

AI in the Cloud: Legal Accountability for Intelligent Infrastructure

KHRAISHA, WASIM*

ABSTRACT *The convergence of Artificial Intelligence (AI) and cloud computing marks a fundamental shift in the digital ecosystem. Modern cloud infrastructures increasingly embed AI-driven mechanisms that autonomously allocate resources, enhance cybersecurity, and enhance performance, creating what may be called “intelligent infrastructure”. This self-learning model transforms the cloud from a passive service platform into an active decision-making environment. However, this transformation raises complex questions of legal accountability and transparency within the European Union’s regulatory framework. The existing legal instruments including the General Data Protection Regulation (GDPR), the NIS2 Directive, the AI Act, and the Cybersecurity Act assign multiple obligations among cloud service providers, users, and AI developers, leaving critical accountability gaps. This article argues that intelligent infrastructures require a reconfiguration of liability models to address autonomous decision-making and shared responsibility. It proposes a hybrid approach that combines contractual governance with regulatory compliance, ensuring that accountability remains traceable, enforceable, and compatible with EU digital law.*

KEYWORDS *Artificial Intelligence, Cloud Computing, Legal Accountability, EU Law, Intelligent Infrastructure.*

1. Introduction

The integration of Artificial Intelligence (AI) into cloud computing infrastructures has fundamentally altered the nature of digital service provision. Cloud platforms no longer operate merely as passive storage or computational environments but increasingly incorporate AI systems capable of autonomous learning, decision-making, and optimization. The result is the emergence of what may be called “*intelligent infrastructure*” which is a dynamic, self-adaptive technological framework that continuously modifies its operations based on real-time data flows and predictive analytics. This evolution holds transformative potential for efficiency, resilience, and innovation within the digital economy, yet

* PhD student, Károli Gáspár University of the Reformed Church in Hungary, Doctoral School of Law and Political Sciences.

it also weaken the established notions of accountability, transparency, and liability under EU laws.

AI-driven automation at the infrastructure: such as risk detection, and data lifecycle management, means that critical operational decisions are often made without direct human intervention.¹ This essential change from human control to algorithmic model challenges the traditional legal models that presuppose identifiable human factor affected of intent and negligence.² Within the EU, regulatory mechanisms such as the General Data Protection Regulation (GDPR),³ the NIS2 Directive,⁴ and the AI Act⁵ collectively establish frameworks for risk management, transparency, and responsibility, yet they remain fragmented when applied to integrated AI–cloud systems. The resulting legal uncertainty raises the question: *who is accountable when intelligent infrastructures make an error or mistake?*

Accountability in the context of intelligent infrastructure must therefore be understood as a distributed concept. Unlike conventional cloud models, where liability could be assigned contractually between the cloud service provider (CSP) and the customer, the introduction of AI creates multi-agent decision environments involving software developers, AI model providers, CSPs, and end-users.⁶ Each actor contributes to the functioning of the system, but no single entity have the full control. The European Commission’s Digital Decade Strategy recognizes that such technological convergence requires “trustworthy, transparent, and accountable” AI systems, especially where they support essential digital services.⁷

Yet, despite these policy ambitions, existing legal frameworks have struggled to reconcile the technical opacity of AI systems with the normative demands of accountability. The so-called *black box* problem where the internal logic of machine learning systems resists interpretability undermines the transparency principles enshrined in Article 5(1)(a) of the GDPR and the rights to explanation

¹ Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing* (NIST Special Publication 800-145, 2011), 3–5.

² Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford: Oxford University Press, 2020), 221–224.

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) 2016.

⁴ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive) 2022.

⁵ European Parliament and Council of the European Union, *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, OJ L, 12 July 2024.

⁶ Christopher Millard, ed., *Cloud Computing Law*, 2nd ed. (Oxford: Oxford University Press, 2021), 45–52.

⁷ European Commission, *2030 Digital Compass: The European Way for the Digital Decade* COM (2021).

under Articles 13–15 and 22 GDPR.⁸ The AI Act attempts to address this through obligations of transparency, documentation, and risk assessment, but it mostly focuses on application-level AI rather than embedded infrastructural intelligence.⁹

This article adopts a doctrinal and analytical method to explore how EU law conceptualizes and allocates accountability in the context of AI-enabled cloud infrastructures. It argues that while EU digital regulation establishes strong sectoral frameworks for data protection, cybersecurity, and AI governance, the intersection of these regimes reveals structural gaps. The absence of a unified approach to intelligent infrastructure risks diffusing responsibility among multiple actors and weakening enforcement. Accordingly, this paper advances three propositions. First, *intelligent infrastructure* constitutes a novel regulatory object that cannot be fully captured by existing categories of software, service, or processor under current EU law. Second, the integration of AI at the infrastructural level creates a need for *shared accountability models* capable of integrating technical traceability, contractual governance, and regulatory oversight. Third, the development of such models requires a hybrid approach combining compliance duties with liability allocation mechanisms.

By dealing with these issues within the evolving EU digital regulatory frameworks including the AI Act, GDPR, NIS2, and the Cybersecurity Act, this article contributes to the broader discussion on how law can maintain effective accountability in the age of intelligent infrastructure.

2. The Technological Context: AI in Cloud Infrastructure

The evolution of cloud computing from a service-based model to an intelligent infrastructure marks a significant shift in the architecture of the digital economy. Traditional cloud environments structured around the delivery of infrastructure, platforms, and software as services are being progressively re-engineered through the integration of AI systems that enable autonomous monitoring, optimization, and security. The resulting convergence has transformed the cloud into a *self-adaptive ecosystem* in which computational resources and network configurations evolve dynamically in response to real-time data patterns.¹⁰

AI systems could be rooted across the three deployment models of cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Within the IaaS, machine-learning algorithms

⁸ Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,” *International Data Privacy Law* 7, no. 2 (2017): 76–99.

⁹ European Commission, *Impact Assessment Accompanying the Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence*, SWD(2021) 84 final, 12–15. Available at: <https://edz.bib.uni-mannheim.de/edz/pdf/swd/2021/swd-2021-0084-1-en.pdf?utm>.

¹⁰ Organisation for Economic Co-operation and Development (OECD), *The Cloud Ecosystem and Its Role in Digital Transformation* (Paris: OECD Publishing, 2021).

manage virtual machines, predict hardware failures, and optimize energy consumption through continuous learning.¹¹ At the PaaS level, AI models orchestrate data pipelines, automate load balancing, and allocate storage in proportion to demand.¹² In SaaS applications, AI governs user authentication, personalization, and threat detection. The cloud thereby becomes not merely a neutral hosting environment but a decision-making entity capable of governing its own performance.¹³

The operational logic of this intelligent infrastructure relies on *data feedback loops*. AI systems take in and deal with vast quantities of operational data, CPU performance metrics, network latency, and user behavior to train predictive models that anticipate future conditions.¹⁴ This enables the infrastructure to scale resources before congestion occurs or to isolate potential security risks before breaches appear.¹⁵ In technical terms, the cloud evolves from a reactive to a *proactive* infrastructure, advanced by anticipatory control and self-recovery mechanisms.¹⁶

However, the autonomy of these systems introduces significant challenges for legal accountability. Decisions once made by system administrators, such as routing data through specific servers or initiating security patches, are now delegated to algorithms that act without human intervention.¹⁷ The European Union Agency for Cybersecurity (ENISA) has recognized that AI-enabled automation in cloud infrastructures blurs the traditional boundaries of control and responsibility between the service providers and users.¹⁸ This automation complicates the application of existing legal doctrines that presuppose a clear chain of human control.

¹¹ National Institute of Standards and Technology (NIST), *The NIST Cloud Computing Reference Architecture*, Special Publication 500-292 (2018), section 2.3.

¹² European Union Agency for Cybersecurity (ENISA), *Artificial Intelligence and Cloud Security: Technical Guidelines* (2023), section 3.1. available at: <https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai?utm>.

¹³ Christopher Millard, ed., *Cloud Computing Law*, (Oxford: Oxford University Press, 2021), ch. 3 “Control and Responsibility in Cloud Service Provision.”

¹⁴ ENISA, *Artificial Intelligence and Cybersecurity: Challenges at the Infrastructure Level* (2021), section 2.

¹⁵ Lekkala, Chandrakanth, “AI-Driven Dynamic Resource Allocation in Cloud Computing: Predictive Models and Real-Time Optimization,” *J Artif Intell Mach Learn & Data Sci* 2 no. 2 (2024) Available at SSRN: <https://ssrn.com/abstract=4908420>.

¹⁶ Buyya, Rajkumar, et al. “Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities.” *10th IEEE International Conference on High Performance Computing and Communications (HPCC 2008)*, 5–13.

¹⁷ Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford: Oxford University Press, 2020), chapter 8 “Accountability and Automation.”

¹⁸ ENISA, *A Multilayer Framework for Good Cybersecurity Practices for AI* (Athens: European Union Agency for Cybersecurity, June 7 2023. Available at: <https://www.enisa.europa.eu/sites/default/files/publications/Multilayer%20Framework%20for%20Good%20Cybersecurity%20Practices%20for%20AI.pdf?utm>.

From a data protection perspective, intelligent infrastructure also transforms the nature of processing activities. Automated orchestration tools continuously analyze data to predict workload trends, potentially resulting in the incidental processing of personal or pseudonymized information during system optimization.¹⁹ This raises interpretive questions under the GDPR regarding the role of cloud providers as controllers or processors when such decisions are not directly instructed by the client.²⁰ The European Data Protection Board (EDPB) has repeatedly emphasized that determining controllership depends on *factual influence over processing*, yet in intelligent infrastructures, that influence is spread across multiple algorithmic and organizational layers.²¹ Beyond data protection, the AI-driven transformation of the cloud has implications for cybersecurity regulation under the NIS2 Directive and the EU Cybersecurity Act. Autonomous systems can boost resilience by detecting errors more rapidly than human operators, but they also create new vulnerabilities when adversarial attacks manipulate machine-learning models themselves.²² The principle of *security by design* explained in Article 21 of NIS2; thus requires explanation in the context of self-modifying infrastructures.

The integration of AI into cloud systems also reflects a broader shift toward what is called *cognitive infrastructure*, digital architectures have decision-making capacities that compete with traditional organizational governance.²³ But, this development raises essential questions about responsibility, whereas if an autonomous resource-allocation system causes a service outage or a security breach -for example-, is liability assigned to the provider who deployed it, the developer who trained the model, or the user whose data caused the decision?²⁴ The answer remains unclear under EU law, where accountability frameworks are still largely based on assumption of human supervision. Finally, intelligent infrastructure complicates contractual governance. Traditional Service Level Agreements (SLAs) specify performance metrics and fault responsibilities,

¹⁹ European Data Protection Board (EDPB), Guidelines 05/2020 on Consent under Regulation 2016/679 (2020), section 36. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf?utm.

²⁰ European Data Protection Board (EDPB), Guidelines 05/2020 on Consent under Regulation 2016/679 (2020), section 36. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf?utm.

²¹ Regulation (EU) 2016/679 (General Data Protection Regulation), Arts. 4(7) and 28.

²² EDPB, *Guidelines 07/2020 on the Concepts of Controller and Processor* (2021), section 13. Available at: https://www.edpb.europa.eu/system/files/en?file=2023-10%2FEDPB_guidelines_202007_controllerprocessor_final_en.pdf&utm.

²³ Luciano Floridi, "Establishing the Rules for the Digital Environment: Accountability and Transparency in AI Infrastructure," *Philosophy & Technology* 35, (2022)

²⁴ Thomas Schneider and Michael Veale, "Algorithmic Governance and the Allocation of Responsibility," *Law and Contemporary Problems* 84, (2021).

assuming predictable human control over the system. When AI algorithms continuously adjust configurations, Performance standards can change independently, making fixed contractual obligations insufficient.²⁵ Scholars have begun to argue that *adaptive contracts*, which evolve through automated monitoring and shared dashboards, may become necessary to ensure legal certainty in AI-driven cloud environments²⁶. Such mechanisms would align with the European Commission’s call for “trustworthy and human-centric AI” while acknowledging that responsibility in intelligent infrastructures must be distributed, auditable, and legally traceable.²⁷

AI integration would transform the cloud infrastructure from what could be described as a passive channel of digital services into an active participant in decision-making. While this evolution enhances efficiency and resilience, it simultaneously challenges legal frameworks that rely on human accountability. The next section, therefore, examines how the EU’s regulatory architecture, including the GDPR, NIS2 Directive, AI Act, and Cybersecurity Act, approaches accountability in the era of intelligent infrastructure.

3. The EU Regulatory Framework for AI and Cloud Accountability

The EU regulatory approach to digital technologies is characterized by a layered architecture of interrelated instruments that collectively govern data protection, cybersecurity, and artificial intelligence. Each of these legal instruments reflects distinct policy rationales, yet their interaction forms the foundation of accountability in intelligent infrastructures. The GDPR for instance, establishes the standard nature of accountability through principles of transparency, lawfulness, and responsibility in data processing.²⁸ While the NIS2 Directive complements this by imposing cybersecurity obligations on entities providing essential and important digital services, including cloud computing providers.²⁹ The Cybersecurity Act contributes to a European framework for certification and trust in digital products,³⁰ while the AI Act seeks to harmonize standards for AI systems according to their risk level.³¹ Together, these regulations constitute a

²⁵ European Commission, *Cloud Contracts and Service Level Agreements for Digital Europe*, 2020, section 2.

²⁶ Jörn Gräber, “Smart Contracts and Dynamic Cloud Services: Legal Perspectives,” *Computer Law & Security Review* 43, (2021).

²⁷ European Commission, *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on Artificial Intelligence (2019). Available at: <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms?utm>.

²⁸ Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1, Art. 5.

²⁹ Directive (EU) 2022/2555 (NIS2 Directive) [2022] OJ L 333/80.

³⁰ Regulation (EU) 2019/881 (Cybersecurity Act) [2019] OJ L 151/15, Art. 46.

³¹ European Commission, “*AI Act | Shaping Europe’s digital future*,” Brussels: European Union, 2024. Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai?utm>.

regulatory framework that seeks to operationalize accountability in a technologically complicated multi-layer environment.

Under the GDPR, accountability is both a principle and a duty. Article 5/2 expressly provides that controllers are responsible for compliance and must be able to demonstrate it.³² This dual aspect *responsibility* and *demonstrability* is central to the governance of intelligent infrastructure, where automated processing decisions may occur without human awareness.³³ The GDPR thus requires that entities deploying AI-enabled cloud services maintain records of processing activities, implement data protection by design and by default (Article 25), and ensure transparency in automated decision-making (Articles 13–15 and 22).³⁴ Yet the regulation suggests that the controller possesses meaningful knowledge of and control over the processing operations. In AI-driven infrastructures, this assumption differs since algorithmic decision-making within the infrastructure may be ambiguous even to the CSPs.³⁵

The European Data Protection Board (EDPB) has clarified that the determination of controllership must rest on the *factual influence* exercised over processing rather than on contractual formalities.³⁶ However, in intelligent infrastructures, that influence is distributed: AI modules developed by one actor may trigger decisions affecting data controlled by another, mediated by a CSP. The GDPR's double distinction between controller and processor, therefore, becomes difficult to afford in the context of distributed AI–cloud ecosystems.³⁷ Scholars have suggested that the model of *joint controllership*, recognized by the Court of Justice of the European Union (CJEU) in *-Wirtschaftsakademie Schleswig-Holstein* and *Fashion ID-* cases, might better capture this shared accountability.³⁸ Yet even joint controllership presumes identifiable human decision-making and may fall in where AI operates autonomously.

Cybersecurity regulation under the NIS2 Directive reinforces accountability through obligations of risk management and incident reporting. The Directive applies to CSPs as entities of high criticality, requiring them to adopt technical and organizational measures equal with the risk level of their services.³⁹ Article

³² GDPR, Art. 5(2).

³³ Christopher Kuner, Lee Bygrave, and Christopher Docksey, eds., *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020).

³⁴ GDPR, Arts. 13–15, 22, and 25.

³⁵ Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford: Oxford University Press, 2020), chapter 8 “Accountability and Automation.”

³⁶ European Data Protection Board (EDPB), *Guidelines 07/2020 on the Concepts of Controller and Processor* (2020), section 13. Available at: https://www.edpb.europa.eu/system/files/en?file=2023-10%2FEDPB_guidelines_202007_controllerprocessor_final_en.pdf&utm.

³⁷ Orla Lynskey, “Distributing Responsibility: Data Controllers in EU Data Protection Law,” *Common Market Law Review* 50 (2013).

³⁸ Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein GmbH v. ULD* [2018] ECLI:EU:C: 2018:388; Case C-40/17 *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV* [2019] ECLI:EU:C: 2019:629.

³⁹ NIS2 Directive, Art. 21(1).

21 of it mandates the implementation of “appropriate and proportionate” security measures, including policies on risk analysis, supply-chain security, and vulnerability management.⁴⁰ These duties align with the principle of *security by design*, yet they raise practical difficulties when AI components autonomously modify system configurations. The Directive’s emphasis on human oversight may not easily translate into environments governed by self-learning algorithms, which can alter network behaviors without operator intervention.⁴¹

The EU Cybersecurity Act complements NIS2 by establishing the European Cybersecurity Certification Framework, under which cloud and AI services may obtain voluntary certification for compliance with defined assurance levels.⁴² The framework aims to strengthen trust and accountability through standardization and transparency. ENISA, acting as the central authority, has proposed certification schemes for cloud services (EUCS) and for AI systems, emphasizing continuous monitoring, risk documentation, and post-market surveillance.⁴³ In principle, these mechanisms could support accountability in intelligent infrastructures by providing auditable assurance trials. However, their voluntary nature and the absence of harmonized criteria for AI–cloud integration limit their effectiveness.

The AI Act introduces a risk-based model of governance that explicitly addresses accountability, albeit primarily for autonomous AI systems rather than established infrastructure. It categorizes AI systems into unacceptable, high, and limited risk, imposing the most firm obligations on high-risk systems.⁴⁴ These include requirements of technical documentation, human supervision, accuracy, and cybersecurity (Articles 9–15).⁴⁵ Cloud infrastructure hosting AI services may itself be classified as *high-risk* when it supports critical digital functions, though the distinction between provider and deployer remains ambiguous.⁴⁶ Recital 60 of the AI Act acknowledges that responsibility should rest with the entity exercising control over the AI system’s operation, but in cloud contexts, control is shared across multiple contractual and technical layers.⁴⁷ This diffusion of responsibility agency challenges the AI Act’s conception of accountability. Importantly, the AI Act interacts with the GDPR and NIS2 requiring careful coordination. Both the European Parliament and the Council have emphasized that the AI Act must be applied -without prejudice- to the GDPR’s data protection

⁴⁰ Ibid., Art. 21(2).

⁴¹ ENISA, *Artificial Intelligence Threat Landscape* (2022), section 5. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022?utm>.

⁴² Cybersecurity Act, Arts. 46–49

⁴³ ENISA, *Cybersecurity of AI and Standardisation* (Athens: ENISA, 7 June 2023). Available at: <https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation?utm>.

⁴⁴ AI Act, Arts. 6–9.

⁴⁵ Ibid., Arts. 9–15

⁴⁶ Baker Donelson, “Who’s Who under the EU AI Act: Spotlight on Key Actors,” Baker Donelson Insights (2024). Available at: <https://www.bakerdonelson.com/whos-who-under-the-eu-ai-act-spotlight-on-key-actors?utm>.

⁴⁷ Baker Donelson, “Who’s Who under the EU AI Act: Spotlight on Key Actors,”

regime and the sectoral obligations of NIS2.⁴⁸ Nevertheless, overlaps are there. For instance, the AI Act's requirement for data quality and bias mitigation overlaps with the GDPR's fairness principle, while its cybersecurity provisions are similar to those in NIS2.⁴⁹ Without explicit cross-references or guidance, operators of intelligent infrastructures may face conflicting or duplicative compliance duties.

Beyond these core instruments, several EU policy initiatives reinforce the accountability framework. The *European Data Strategy* (2020) and *Digital Decade Policy Programme* (2022) indicate the vision of a -trusted and human-centric digital environment- based on transparency, traceability, and interoperability⁵⁰. The forthcoming *European Cloud Rulebook* aims to harmonize contractual and technical standards for cloud providers, further embedding accountability within service governance.⁵¹ ENISA's guidelines on AI security complement these efforts by recommending continuous risk assessments, explainability tools, and auditable logging mechanisms for AI components in cloud environments.

The EU's legal landscape on AI and cloud accountability is comprehensive yet fragmented. The GDPR maintains the principle of accountability in data processing, the NIS2 Directive and Cybersecurity Act extend it to system resilience and certification, and the AI Act introduces risk-based oversight for AI systems. What remains unresolved is the integration of these frameworks into a coherent model capable of governing *intelligent infrastructure* systems in which accountability must overpass algorithmic, contractual, and regulatory boundaries.

4. Legal Challenges of Accountability in Intelligent Infrastructure

The introduction of AI into cloud infrastructure exposes deep gaps in the legal concept of accountability. While in the traditional doctrines of liability are predicated on identifiable actors – natural or legal persons whose decisions can be traced, evaluated, and sanctioned, in intelligent infrastructures, however, much of the decision-making process occurs autonomously, arranged by algorithms

⁴⁸ Council of the European Union, *General Approach on the Artificial Intelligence Act*, 6 December 2022, section 5.

⁴⁹ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), *Joint Opinion 5/2021 on the Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act)* (Brussels, 18 June 2021), available at: https://www.edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf?utm_

⁵⁰ European Commission, *Digital Decade Policy Programme 2030* (Brussels: Decision (EU) 2022/2481, 14 December 2022). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022D2481&utm_

⁵¹ European Commission, "Cloud computing | Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/policies/cloud-computing?utm_

that evolve through continuous learning.⁵² This creates a structural asymmetry in the legal responsibility.

The first and most fundamental challenge concerns the **Assignment of responsibility**. Under EU law, accountability typically follows control: the entity that determines the purposes and means of processing -under the GDPR- or the operator of an important service under NIS2 is considered responsible for compliance.⁵³ Yet intelligent infrastructures challenge these dual roles. Decision-making power is distributed across multiple layers, AI model developers, CSPs, and customers, all contributing to a system whose behavior emerges from the interaction of numerous subsystems.⁵⁴ When an AI-optimized resource allocator unintentionally deprioritizes in important data set, leading to a service outage, determining the liable party becomes nearly impossible.⁵⁵ This dispersion arises in the opacity of AI systems, and machine learning models that are rooted within infrastructure layers of the intelligent infrastructure, such as anomaly detection or predictive scaling operate through statistical connections that are often non-interpretable even to their creators.⁵⁶ The GDPR's transparency obligations (Articles 5 and 13–15) entail the existence of human understandable explanations for processing activities, yet this assumption collapses in the face of algorithmic opacity.⁵⁷ Similarly, the AI Act's provisions on documentation and human oversight require that systems be (sufficiently transparent to enable users to interpret their output),⁵⁸ a standard difficult to satisfy when the user is itself another automated process within a cloud platform.⁵⁹ The lack of interpretability thus creates a practical space, and then responsibility cannot be meaningfully exercised when the underlying decisions cannot be reconstructed or explained.⁶⁰ The **contractual structure** such as Service Level Agreements (SLAs) and Data Processing Agreements (DPAs) define roles, responsibilities, and liability caps between CSPs and cloud customers, but these instruments were designed for what

⁵² Luciano Floridi, "Establishing the Rules for the Digital Environment: Accountability and Transparency in AI Infrastructure," *Philosophy & Technology* 35, (2022).

⁵³ GDPR, Art. 4(7); NIS2 Directive, Art. 21.

⁵⁴ Christopher Millard, ed., *Cloud Computing Law*, 2nd ed. (Oxford: Oxford University Press, 2021), ch. 3 "Control and Responsibility in Cloud Service Provision.

⁵⁵ Jörn Gräber, "Smart Contracts and Dynamic Cloud Services: Legal Perspectives," *Computer Law & Security Review* 43, (2021).

⁵⁶ Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law* 7, no. 2 (2017).

⁵⁷ GDPR, Arts. 5 and 13–15.

⁵⁸ AI Act, Art. 13.

⁵⁹ European Commission, *Impact Assessment Accompanying the Proposal for the AI Act*, SWD(2021) 84 final, section 4.3. available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0084>.

⁶⁰ ENISA, *Artificial Intelligence Threat Landscape* (2022), section 5. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022?utm>.

are called “deterministic systems”.⁶¹ Where the performance metrics, fault conditions, and data flows are predictable and controllable by human operators. On the other hand, intelligent infrastructure, by contrast, could be described as “probabilistic and adaptive”. Its performance parameters shift dynamically based on data-driven learning processes.⁶² Consequently, a provider may find itself technically compliant with an SLA’s uptime guarantee even as the AI subsystem has autonomously reallocated resources causing data loss or service regression.⁶³ Thus, the contractual notion of breach becomes unclear when neither party can conclusively attribute the reason that caused damage.

The difficulty of attributing responsibility also undermines **risk allocation mechanisms**. Where classical contract law relies on foreseeability as parties allocate risks that they can identify and assess. Contrary to that, in intelligent infrastructures, many risks arise emergently discovered only after deployment, when AI systems interact in unanticipated ways.⁶⁴ Attempts to predefine liability through indemnities or warranties thus fail, as no party can fully predict the behavior of a self-learning system. The European Commission’s proposal for an *AI Liability Directive* acknowledges this difficulty by introducing a rebuttable presumption of the cause for claimants harmed by AI systems, effectively shifting the burden of proof.⁶⁵ Yet its scope remains limited to independent AI applications, not rooted in infrastructural systems.

The **allocation of accountability** is further complicated by the multi-jurisdictional nature of the cloud operations. Data and computational processes often navigate multiple EU and non-EU territories, invoking the extraterritorial reach of the GDPR (Article 3) and conflicting national cybersecurity requirements.⁶⁶ When an AI-based system autonomously transfers workloads between data centers in different jurisdictions, questions of applicable law and supervisory competence arise.⁶⁷ The European Data Protection Board has cautioned that effective enforcement in cloud ecosystems requires cross-border

⁶¹ Christopher Millard, ed., *Cloud Computing Law* (Oxford: Oxford University Press, 2021).

⁶² Angelis, A., et al. “An Overview on the Landscape of Self-Adaptive Cloud Computing: Patterns, Mechanisms and Challenges.” *Future Internet* 17, no. 10 (2025). Available at: <https://www.mdpi.com/1999-5903/17/10/434>.

⁶³ European Union Agency for Cybersecurity (ENISA), *Securing Machine Learning Algorithms* (Athens: ENISA, December 2021), <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>.

⁶⁴ European Commission, *Impact Assessment Accompanying the Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act)*, SWD (2021) 84 final, April 21 2021, p. 32–33. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0084>.

⁶⁵ Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), COM (2022) 496 final, Arts. 3–4. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>.

⁶⁶ GDPR, Art. 3.

⁶⁷ Ahmed Omar Youssef, “The Law Applicable to Cloud Computing,” *Arab Law Quarterly* 36, no. 4 (2022): 371–394.

cooperation mechanisms capable of addressing “functional fragmentation.”⁶⁸ However, existing enforcement structures remain oriented toward identifiable controllers and processors, not autonomous decision chains.

The **ethical side** of legal accountability also remains unresolved. The EU’s policy, as explained in the *Ethics Guidelines for Trustworthy AI*, promotes principles of human oversight, fairness, and explainability.⁶⁹ However, these principles are formulated at a level of abstraction that offers limited guidance for technical implementation in cloud systems. ENISA and the High-Level Expert Group on AI have both acknowledged that operationalizing these principles requires integrating accountability features into the design of cloud architectures, such as auditable logs, traceability modules, and algorithmic impact assessments.⁷⁰ While these mechanisms can support transparency, they depend on voluntary adoption and lack uniform legal enforceability.

Finally, the challenge of accountability in intelligent infrastructures reveals a deeper conceptual uncertainty within EU law between individual and systemic responsibility. Traditional liability regimes are based on actual actors seeking to identify a responsible subject and assign responsibility. Intelligent infrastructures, by contrast, function as *socio-technical assemblages* where responsibilities are distributed among algorithms, engineers, operators, and regulatory standards.⁷¹ Addressing accountability in such systems may therefore require shifting from a model of individual fault to one of *shared and procedural accountability*, emphasizing documentation, auditability, and governance.⁷² This shift aligns with emerging scholarship advocating for “networked accountability” in digital ecosystems where responsibility is reconstructed as a continuous process embedded in organizational and technical practices.⁷³

In the end, the legal challenges surrounding accountability in intelligent infrastructures expose the inadequacy of current regulatory and contractual frameworks. Attribution of responsibility is hindered by technological opacity, risk allocation failures in complicated environments, and systemic vulnerabilities that override individual liability. To reconcile technological autonomy with normative responsibility, EU law must evolve toward hybrid frameworks that integrate compliance-by-design, dynamic contracts, and continuous monitoring obligations bridging the gap between legal theory and the realities of intelligent infrastructure.

⁶⁸ EDPB, *Guidelines 07/2020 on the Concepts of Controller and Processor* (2020), section 26. Available at: https://www.edpb.europa.eu/system/files/en?file=2023-10%2FEDPB_guidelines_202007_controllerprocessor_final_en.pdf&utm.

⁶⁹ European Commission, *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on Artificial Intelligence (2019). Available at: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-en?utm>.

⁷⁰ ENISA, *AI Threat Landscape* (2022), section 6. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022?utm>.

⁷¹ Ahmed Omar Youssef, “The Law Applicable to Cloud Computing”.

⁷² Ahmed Omar Youssef, “The Law Applicable to Cloud Computing”.

⁷³ Thomas Schneider and Michael Veale, “Algorithmic Governance and the Allocation of Responsibility,” *Law and Contemporary Problems* 84 (2021).

5. Conclusion

This article contributes to the growing body of scholarship addressing accountability within AI-enabled cloud infrastructures by highlighting the structural tensions that emerge at the intersection of EU digital regulatory regimes. While it is accurate that the overlap between instruments such as the GDPR, the NIS2 Directive, the Cybersecurity Act, and the AI Act reveals both normative convergence and enforcement gaps, these challenges also point toward concrete avenues for regulatory and contractual improvement.

First, a recurring enforcement gap arises in the allocation of responsibility between cloud service providers and AI deployers in complex service chains. For example, in AI-driven cloud environments where automated resource allocation or security monitoring systems are embedded at the infrastructure layer, it remains unclear whether accountability for systemic failures should rest primarily with the cloud provider as infrastructure operator or with the AI developer as system controller. Addressing this ambiguity requires clearer guidance, either through regulatory interpretation or soft-law instruments on how shared controllership and joint responsibility should be assessed in AI-enabled cloud services.

Second, contractual mechanisms can be strengthened to operationalize regulatory obligations more effectively. Cloud service agreements and data processing agreements could incorporate dynamic compliance clauses, such as real-time audit rights, continuous risk assessment obligations, and automated incident-reporting triggers aligned with NIS2 obligations. Such clauses would move cloud contracts beyond static risk allocation toward adaptive governance instruments capable of responding to the evolving behavior of AI systems.

Third, certification and conformity assessment mechanisms under the Cybersecurity Act and the AI Act could be more closely aligned. For instance, EU-wide cybersecurity certification schemes for cloud services could be explicitly linked to AI risk classifications, allowing certified cloud infrastructures to serve as presumptive evidence of compliance for certain categories of high-risk AI systems. This would reduce regulatory fragmentation while incentivizing providers to embed security and accountability measures at the design stage.

Finally, regulators and supervisory authorities may benefit from enhanced coordination mechanisms, particularly where overlapping obligations trigger parallel enforcement under different legal regimes. Joint supervisory guidance or interoperable reporting frameworks could mitigate duplication and improve legal certainty for market actors operating across multiple compliance domains.

By grounding accountability in concrete technical, contractual, and institutional practices, the EU can move toward a more coherent governance model for intelligent cloud infrastructure, one that preserves innovation while ensuring transparency, resilience, and trust.