Available Online: 4 November 2026 DOI: 10.54254/2753-7102/2026.38610

Legal reconstruction of corporate digital responsibility in the context of artificial intelligence governance

Jingjing Cheng

Melbourne Law School, The University of Melbourne, Melbourne, Australia

chengjingjing0122@163.com

Abstract. The emergence of artificial intelligence now influences corporate decision-making, information processing, automatic evaluations, and relationships with stakeholders, thus raising the question of corporate digital responsibility as the subject of corporate governance. Comparative analysis addresses the possibility of transforming corporate digital responsibility from voluntary ethical commitment into legally verifiable obligation via the algorithmic lifecycle approach. The corpus consists of 18 laws, regulations, and authoritative corporate governance guidelines released during 2021-2025 and 3-4 key documents of each of the 15 selected digital companies in the European Union, China, and the United States. Twenty indicators were coded in the following categories: data governance, fairness control, transparency, human oversight, and audit/ remedy. Every indicator includes absence of commitment, general commitment, and verifiable procedures, while legal requirement-responsibility indicator-scoring basis matrix provides the link between corporate data and normative requirement. The findings reveal that transparency, human oversight, and audit/ remedy are characterized by significant differences among jurisdictions, while data governance and fairness control are more alike. The median score for audit/remedy is 75.0 in the European Union and 50.0 in China and the United States. These findings support lifecycle-based legal reconstruction connecting corporate digital responsibility with identifiable duties of care, disclosure, oversight, auditing, correction, and compensation through a framework.

Keywords: artificial intelligence governance, corporate digital responsibility, algorithmic accountability, legal obligation, lifecycle regulation

1. Introduction

AI has enabled companies to enhance their capabilities of gathering data, classifying people, automating decision making and impacting access to services, thus creating risks of responsibility in organizational ecosystems. Corporate digital responsibility is the concept that helps manage ethical and responsible use of data and digital technology within these ecosystems [1]. Generative and decision-making systems exacerbate such responsibility since the risks may occur in the course of data gathering, model creation, implementation, monitoring, and post-risk management [2]. Thus, it is important to apply the concept of an algorithmic lifecycle in order to link responsibility to the particular lifecycle stage when risks were created, detected, controlled and remedied. Current research covers such topics as privacy, fairness, transparency, oversight and

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

accountability; however, legal nature of these responsibilities is uneven around the world. The paper explores the requirements and corporate disclosure regarding these responsibilities in the European Union, China and the United States.

2. Literature review

2.1. Conceptual evolution of corporate digital responsibility

Digital corporate responsibility has evolved from corporate social responsibility into a set of principles which take into account the responsibilities that result from data, technologies, and interactions between stakeholders through technologies. Digital corporate responsibility has been researched with regard to privacy, security, transparency, fairness, accessibility, and responsible technology utilization [3]. The notion of artificial intelligence broadens this agenda as responsibility must be determined by data quality, behavior of the model, automated results, and consequences as opposed to any particular organizational decision. Corporate responsibility in relation to AI-enabled service automation is researched with regard to data gathering, storage, access, quality, equality, and consumer protection [4]. This makes digital corporate responsibility a fitting framework for AI governance; however, the voluntary nature of the principle does not resolve the question of how ethics turn into law.

2.2. Normative structure of artificial intelligence governance

The regulation of artificial intelligence includes risk categorization, transparency, human supervision, technical standards, and accountability, but all of these tools are implemented differently across different states. Comparing different regimes reveals that the EU, China, and the USA follow their regulatory goals by designating the respective roles to rights protection, state coordination, market regulation, and international leadership [5]. The bilateral comparison reveals the different pathways of governance of artificial intelligence in the United States and China even though both nations are concerned with issues such as safety, accountability, and development of technology [6]. The comparative analysis reveals that different regulatory regimes achieve the proper balance between technological innovation and moral limitations through different institutional logics [7]. Such differences demand an analytical framework which maintains legal differences while transforming similar obligations into responsibility indicators.

2.3. Existing limitations of responsibility regimes

A responsible AI research approach entails making a distinction between high-level normative principles and the lower-level procedures necessary for putting such principles into practice along the entire AI lifecycle [8]. Human oversight serves as an example of this challenge since human involvement in AI operations only becomes relevant when it includes defined authority, expertise, intervention processes, and review mechanisms [9]. The corporate digital responsibility concept has an evidentiary gap as it promises certain qualities such as fairness, transparency, or accountability in statements without providing proof of testing, responsible parties, escalation pathways, audit trails, or remedies. Existing literature on responsible AI suffers from three blind spots, namely lifecycle-based responsibility fragmentation, poor comparability of legal and corporate evidence, and low connections between responsibility principles and legal consequences. Such gaps call for developing a coding framework.

3. Experimental methods

3.1. Corpus selection

Corpora are built using publicly available legal and corporate documents in order to ensure reproducibility and feasibility of the analysis. The legal corpus consists of 18 laws, regulations, and authoritative governing documents published between 2021 and 2025 in the EU, China, and the US. The sample of corporate documents involves 15 large companies publicly traded in the digital industry, with five companies from each jurisdiction. For each of these companies, three to four main documents are taken from their official sites or investor relations pages, including annual or sustainability reports, AI principles, transparency reports, privacy/data governance statements, and AI-governance statements in particular. Documents are retained only if the full text is provided, the issuer and the year of publication are identified, and the document provides information on corporate digital responsibility. The duplicates, promotional pages, press releases, and any other documents that do not have any responsibility-related provisions are removed. All documents are coded with a jurisdiction, company name, year, document type, its lifecycle stage, and source number. The resulting corporate corpus has 45 to 60 main documents. NVivo is used to code texts, whereas Excel stores metadata and builds the necessary matrix of provisions/indicators/scoring basis for further measurements. Selection ensures the equality of the number of firms in all three jurisdictions.

3.2. Responsibility indicator coding

The measures for corporate digital responsibility can be found in 20 different indicators, which are drawn from the legal regulations, governance guidelines, and corporate digital responsibility literature [10]. Five different measures include four indicators each. Data governance includes indicators on legal data sources, data quality, data security, and deletion rights; fairness control includes indicators on bias testing, non-discrimination testing, representative data, and correction mechanism; transparency includes indicators on AI use declaration, outcome explanation, limits declaration, and process traceability; human oversight includes indicators on human intervention power, escalation management, personnel training, and final decision making; audit or remedy includes indicators on impact assessment, regular audit, complaints mechanism, and correction or compensation. The standardized dimension score is calculated as shown in Formula (1).

$$CDR_{id} = 100 \times \frac{\sum_{k=1}^{K_d} s_{idk}}{2K_d} \tag{1}$$

Here, CDR_{id} denotes firm i's standardized corporate digital responsibility score in dimension d, s_{idk} is the coded value of indicator k, and K_d equals four. Two coders independently code the corpus after a pilot exercise. Inter-coder reliability is calculated as shown in Formula (2).

$$\kappa = \frac{P_o - P_e}{1 - P_e} \tag{2}$$

Here, P_o denotes observed agreement and P_e denotes agreement expected by chance. A κ value of at least 0.75 is required before final coding, and disagreements are resolved through documented review.

3.3. Analytical procedure

Analysis links every corporate digital responsibility score to a jurisdiction-specific legal benchmark and its corresponding textual evidence. Comparable policy-text analysis shows that structured coding can reveal systematic differences across China, the European Union, and the United States while retaining institutional characteristics [11]. For each dimension, the implementation gap is calculated as shown in Formula (3).

$$G_{id} = L_{jd} - C_{id} \tag{3}$$

Here, G_{id} denotes the implementation gap, L_{jd} is the legal benchmark for jurisdiction j and dimension d, and C_{id} is the standardized corporate score. Positive values indicate under-implementation, zero indicates alignment, and negative values indicate corporate practice exceeding the coded minimum. Jurisdictional differences are examined with the Kruskal–Wallis statistic shown in Formula (4).

$$H = \frac{12}{N(N+1)} \sum_{j=1}^{3} \frac{R_j^2}{n_j} - 3(N+1) \tag{4}$$

Here, N denotes the total number of firms, n_j is the number of firms in jurisdiction j, and R_j is the corresponding rank sum. Fifteen companies and twenty measures yield 300 firm-measure pairs, where each of the four responsibility dimensions contains 60 firm-measure pairs. The median and interquartile range are used to characterize the dimension score, and the H-statistics and p-values to compare the differences across jurisdictions at the 0.05 significance level. Then, the qualitative analysis will connect the statistically significant differences to the particular legal clauses and firm evidences.

4. Results

4.1. Responsibility coverage profile

Responsibility coverage differed in externally accountable dimensions. As shown in Table 1, data-governance medians were 87.5 in the European Union, 87.5 in China, and 75.0 in the United States, while fairness-control medians were 75.0 in all three jurisdictions. Neither dimension showed a significant jurisdictional difference, with p values of 0.226 and 0.660. Transparency produced medians of 87.5, 62.5, and 62.5, respectively, with H = 7.35 and p = 0.025. Human oversight showed separation: 87.5 in the European Union, 62.5 in China, and 50.0 in the United States, with H = 7.16 and p = 0.028. Audit or remedy also differed significantly, with medians of 75.0, 50.0, and 50.0 and p = 0.022. These results indicate that digital responsibility is documented more consistently in internal governance than in procedures requiring external explanation, intervention, auditability, or remediation.

Table 1. Corporate digital responsibility coverage profile across jurisdictions

Dimension	European Union Median (IQR)	China Median (IQR)	United States Median (IQR)	H	p
Data governance	87.5 (12.5)	87.5 (12.5)	75.0 (12.5)	2.97	0.226
Fairness control	75.0 (12.5)	75.0 (12.5)	75.0 (12.5)	0.83	0.660
Transparency	87.5 (12.5)	62.5 (25.0)	62.5 (25.0)	7.35	0.025
Human oversight	87.5 (25.0)	62.5 (25.0)	50.0 (25.0)	7.16	0.028
Audit or remedy	75.0 (12.5)	50.0 (25.0)	50.0 (12.5)	7.63	0.022

4.2. Normative implementation gap

A review of implementation-gap analysis yielded a distinct result from absolute responsibility coverage. As depicted in Figure 1, the European Union had a median gap of 12.5 for data governance, fairness control, transparency, and human oversight, while audit or remedy had 25.0. The case of China is one where there was an alignment in data governance, fairness gap of 12.5, gaps of 25.0 in transparency and human oversight, and the biggest audit or remedy gap of 37.5 points. Meanwhile, the United States has data governance of 12.5 points, no fairness control, 12.5 transparency, and 25.0 points each in human oversight and audit or remedy.

The clustering of big gaps in post-deployment accountability suggests that formal responsibility requirements go beyond the reported corporate procedures in the areas of review, escalation, auditing, complaint handling, and compensation. The heat-map format also distinguishes better legal standards from poorer corporate performance to prevent a small gap from being considered high substantive responsibility.

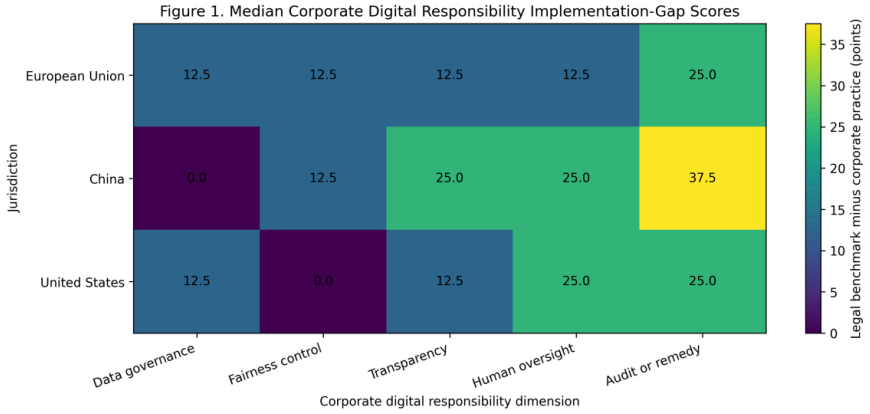


Figure 1. Median corporate digital responsibility implementation-gap scores

5. Discussion

The findings show that obligations are more amenable to institutionalization if they align with current roles played by internal control structures. Governance of data can become part of procedures related to privacy, cybersecurity, compliance, and information management, while transparency, human intervention, and audit or remedy need additional procedures of external inspection, intervention, and redress. The approach to the algorithmic lifecycle explains the differences because deficiencies can pile up through the lifecycle: bad data quality can contribute to bias, lack of transparency can limit review possibilities, and insufficient authority to intervene can slow down correction. Thus, the duty of care becomes an interesting legal tool that connects appropriate corporate conduct with certain lifecycle stages, responsible parties, evidentiary standards, and predictable harms. Differences between jurisdictions also have to be considered in relation to legal standards since even small gaps might mean less rigorous normative requirements rather than better practice. Public disclosure still remains partial evidence, and documentary scores should be considered alongside legal standards, auditability, and remedies of each of the reviewed jurisdictions.

6. Conclusion

Legal reconceptualization of corporate digital responsibility may take place based on the algorithmic life cycle approach, which correlates the requirements, corporate processes, and documentation. An analysis of 15 listed digital companies against 20 criteria reveals great jurisdictional variations in terms of transparency, human supervision, and audit/remedy while the data governance and fairness control seem to be more convergent. The main gaps in implementing those responsibilities are found in the sphere of procedures, which should be externally accountable, especially regarding auditing, complaints, and remedy process. Consequently, the coding scheme allows correlating the duty of care with actors, stages of the life cycle, documentation, and remedial measures. However, due to reliance on public reporting, it becomes impossible to estimate the effectiveness of operational performance and comparative analysis.

References

[1] Wirtz, J., Kunz, W. H., Hartley, N., & Tarbit, J. (2023). Corporate digital responsibility in service firms and their ecosystems. *Journal of Service Research, 26*(2), 173-190.

[2] Kunz, W. H., & Wirtz, J. (2024). Corporate digital responsibility (CDR) in the age of AI: Implications for interactive marketing. *Journal of Research in Interactive Marketing, 18*(1), 31-37.

[3] Carl, K. V., & Hinz, O. (2024). What we already know about corporate digital responsibility in IS research: A review and conceptualization of potential CDR activities. *Electronic Markets, 34*, 27.

[4] Scarpi, D., & Pantano, E. (2024). 'With great power comes great responsibility': Exploring the role of corporate digital responsibility (CDR) for artificial intelligence responsibility in retail service automation (AIRRSA). *Organizational Dynamics, 53*(2), 101030.

[5] Mokry, S., & Gurol, J. (2024). Competing ambitions regarding the global governance of artificial intelligence: China, the US, and the EU. *Global Policy, 15*(5), 955-968.

[6] Hine, E. (2024). Governing Silicon Valley and Shenzhen: Assessing a new era of artificial intelligence governance in the United States and China. *Digital Society, 3*, 50.

[7] Tuzov, V., & Lin, F. (2024). Two paths of balancing technology and ethics: A comparative study on AI governance in China and Germany. *Telecommunications Policy, 48*(10), 102850.

[8] Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems, 34*(2), 101885.

[9] Laux, J. (2024). Institutionalised distrust and human oversight of artificial intelligence: Towards a democratic design of AI governance under the European Union AI Act. *AI & Society, 39*(6), 2853–2866.

[10] Merbecks, U. (2024). Corporate digital responsibility (CDR) in Germany: Background and first empirical evidence from DAX 30 companies in 2020. *Journal of Business Economics, 94*(7), 1025–1049.

[11] Wang, S., Zhang, Y., Xiao, Y., & Liang, Z. (2025). Artificial intelligence policy frameworks in China, the European Union and the United States: An analysis based on structure topic model. *Technological Forecasting and Social Change, 212*, 123971.