack M., *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020).
[2] Bamberger, Kenneth A. & Mulligan, Deirdre K., *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).
[3] Bello y Villarino, José-Miguel & Bronitt, Simon, *AI-Driven Corporate Governance: A Regulatory Perspective*, 33(4) GRIFFITH L. REV. 355 (2024).
[4] Calo, Ryan, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399 (2017).
[5] Chauhan, Rubi, *AI-Powered Decision-Making in Corporations: Legal Liability, Corporate Governance, and the Question of Legal Personhood*, 7 INDIAN J.L. & LEGAL RSCH. 2703 (2025).
[6] Chen, Quancheng & Hu, Xuemei, *Tort Liability for the Application Risk of Generative Artificial Intelligence Technology in the Circular Economy and Financial Industry: Evidence from China*, 12 HUMANITIES & SOC. SCI. COMMCNS 1042 (2025).
[7] Edwards, Lilian, *Regulating Artificial Intelligence in Europe*, 10 EUR. J. RISK REG. 573 (2019).
[8] Eroğlu, Mustafa & Kaya, Özgür, *Impact of Artificial Intelligence on Corporate and Competition Law*, 23 EUR. BUS. ORG. L. REV. 347 (2022).
[9] Frankel, Tamar, *Fiduciary Law*, 71 CAL. L. REV. 795 (1983).
[10] Ge, Yijun (Jenny), *AI and Corporate Governance: How May AI Assist the Board in Informed Decision-Making?*, 24 UC DAVIS BUS. L.J. 115 (2024).
[11] Hartzog, Woodrow & Richards, Neil M., *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).
[12] Hashmi, Muhammad Ahsan Iqbal et al., *Criminal Liability in the Age of Autonomous Systems: Rethinking Mens Rea and Actus Reus*, 3 CRITICAL REV. SOC. SCIS. STUD. 290 (2025).
[13] Huang, Xinbo & Guo, Liu, *Navigating the Risks of Generative AI: A Comparative Analysis of International Regulatory Approaches*, 20 PROBLEMS OF SUSTAINABLE DEV. 11 (2025).
[14] Janssen, Marijn, *Responsible Governance of Generative AI: Conceptualizing GenAI as Complex Adaptive Systems*, 44 POL'Y & SOC'Y 38 (2025).
[15] Okuno, Mayumi J. & Okuno, Hiroshi G., *Legal Frameworks for AI Service Business Participants: A Comparative Analysis of Liability Protection Across Jurisdictions*, 40 AI & SOC'Y 5667 (2025).

[16] Papagiannidis, Emmanouil, Mikalef, Patrick & Conboy, Kieran, *Responsible Artificial Intelligence Governance: A Review and Research Framework*, 34 J. STRATEGIC INFO. SYS. 101885 (2025).
[17] Passador, Maria Lucia & Montagnani, Maria Lilla, *Fiduciary Duties and the Business Judgment Rule 2.0 in the AI Act Age*, OXFORD BUS. L. BLOG (Jan. 29, 2026).
[18] Petrin, Martin, *Corporate Management in the Age of AI*, 2019 COLUM. BUS. L. REV. 965 (2019).