Chen S, Giacalone M, 'From Accountability to Liability: How Accountability Mechanisms Shape the Non-Contractual Liability of Generative AI in the EU and China' (2026) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT262SCMG

EJPLT
ISSN 2704-8012



From Accountability to Liability: How Accountability Mechanisms Shape the Non-Contractual Liability of Generative AI in the EU and China

Dalla responsabilità alla colpevolezza: come i meccanismi di accountability influenzano la responsabilità extracontrattuale dell'IA generativa nell'UE e in Cina

SIMENG CHEN
Ph.D.(s), Vrije Universiteit Brussel, Brussels Research Institute on Development, Governance and Empowerment, through law (BRIDGE)

MARCO GIACALONE
Research professor, Vrije Universiteit Brussel, Brussels Research Institute on Development, Governance and Empowerment, through law (BRIDGE)

Abstract

The article compares how accountability mechanisms shape non-contractual liability for generative AI in the European Union and China. Through a structured analysis of each regime's approach, it identifies two distinct models: the EU's horizontal, ex ante framework and China's vertical, sector-specific framework. The study finds that accountability measures lead to liability outcomes only when they are legally formalised and provide enforceable standards or evidence for courts. In the EU, mandatory risk controls, transparency, and record-keeping create clear benchmarks and an auditable trail that facilitate fault attribution under updated liability laws. In China, accountability remains largely an administrative oversight tool; compliance records do not automatically translate into liability standards, making any civil redress contingent on prior regulatory action. The article concludes that accountability is a necessary precursor to effective AI liability, but it must be designed as a legally actionable and judiciary-ready mechanism to bridge the "accountability gap" in AI governance.

© The author(s) 2026, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
L'articolo mette a confronto il modo in cui i meccanismi di responsabilità danno forma alla responsabilità extracontrattuale per l'intelligenza artificiale (IA) generativa nell'Unione Europea (UE) e in Cina. Attraverso un'analisi strutturata dell'approccio di ciascun regime, individua due modelli distinti: il quadro orizzontale, ex ante, dell'UE e il quadro verticale settoriale della Cina. Lo studio rileva che le misure di responsabilità producono esiti positivi solo quando sono formalizzate giuridicamente e forniscono ai tribunali norme o prove applicabili. Nell'UE, i controlli obbligatori dei rischi, la trasparenza e la tenuta dei registri costituiscono parametri di riferimento chiari e una pista udibile che facilitano l'attribuzione degli errori ai sensi delle leggi aggiornate in materia di responsabilità. In Cina, la responsabilità rimane in gran parte uno strumento di controllo amministrativo; i precedenti in materia di conformità non si traducono automaticamente in norme di responsabilità, il che rende qualsiasi ricorso civile subordinato a una precedente azione regolatoria. L'articolo conclude che la responsabilità è un presupposto necessario per una responsabilità efficace in tema di IA, ma deve essere concepita come un meccanismo giuridicamente perseguibile e pronto ad agire per colmare il "vuoto di responsabilità" nella governance dell'IA.

Keywords: Generative Artificial Intelligence (GAI); Accountability; Non-contractual Liability; Eu AI Act; China AI regulation

Summary: 1. Introduction – 2. The Connection between Accountability Mechanisms and Non-Contractual Liability in Generative AI – 3. Comparative Analysis of Generative AI Accountability Mechanisms in the EU and China – 3.1 The EU: Horizontal Accountability through Unified Rules – 3.1.1 Establishing Obligations through Legally Prescribed Procedures – 3.1.2 Demonstrating Compliance through Third-Party Audits and Documentation – 3.1.3 Enforcing Accountability through a Multi-Nodal Network – – 3.2 China: Vertical Accountability through Sectoral Governance – 3.2.1 Defining Obligations through Administrative Mandates – 3.2.2 Validating Compliance through Administrative Procedures – 3.2.3 Enforcing Accountability through a Vertically Integrated Administrative Network – 4. Accountability Mechanisms and the Attribution of Non-Contractual Liability in Generative AI – 4.1 A Comparison of Obligation-Setting Paradigms – 4.2 Comparing How Compliance Evidence Is Produced and Used – 4.3 A Comparison of Enforcement Networks – 5. Conclusion.

1. Introduction

Generative AI systems have created new challenges for legal responsibility when they cause harm, exposing gaps in traditional liability frameworks. The opacity, autonomy, and complexity of advanced AI make it difficult to prove causation or fault under conventional negligence-based tort law. As a result, the risks associated with advanced AI, such as the erosion of individual autonomy and the proliferation of high-risk technologies, necessitate

legislative intervention to ensure that AI development remains within a safe and socially acceptable trajectory.[1] In response, policymakers and scholars have increasingly emphasised accountability mechanisms – such as transparency, documentation, and oversight requirements – as tools to bridge this "accountability gap" in AI governance.[2] By mandating measures like record-keeping, impact assessments, and human oversight, these mechanisms aim to ensure that someone can be called to account for an AI's actions. However, it remains unclear to what extent such accountability translates into actual non-contractual liability for damages. Does having an accountable AI system guarantee that victims can find a liable party and obtain compensation when things go wrong? This question is especially pressing in the context of generative AI, where outputs and risks may be unpredictable and diffuse.

The core inquiry asks: under what institutional conditions does accountability meaningfully contribute to assigning legal responsibility and allocating losses when AI-induced harm occurs? The European Union (EU) and China provide a revealing comparison because both have been at the forefront of AI regulation, but with contrasting approaches. This article examines how and under what conditions these accountability tools shape the attribution of non-contractual liability for generative AI in two major jurisdictions: the EU and China. By comparing these two regimes, the article sheds light on how different legal systems embed accountability into AI governance and what that means for victims seeking redress.

Our comparative analysis finds that accountability alone does not automatically guarantee liability. Accountability mechanisms only influence non-contractual liability outcomes when they are institutionalised in a legally actionable form. In practice, this means that mechanisms must produce clear standards of conduct and evidence that courts can use to adjudicate fault. The EU's framework establishes formal duties (e.g., on transparency and risk mitigation) and tangible compliance records (logs, technical documentation, conformity assessment reports) that can reduce evidentiary barriers in litigation. An injured party in the EU can thus rely on violations of these duties or on audit trails to establish negligence or defect, thereby linking *ex ante* accountability to *ex post* liability. China's model, on the other hand, treats accountability primarily as an administrative matter; the fulfilment or breach of AI governance duties is handled by regulators and does not inherently give rise to civil liability. Any link between accountability and tort liability in China is indirect: it depends on regulatory intervention (e.g., an authority sanctioning a provider for non-compliance) and on a court subsequently recognising that violation as evidence of fault in a lawsuit. Thus, differing institutional designs have led to divergent responsibility architectures: the EU's legal system

[1] W Shen, 'China's Future-Oriented Artificial Intelligence Legislation: Approaches and Key Priorities' (2024) Exploration and Free Views 5, 7 (publication readable in Chinese only).

[2] European Commission, 'Regulatory framework for AI' *Shaping Europe's digital future* (European Commission Digital Strategy) https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#1720699867912-1 accessed 19 January 2026; L Gatt, MT Lo Conte and ME Mazzarella, 'Analysis and Perspectives on the AI Act: Scope and Impact Assessment| Analisi e Prospettive Dell'AI Act: Ambito Di Applicazione e Valutazione d'impatto' (2025) 2 European Journal of Privacy Law & Technologies.; A Batool, D Zowghi and M Bano, 'AI Governance: A Systematic Literature Review' (2025) 5 AI and Ethics 326.

proactively integrates accountability into the liability regime, whereas China's system leaves a gap between the two, which is bridged on a case-by-case basis through administrative and judicial discretion.

In the following sections, the article first clarifies the theoretical link between accountability and liability in the AI context (Section 2), explaining how accountability is defined as a relational, process-oriented concept and why AI's features strain traditional liability models. Section 3 then provides a comparative examination of the EU and Chinese approaches to generative AI accountability, focusing on key dimensions such as the scope of obligations, the generation and use of compliance evidence, and enforcement structures. Next, Section 4 discusses how these accountability mechanisms shape or inform the attribution of non-contractual liability in each jurisdiction – illustrating, for example, how the EU's risk-based procedural obligations create pathways for legal claims, whereas China's approach makes liability contingent on administrative findings. Finally, Section 5 concludes by summarising the insights from this comparison. The conclusion highlights that accountability mechanisms are a necessary structural precondition for effective liability in AI governance, but their impact depends crucially on institutional design choices.

2. The Connection between Accountability Mechanisms and Non-Contractual Liability in Generative AI

Accountability is not a new term. It is widely regarded as an inherently positive principle, often invoked to signal transparency and reliability in governance. Accountability is essentially contested – there is no universal standard for what counts as accountable behaviour.[3] Standards vary across roles, over time, across contexts, and between different actors.[4] Broadly conceived, accountability serves as an umbrella concept in contemporary political and academic discourse. Koppell distinguished it in terms of five perspectives: transparency, liability, controllability, responsibility, and responsiveness.[5] Based on these perspectives, liability emerges as one dimension of accountability. In this evaluative sense, accountability denotes a positive judgment of institutional or individual behaviour, akin to notions of responsiveness and moral responsibility.[6] To be concise, accountability refers to the obligation to explain and justify actions, a notion that inherently presupposes a relationship between an actor (the accountor) and a forum (the accountholder or accountee).[7]

[3] WB Gallie, 'Essentially Contested Concepts' (1956) 56 Proceedings of the Aristotelian Society 167, 121–146.
[4] E Fisher, 'The European Union in the Age of Accountability' (2004) 24 Oxford Journal of Legal Studies 495, 510.
[5] JGs Koppell, 'Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder"' (2005) 65 Public Administration Review 94, 96.
[6] M Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' (2007) 13 European Law Journal 447, 450.
[7] C Pollitt, *The Essential Public Manager: Public Policy and Management* (Open University Press 2003) 89.

In legal accountability, the forum is typically a court. Legal accountability is the clearest form of accountability, as the evaluation of conduct relies on detailed legal standards established by civil, criminal, or administrative law, or by judicial precedent.[8] Since the emergence of AI technologies, accountability has evolved beyond its traditional legal and administrative meanings, encompassing new forms of responsibility and transparency in human–machine interactions.

Some scholars argue that accountability is a governance model that relies on assessing the social, economic, and ethical impacts, particularly in automated decision-making systems in sensitive domains. They note that in the AI era, accountability imposes on system developers the duty to assess and trace the real-world implications of their systems beyond technical metrics. It also requires them to ensure fairness in decision-making processes and to meet the public's expectations for responsible, safe, and trustworthy technologies. [9]

Accordingly, accountability in AI can be understood as a process-oriented model operating *ex ante*, in medias, and *ex post*. Thus, analysing accountability requires a structured framework. Bovens proposed a four-dimensional analytical framework that maps accountability relations according to four interrelated aspects: the nature of the forum before which an actor must justify its conduct, the type of actor bearing responsibility, the aspect of conduct for which account is rendered, and the nature of the obligation that binds the actor to respond. [10] Together, these dimensions provide a structured lens for understanding how accountability functions across institutional, legal, and technological contexts.

Drawing on the above structure, it is evident that accountability mechanisms can influence non-contractual liability. The primary aim of a liability mechanism is to secure post-harm remedies for victims and to facilitate the fair distribution of losses. [11] Therefore, liability functions primarily as an *ex post* remedy, addressing harm that has already occurred rather than preventing it *ex ante*. Due to the inherent complexity, opacity, and autonomy of AI and other emerging digital technologies, scholars have questioned whether the rationale of existing civil liability regimes remains effective for AI-related harm. [12] Under traditional legal frameworks, it becomes difficult to prove the causation of harm or to attribute liability to a specific human fault. [13] In the context of AI, accountability mechanisms play a compensatory role in addressing the "accountability gap" created by the opacity and autonomy of algorithmic systems. By imposing documentation, explainability, and traceability

[8] Bovens (n 6) 456.
[9] C Novelli, M Taddeo and L Floridi, 'Accountability in Artificial Intelligence: What It Is and How It Works' (2024) 39 AI & Society 1871.
[10] Bovens (n 6) 454-462.
[11] B A Koch, 'Liability for Emerging Digital Technologies: An Overview' (2020) 11 Journal of European Tort Law 115, 116.
[12] B Soyer and A Tettenborn, 'Artificial Intelligence and Civil Liability—Do We Need a New Regime?' (2023) 30 International Journal of Law and Information Technology 385, 387–388.
[13] Koch (n 11) 119-122.

requirements, such mechanisms provide the factual and normative basis for attributing non-contractual liability when harm occurs. [14]

3. Comparative Analysis of Generative AI Accountability Mechanisms in the EU and China

This section compares the EU's and China's generative AI accountability frameworks across three key dimensions, illustrating how each model's accountability mechanisms operate and how they shape conditions for legal responsibility.

3.1 The EU: Horizontal Accountability through Unified Rules

The EU AI Act exemplifies a horizontal accountability model: it imposes unified, cross-sectoral procedural duties (e.g. data governance, technical documentation, conformity assessments) across industries in a risk-based, proactive framework. [15] This shifts AI governance from after-the-fact punishment to proactive responsibility and creates a system of checks and balances that makes high-risk AI systems demonstrable and auditable.[16]

Some scholars argue that the principle of accountability in the EU operates as a meta-principle, providing the structural foundation for AI governance. It requires system operators to proactively document and demonstrate that relevant legal principles, duties, and regulatory rules have been implemented lawfully and appropriately, thereby ensuring the overall legal addressability and traceability of AI systems. [17] According to the Assessment List for Trustworthy Artificial Intelligence (ALTAI), accountability means an actor must take responsibility for their actions and the consequences that result. It also requires the actor to explain the purposes, motivations, and justifications behind those actions. This underscores that accountability is a multidimensional concept that often reflects ethical or normative expectations but does not always entail legally enforceable consequences. [18]

As the world's first comprehensive AI legislation, the EU AI Act does not provide an explicit definition of accountability. Nevertheless, it governs all AI systems and classifies them by risk level. By introducing a distinct category of high-risk AI systems, the Act frontloads a series of obligations – such as transparency, human oversight, and traceability – into the earliest stages of

[14] K Nabben, 'AI as a Constituted System: Accountability Lessons from an LLM Experiment' (2024) 6 Data & Policy e57, 1–4.
[15] A Bradford, 'The Brussels Effect' in Anu Bradford, *The Brussels Effect* (1st edn, Oxford University PressNew York 2020), 1-3, <https://academic.oup.com/book/36491/chapter/321182245> accessed 1 December 2025.
[16] M Ebers, 'Standardizing AI-The Case of the European Commission's Proposal for an Artificial Intelligence Act' [2021] The Cambridge handbook of artificial intelligence: global perspectives on law and ethics.
[17] M Durante and L Floridi, 'A Legal Principles-Based Framework for AI Liability Regulation' in J Mökander and M Ziosi (eds), *The 2021 Yearbook of the Digital Ethics Lab* (Springer International Publishing 2022), 101-102, <https://doi.org/10.1007/978-3-031-09846-8_7>.
[18] P Ala-Pietilä and others, *The Assessment List for Trustworthy Artificial Intelligence (ALTAI)* (European Commission 2020), 21-30.

system design. It requires developers to implement decision-logging mechanisms that support *ex ante* conformity assessments conducted by notified bodies. This model of preventive accountability departs from the traditional principle in continental civil liability law – namely, that in the absence of harm, no legal remedy is triggered – and instead establishes an active, preventive regulatory framework grounded in risk-prevention logic. [19]

The Act establishes an *ex ante* conformity assessment regime for high-risk AI systems, requiring developers to embed risk-mitigation measures throughout the technology's lifecycle, from design onward. In this sense, the EU's accountability framework shifts from *ex post* sanctioning to *ex ante* prevention. More specifically, based on the structure and regulatory design of the AI Act, the EU's logic of AI accountability can be understood as comprising three components:

3.1.1 Establishing Obligations through Legally Prescribed Procedures

The horizontal accountability model established by the EU AI Act is characterised by its transformation of accountability into a series of standardised procedural obligations spanning the entire lifecycle of an AI system (especially for high-risk AI systems). This reflects the EU's precautionary regulatory approach to uncertain risks, which focuses on regulating the development process rather than imposing specific outcomes. More specifically, these obligations form a coherent "procedural chain" that runs from upstream requirements (a risk management system under Article 9 and data governance under Article 10), through midstream requirements (comprehensive technical documentation under Article 11 and Annex IV), and ultimately to downstream obligations (human oversight under Article 14). [20]

This procedural chain embodies the shift toward an *ex ante* accountability framework. [21] For example, Article 10 establishes a legally enforceable duty of data justification. The requirements concerning data quality, representativeness, bias assessment, and documentation create a framework in which providers must be able to demonstrate *ex post* that their training data complied with the standards set out in Article 10. Where discriminatory harm occurs, courts may examine whether these obligations were fulfilled. Failure to do so constitutes a breach of statutory duty and provides strong evidence for fault. In this way, broad principles such as non-discrimination are translated into concrete requirements regarding data representativeness and bias mitigation,

[19] J Zhao and K Zhang, 'Legal Definition and Optimisation Paths of Artificial Intelligence Accountability'[2025] Journal of Beijing University of Aeronautics and Astronautics(Social Sciences Edition) 38, 42, 46, (publication readable in Chinese only).

[20] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L2024/1689.

[21] G Malgieri and F A Pasquale, 'From Transparency to Justification: Toward Ex Ante Accountability for AI' [2022] SSRN Electronic Journal <https://www.ssrn.com/abstract=4099657> accessed 1 December 2025.

supplying a traceable starting point for *ex post* review in discrimination litigation.[22] Likewise, the continuous risk-management obligation under Article 9 operationalises the abstract notion of a reasonable duty of care by embedding it in a dynamic, auditable management process. This provides objective behavioural standards against which fault can be assessed.

A particularly important feature of these procedural obligations is that they generate a set of standardised compliance documentation, including technical documentation and assessment reports, which primarily support regulatory audits and *ex post* accountability. According to Article 11 and Annexe IV, the technical file institutionalises regulatory transparency and serves as the link between these procedural obligations and the requirement of auditability. In liability proceedings, this documentation can become the first instrument for opening the algorithmic "black box." Failing to provide such documentation, or finding inconsistencies or deficiencies in it, constitutes non-compliance. These defects can be used to demonstrate fault or system deficiency, significantly reducing the information costs of verifying compliance at various checkpoints.[23]

Consequently, these obligations function not only as internal governance requirements, but also as outward-facing, standardised responsibility statements directed at notified bodies, market-surveillance authorities, and courts. They establish an objective, factual, and evidentiary foundation for subsequent conformity assessments [24] and for potential determinations of non-contractual liability.

3.1.2 Demonstrating Compliance through Third-Party Audits and Documentation

The AI Act ensures the effectiveness of procedural obligations by instituting a regime of mandatory demonstrability and auditability. This reflects a deliberate shift towards *ex ante* accountability, which requires not only implementing safeguards but also providing auditable justifications for them.[25] This approach builds upon the logic of earlier EU digital regulations, which also rely on documentation and verifiability to enforce compliance. [26] More specifically, the AI Act establishes a regulatory framework for high-risk systems that is designed to ensure demonstrability and auditability. At its core, this framework converts the compliance process into a verifiable and traceable chain of evidence that can be reviewed by the competent authorities. The framework follows a progressively layered logic:

First, the Act embeds transparency into a structured set of procedural obligations, transforming opaque system behaviour into traceable evidence. For example, Article 12's logging requirement mandates that high-risk AI

[22] Ebers (n 16) 15–16.
[23] H Felzmann and others, 'Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns' (2019) 6 Big Data & Society 1–4,11.
[24] J Mökander and others, 'Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations' (2021) 27 Science and Engineering Ethics 44, 8–10.
[25] Malgieri and Pasquale (n 21).
[26] M S Gal and O Aviv, 'The Competitive Effects of the GDPR' (2020) 16 Journal of Competition Law & Economics 349.

systems record relevant events to enable traceability, *ex post* verification, and supervisory oversight. Although Article 12 does not mandate immutable logs, it creates a system-level audit trail that directly addresses longstanding concerns about the accountability gap in opaque machine-learning systems. Rather than relying on the debated "right to explanation" for individual decisions, this mechanism ensures that regulators and auditors have access to structural transparency across the system's lifecycle.[27] Second, before a high-risk AI system is placed on the market, its compliance must undergo a formal conformity assessment. Section 3 (Articles 16–27) details specific obligations for providers, deployers, and other relevant actors. In addition, Articles 40–49 outline standards for conformity assessment, certification, and registration applicable to high-risk AI, ensuring that the entire compliance process is rule-based and traceable.

Finally, technical documentation and evidence of compliance must remain accessible for review. Under Article 21, providers must keep technical documentation readily available upon request by competent authorities, which is closely tied to the Union-level market surveillance powers in Article 74. As noted earlier, Article 11 requires that technical documentation be prepared to demonstrate the system's compliance and to provide the authority with all necessary information for a comprehensive assessment. Article 12 further specifies that, to maintain appropriate traceability, providers must implement logging capabilities to record relevant events.

Taken together, these requirements indicate that documentation must be maintained in a harmonised format. If harm occurs, such materials provide authorities and courts with a standardised factual basis. This greatly enhances the ability to verify whether statutory obligations were breached and significantly reduces the evidentiary burden of establishing fault.

3.1.3 Enforcing Accountability through a Multi-Nodal Network

The AI Act establishes a coordinated EU-wide governance system, in which national authorities and the European AI Office jointly oversee and enforce binding AI rules.[28]

It operates as a multi-node enforcement network composed of distinct but coordinated entities. National authorities and the European AI Office jointly oversee and enforce binding AI rules, with each acting as a node in a connected oversight system. [29] The national competent authorities constitute the distributed nodes on which the system heavily relies. Under Article 70 of the AI Act, each Member State acts as a node by designating "at least one notifying authority and at least one market surveillance authority". These national nodes

[27] S Wachter, B Mittelstadt and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International data privacy law 76.

[28] C Cancela-Outeda, 'The EU's AI Act: A Framework for Collaborative Governance' (2024) 27 Internet of Things 1, 8.

[29] European Commission, 'AI Office — Tasks and Governance' (Digital Strategy, European Commission, last updated 2025) <https://digital-strategy.ec.europa.eu/en/policies/ai-office#ecl-inpage-tasks-of-the-ai-office> accessed 3 December 2025.

are responsible for market surveillance and for ensuring compliance within their respective territories. The European Artificial Intelligence Board serves as the connector between the central node and the distributed nodes. Composed of one representative from each Member State, the Board is designed to promote consistency and coordination across the network. In addition, the Advisory Forum and the Scientific Panel operate as expert nodes, supplying technical input to the broader governance network (Articles 67–68).

3.2 China: Vertical Accountability through Sectoral Governance

In contrast to the EU's horizontal accountability approach, China adopts a vertical model. This vertical approach involves designing application-specific regulatory measures tailored to different categories of AI technologies and products. [30] Some scholars describe it as a "vertical and iterative" regulatory strategy, under which the state does not begin with a single comprehensive framework law, but instead regulates specific AI applications (such as recommendation algorithms and generative AI) sequentially and adaptively, refining techniques through successive rounds of rule-making and enforcement. [31] Based on China's current regulatory framework for artificial intelligence, it is evident that Chinese law classifies AI into distinct application types and regulates each category through separate, dedicated instruments (see Table 1).

Table 1

Name	Effective Date
Internet Information Service Algorithmic Recommendation Management Provisions[32]	01/03/2022
Provisions on the Administration of Deep Synthesis of Internet-Based Information Services [33] (The "Deep Synthesis Provisons")	10/01/2023
Interim Measures for the Administration of Generative Artificial Intelligence Services[34] (The "Interim Measures")	15/08/2023

[30] M Zou and L Zhang, 'Navigating China's Regulatory Approach to Generative Artificial Intelligence and Large Language Models' (2025) 1 Cambridge Forum on AI: Law and Governance e8, 3.
[31] M Sheehan, 'China's AI Regulations and How They Get Made' [2023] Horizons: Journal of International Relations and Sustainable Development 108, 116–117.
[32] Internet Information Service Algorithmic Recommendation Management Provisions (2022) Internet Information Service Algorithmic Recommendation Management Provisions (Department Rules, 2022) https://www.lawinfochina.com/display.aspx?id=37324&lib=law accessed 4 December 2025.
[33] Provisions on the Administration of Deep Synthesis of Internet-Based Information Services (2023)
Provisions on the Administration of Deep Synthesis of Internet-Based Information Services (Department Rules, 2023) https://www.lawinfochina.com/display.aspx?id=40228&lib=law accessed 4 December 2025.
[34] Interim Measures for the Administration of Generative Artificial Intelligence Services (2023) Interim Measures for the Administration of Generative Artificial Intelligence Services (Department Rules, 2023) https://www.chinalawtranslate.com/en/generative-ai-interim/#gsc.tab=0 accessed 4 December 2025.

Measures for Scientific and Technological Ethics Review (for Trial Implementation)[35]	01/12/2023
Measures for Labeling of AI-Generated Synthetic Content[36] (The "Labelling Measures")	01/09/2025

It should be emphasised that, in a strict normative sense, these four instruments are not statutory laws. They are administrative regulations jointly promulgated by central government authorities and are formally classified as departmental rules. Despite their non-statutory status, these instruments are legally binding and enforceable, and non-compliance may result in administrative penalties. Within this context, China's approach to AI accountability can be structured into three interrelated dimensions.

3.2.1 Defining Obligations through Administrative Mandates

As discussed above, China's current approach to AI governance is characterised by a decentralised, modular regulatory structure composed of sector-specific departmental rules, with a strong administrative orientation. Regulatory obligations are dispersed across multiple instruments rather than organised around a unified, process-oriented standard.

The Interim Measures constitute the key regulatory instrument targeting generative AI in China. However, they operate within the public law domain, imposing administrative duties on generative AI service providers. [37] These obligations may be quite concrete, but they are not designed to protect individual rights. Thus, compliance with the Interim Measures does not, by itself, constitute grounds for private civil liability. [38]

As a result, when generative AI-related non-contractual harms arise, the Interim Measures provide no direct guidance on how such harm should be translated into concrete private-law claims or liability rules. Although Chapter III of the Interim Measures sets out service norms and enumerates various duties of care for generative AI providers, and Chapter IV on supervision, inspection, and non-contractual liability continues to address provider responsibilities, these obligations are not self-contained within the Interim Measures. Specifically, Article 12 requires service providers to label generated content (such as images and videos) in accordance with the Provisions of Deep Synthesis, and Article 17 mandates that providers offering generative AI services with public opinion–shaping or social mobilization capacity conduct

[35] Measures for Scientific and Technological Ethics Review (for Trial Implementation) (2023) Measures for Scientific and Technological Ethics Review (for Trial Implementation) (Administrative Normative Document, 2023) https://www.lawinfochina.com/display.aspx?id=42015&lib=law accessed 4 December 2025.
[36] Measures for the Labeling of Artificial Intelligence Generated and Synthesized Content (2025) Measures for the Labeling of Artificial Intelligence Generated and Synthesized Content (Administrative Normative Document, 2025) https://www.lawinfochina.com/display.aspx?id=44383&lib=law accessed 4 December 2025.
[37] Z Yao, 'Legal Nature of Generative Artificial Intelligence Service Providers under Private Law' (2024) Journal of Shanghai Jiaotong University(Philosophy and Social Sciences) 32, 127, 127 (publication readable in Chinese only).
[38] H Zhang, 'The Imputation and Constituent Elements of Generative AI Tort Liability under the Dynamic Systems Theory' (2025) Law Science Magazine 46, 82, 90 (publication readable in Chinese only).

security assessments and complete algorithm filing, modification, or deregistration procedures pursuant to the Provisions on the Administration of Algorithmic Recommendation Services. These cross-references reveal that generative AI obligations are distributed across multiple instruments, all of which are departmental rules with a distinctly administrative character.

Furthermore, Article 7 of the Interim Measures enumerates obligations for training data processing and explicitly refers to higher-level statutes, including the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, and the Personal Information Protection Law of the People's Republic of China. However, the provision remains broadly framed. For instance, it merely requires providers to "take effective measures to improve the quality of training data," without specifying what constitutes "effective measures" or establishing clear evaluative criteria. In addition, the multiple statutory references in Article 7 overlap in scope, potentially making it difficult for regulated entities to delineate compliance boundaries and determine the precise allocation of responsibilities. This broad regulatory style, while offering flexibility to administrative authorities, undermines the rules' operability and weakens regulatory certainty in enforcement.

3.2.2 Validating Compliance through Administrative Procedures

Unlike the EU AI Act, China has not yet developed a comprehensive, unified compliance procedure for regulating generative AI. Nevertheless, its regulatory framework exhibits a three-stage structure encompassing *ex ante*, ongoing, and *ex post* controls.

Ex ante regulation: China has introduced security assessment and algorithm filing requirements for generative AI systems deemed capable of producing a significant social impact. Article 17 of the Interim Measures requires providers of generative AI services with public opinion–shaping or social mobilisation capacity to submit relevant materials to the authorities, pass a security assessment, and complete algorithm filing. Notably, this filing mechanism operates through reporting to and approval by administrative authorities. It is an upward-facing proof of compliance, rather than an audit by independent third parties or the public.

Ongoing regulation: Article 12 of the Interim Measures requires service providers to label AI-generated content (such as images and videos) in accordance with the Deep Synthesis Provisions. In March 2025, China promulgated the Labelling Measures, which specify in detail how AI-generated or synthetic content must be labelled. Article 20 of these Labelling Measures further requires providers, when completing procedures like algorithm filing and security assessment, to submit documentation on content labelling. In this way, process-based proof (labelling) supports the *ex ante* proof (filing), forming a closed evidentiary loop in the regulatory process.

Ex post regulation: The Interim Measures designate enforcement actors in very general terms, referring to "relevant authorities" without clarifying which specific bodies or how their responsibilities are divided. Article 19 obliges service providers to cooperate with inspections by competent authorities and to explain matters related to "the sources, scale, types, and labelling rules of

training data, as well as algorithmic mechanisms and principles," and to provide necessary technical and data support. The result is a governance structure with fragmented, overlapping oversight, often described as "multiple authorities governing the same domain." [39]

Some scholars have noted that, under the Interim Measures, China's regulation of generative AI services predominantly focuses on content generation as an information service, leaving unaddressed the potential risks to bodily integrity and health arising from the use of generative AI in physical systems such as robotics. [40]

3.2.3 Enforcing Accountability through a Vertically Integrated Administrative Network

China's vertical accountability model emphasises supervision and enforcement centred on administrative authority. The reference to "relevant competent authorities" in Article 19 of the Interim Measures is elastic, pointing to an administrative consortium in which the Cyberspace Administration of China (CAC) plays a central role, while other authorities (responsible for areas like development and reform, science and technology, industry and information technology, and public security) participate in a coordinated manner according to their mandates. [41] This design enables regulatory oversight to span the entire lifecycle of generative AI services, from data sources to algorithmic mechanisms. When service providers are required to "provide explanations" or "offer support," they are responding not to an independent auditor, but to a state administrative apparatus.

The shared supervisory and inspection powers exercised by multiple administrative bodies, each acting under its statutory functions, further reinforce the "vertical" character of accountability: providers are directly accountable to multiple administrative superiors, and enforcement standards and priorities may vary across authorities. While this arrangement enhances the deterrent effect of regulation, it may also increase compliance complexity and uncertainty. As some scholars have observed, unclear functional delineations among regulatory authorities may give rise to both overlapping supervision and regulatory gaps simultaneously. [42]

4. Accountability Mechanisms and the Attribution of Non-Contractual Liability in Generative AI

4.1 A Comparison of Obligation-Setting Paradigms

[39] B Xiao, 'Agile and Iterative Governance: China's Regulatory Response to AI' (2025) 58 Computer Law & Security Review 106183, 10.
[40] Yao n(37), 129.
[41] Interim Measures for the Administration of Generative Artificial Intelligence Services (n 34) art 16.
[42] X Shou, 'Normalised Regulatory Approaches to Competition over Generative Artificial Intelligence Foundation Models' [2025] Journal of Northwest Minzu University(Philosophy and Social Sciences) 93, 96–97 (publication readable in Chinese only).

From a comparative perspective, the EU and China adopt different paradigms for constructing obligations in generative AI governance. Both systems seek to set expectations for responsible AI development and deployment, but they diverge significantly in regulatory structure, normative technique, and their connection to legal consequences.

First, the two regimes differ in their overall regulatory orientation. As discussed in Part 3, the EU does not have a dedicated regulatory regime exclusively for generative AI. Instead, under the AI Act, generative AI systems are governed within a horizontal, risk-based framework in which obligations are triggered by the system's risk level in a given context of use. Depending on the sector and function in which a generative AI system is introduced, it may fall into one of four risk categories—unacceptable risk, high-risk, limited-risk, or minimal or no risk—each entailing a different set of obligations. By contrast, China adopts a more sector- and technology-specific approach.[43] Building on a subject- and service-oriented governance paradigm, Chinese regulators have promulgated dedicated rules targeting generative AI services, most notably the Interim Measures for Generative Artificial Intelligence Services, which directly address generative AI as a distinct regulatory object.

Second, the techniques of obligation-setting also differ markedly. Under the EU AI Act, accountability for high-risk AI systems is operationalised through standardised procedural obligations that collectively constitute a lifecycle "procedural chain". In contrast, China's Interim Measures impose public-law obligations on generative AI service providers primarily. [44]

Third, and most importantly, the two systems differ in the extent to which obligation-setting is linked to judicial consequences. In the EU, obligations under the AI Act are situated within a broader reform of AI liability. While the AI Act itself does not establish civil liability, it works in tandem with the revised Product Liability Directive (revPLD) to create a structured link between *ex ante* regulatory obligations and *ex post* liability assessment. [45]

More specifically, the AI Act serves as an *ex ante* control, prescribing mandatory safety, transparency, and risk-management requirements that AI systems must meet before entering the market. This role is especially pronounced for high-risk AI systems, which are subject to conformity assessments and extensive documentation and traceability obligations designed to render system behaviour auditable and reviewable. [46] These revPLD reforms complement the EU's accountability framework by ensuring

[43] Xin Zhang, 'Algorithmic Governance Challenges and Governance-Oriented Regulation of Generative Artificial Intelligence' (2023) Modern Law Science 45(3), 108, 108, 121–122 (publication readable in Chinese only).
[44] Yao (n 37), 127.
[45] Besides the AI Act, the EU institutions also debated the establishment of a dedicated AI liability regime. The proposed AI Liability Directive was ultimately withdrawn, and issues of civil liability for AI-related harm are now addressed primarily through the revised Product Liability Directive, which integrates AI systems and software into the existing product liability framework. European Parliament, 'AI Liability Directive' (Legislative Train, A Europe Fit for the Digital Age) <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive> accessed 2 January 2026.
[46] F Teichmann, 'Risk, Reasonableness and Residual Harm under the EU AI Act: A Conceptual Framework for Proportional Ex-Ante Controls' [2026] European Journal of Risk Regulation 1.

that victims of AI-related harm have clearer pathways to compensation,[47] thereby illustrating the EU's preference for strengthening legal remedies as part of its accountability strategy.

By contrast, China has not undertaken a similar update of its civil liability regime specifically for AI-related harm. Generative AI-related damage continues to be governed primarily by the general tort provisions of the Civil Code.[48] As a result, the obligations set out in administrative regulations like the Interim Measures do not automatically translate into legally actionable standards for civil liability. This divergence in techniques has important implications for legal addressability. As noted in Section 3.1.1, in the EU, accountability obligations are deliberately designed as legally reviewable standards of conduct, such that their violation may be directly invoked in *ex post* judicial proceedings to assess fault. As noted in Section 3.2.1, China's obligations remain administrative and don't carry over to civil liability unless picked up by courts.

4.2 Comparing How Compliance Evidence Is Produced and Used

The allocation of compliance responsibilities differs: the EU spreads obligations across various actors in the AI value chain (providers, deployers, etc.), whereas China's rules concentrate obligations mainly on service providers (i.e., AI developers).

As noted in Section 3.1.2, the AI Act mandates documentation and audits, thereby producing evidence that can later be used in court. By contrast, the Interim Measures define AI developers primarily through the lens of service provision.[49] This definitional divergence reflects a deeper regulatory orientation. The AI Act centres on development and placing on the market as the core triggers of regulatory responsibility, whereas the Interim Measures place greater emphasis on the use of the technology and the provision of services, thereby anchoring obligations more directly to service-facing activities rather than the full AI lifecycle of development and commercialisation.

With respect to liability, the EU and China diverge in the extent to which compliance evidence translates into proof of fault. The EU's system intentionally produces what might be described as a "pre-packaged" evidentiary kit for liability. Technical documentation, conformity assessments, and audit logs constitute a harmonised body of evidence that can be used directly in civil or administrative proceedings. Because the AI Act requires detailed technical documentation and record-keeping for high-risk systems, this documentation serves not only as evidence of compliance but also as evidence that courts can rely on when deciding liability. Non-compliance or inconsistencies in this evidence can constitute prima facie evidence of a breach

[47] B Botero Arcila, 'AI Liability in Europe: How Does It Complement Risk Regulation and Deal with the Problem of Human Oversight?' (2024) 54 Computer Law & Security Review 106012.
[48] L Wang, 'Principles of Attribution of Liability and Fault Determination in Generative Artificial Intelligence Torts' (2025) China Law Review (04), 15, 16 (publication readable in Chinese only).
[49] Interim Measures for the Administration of Generative Artificial Intelligence Services (n 34) art 22 (1) (2).

of statutory duty, thereby easing the informational burden for claimants in complex AI cases.[50]

In China, by contrast, administrative compliance records are not as readily converted into standardised evidence of civil fault. Violations (for example, operating without a required filing) will directly trigger administrative penalties, but their significance in private litigation is more indirect. The Chinese regime places primary responsibility for AI risk and safety within administrative frameworks such as the Interim Measures and related data or security statutes. However, these measures do not create a clear, unified evidentiary pathway for civil liability that aligns with civil procedural expectations of documentation and proof,[51] as observed in other jurisdictions. As noted by scholars, while the Interim Measures fall short of offering detailed regulation on issues like data processing, service provider obligations, and user rights in the context of generative AI, they nonetheless function as a regulatory bridge through which generative AI is brought within the scope of existing legal governance structures.[52]

Taken together, these differences reveal a structural contrast in legal design. The EU model produces generic, system-level compliance evidence deliberately engineered to travel across regulatory and judicial forums, creating a well-defined pipeline from accountability to liability. China's model produces authoritative but context-specific administrative records, whose primary function lies within the bureaucratic hierarchy and whose migration into civil liability adjudication is neither automatic nor guaranteed.

4.3 A Comparison of Enforcement Networks

The EU and China establish distinct enforcement networks for AI governance. The EU's model is multi-nodal and horizontally coordinated, with supervisory and enforcement powers distributed across both EU-level and national authorities. The European AI Office operates as a central coordinating node within the Commission, while national competent authorities act as distributed nodes responsible for market surveillance in their jurisdictions, connected through the European Artificial Intelligence Board and supported by expert bodies such as the Advisory Forum and the Scientific Panel.[53] By contrast, China's model is state-centric,[54] operating through a vertically integrated

[50] C Novelli and others, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity' (2024) 55 Computer Law & Security Review 106066, 2–4; D F Llorca and others, 'Liability Regimes in the Age of AI: A Use-Case Driven Analysis of the Burden of Proof' (2023) 76 Journal of Artificial Intelligence Research 613, 616,628.

[51] Le Ma, 'A Study on the Attribution Path of Deep Synthesis Service Provision' [2025] Seeking Truth 52, 123, 131–132 (publication readable in Chinese only).

[52] Xiongbiao Ye and others, 'Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective' (2024) 48 Telecommunications Policy 102851, 5.

[53] European Commission, 'Governance and enforcement of the AI Act' (EU Digital Strategy, last updated 2025) <https://digital-strategy.ec.europa.eu/en/policies/ai-act-governance-and-enforcement> accessed 5 January 2026; European Commission, 'Article 70: Designation of national competent authorities and a single point of contact' (AI Act Service Desk) <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-70> accessed 5 January 2026.

[54] J Qian, *Governing China's Digital Transformation: Industrial Policy, Regulatory Governance, and Innovation* (Taylor & Francis 2025),16.

administrative network in which supervisory authority is concentrated within a constellation of regulators led by the CAC, complemented by the participation of other departments pursuant to their statutory mandates. Rather than coordination among autonomous nodes, accountability in China is embedded in hierarchical administrative relationships.[55]

These enforcement networks entail distinct trade-offs among legal certainty, enforcement intensity, and compliance predictability. The AI Act explicitly enumerates supervisory bodies and assigns their competences in a relatively precise manner. By contrast, the Interim Measures rely on the open-ended notion of supervision by "relevant competent authorities," without clearly defining which authorities it covers or how their competences are delineated.

This regulatory openness is not accidental; it reflects what has been described as the "fuzzy logic" of Chinese technology and innovation policy, in which key legal concepts are deliberately left underdefined to preserve administrative flexibility and enable agile regulatory intervention.[56] Within this framework, China's vertically integrated enforcement model strengthens regulatory deterrence and responsiveness by facilitating swift and comprehensive administrative action. However, it may also increase compliance uncertainty for regulated actors, as overlapping mandates and elastic references to "relevant competent authorities" blur the boundaries of responsibility and enforcement expectations. [57] By contrast, the EU's networked enforcement structure under a horizontal legal framework enhances procedural predictability and legal certainty by anchoring accountability in rule-based supervisory processes with clearly allocated institutional competences, [58] but it may simultaneously dilute enforcement intensity due to institutional fragmentation and the need for inter-authority coordination.[59]

5. Conlusion

Recall that AI's opacity and complexity strain traditional liability models, which is why accountability mechanisms are intended to bridge this 'accountability gap'. The analysis indicates that accountability shapes the non-contractual liability of generative AI only when it is institutionalised in a legally addressable and judicially usable form. It does not gain legal significance through normative appeal or regulatory intensity alone, but through its capacity to crystallise clear standards of conduct, generate transferable compliance evidence, and allocate responsibility within forums capable of adjudicating fault and remedies. From this perspective, the EU's accountability model is structurally aligned with civil liability attribution: procedural obligations under the AI Act function as binding standards, lower evidentiary

[55] R Creemers, 'The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy' (2024) 33 Journal of Contemporary China 173, 183.
[56] M Parasol, *AI Development and the 'fuzzy logic'of Chinese Cyber Security and Data Laws* (Cambridge University Press 2021), 7,12–13,38.
[57]Xiao (n 39), 9.
[58] ibid, 13.
[59] C Novelli and others, 'AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act' (2024) 3 Digital Society 13, 19–20.

barriers in AI-related harm cases, and enable regulatory findings to flow into judicial proceedings. China's accountability framework, by contrast, prioritises administrative supervision and regulatory flexibility, confining accountability largely within vertically integrated enforcement networks. While this model enhances regulatory responsiveness, it also means that the relationship between accountability and civil liability is contingent on administrative intervention and subsequent judicial reception, rather than being built into the system's design.

Accountability is not a substitute for liability and by itself offers no guarantee of compensation. Instead, it serves as a necessary structural precondition for the effective functioning of liability in generative AI governance, and institutional choices in the EU and China have led to divergent responsibility architectures.