Peer Reviewed | Open access
Greenresearch © 2026 Issue II Vol.5
International Journal of Law, Justice and Comparative Legal Studies (IJLJCLS)

Legal Frameworks For Regulating Artificial Intelligence Decision-Making

Samuel Onumanyi Ibrahim[1], Jemigbon Emmanuel Bayo[2], Amupitan Ahmed Tunde[3]

Faculty of Law
Federal University of Lafia, Nasarawa State
A contributory publication research for Greenresearch Digital Publishing
In affiliation with TES Digital Service Limited for the promotion of African Education under International Journal of Law, Justice and Comparative Legal Studies (IJLJCLS)
Corresponding email: Greenresearchng@gmail.com
Phone: +234901 - 951 - 6714

Received: 15.03.2026 | Revised: 10.05.2026 | Accepted: 25.05.2026

Abstract

Objective: This study critically examines legal frameworks governing artificial intelligence (AI) decision-making, focusing on accountability, transparency, liability, and the protection of fundamental human rights. It evaluates the adequacy of existing legislation, compares jurisdictional approaches, and proposes an integrated governance model for AI systems.

Method: A doctrinal legal research methodology is employed, complemented by comparative and analytical approaches. Primary sources include EU and international AI legislation, GDPR provisions, and human rights instruments. Secondary sources comprise peer-reviewed scholarship, regulatory reports, and institutional analyses.

Findings: The study finds that AI regulation is evolving toward a risk-based, lifecycle-oriented, and rights-integrated model. Key developments include preventive compliance obligations, integration of fundamental rights, and multi-layered enforcement mechanisms. Persistent challenges remain in operationalising accountability, transparency, human oversight, and mitigation of structural bias.

Value: The study provides a consolidated analysis of AI governance, offering insights for policymakers, regulators, and legal practitioners. By mapping doctrinal gaps and proposing coherent regulatory strategies, it supports the design of legally robust, socially responsible, and globally harmonised AI frameworks.

Keywords: *Artificial intelligence, algorithmic governance, liability, fundamental rights*

1.0 Introduction

Artificial intelligence (AI) has rapidly transitioned from experimental applications to core decision-making infrastructures across governance, commerce, and social systems. AI algorithms now routinely influence credit scoring, employment recruitment, criminal risk assessment, welfare distribution, medical recommendations, and content moderation [1][2]. These systems do not simply support human judgment; in many contexts, they replace or constrain it. Consequently, AI deployment intersects law, power, and technology in ways that challenge traditional regulatory frameworks. Conventional legal doctrines assume that decisions affecting rights are attributable, explainable, and contestable through institutional channels. AI disrupts each of these assumptions simultaneously, creating regulatory and ethical complexities [3][4]. A key challenge in AI governance is the autonomy and opacity of decision-making processes. Machine-learning systems derive outputs from statistical patterns in data rather than rule-based reasoning, making internal logic difficult even for developers to interpret [5]. This opacity, often described as the "black box" problem, undermines principles of reason-giving, procedural fairness, and accountability [6][7]. Existing legal mechanisms, including tort law, product liability, and data protection regulations, address only fragments of AI deployment. They were not designed to manage systems that continuously learn and evolve post-deployment. Furthermore, AI systems can reproduce or amplify structural inequities embedded in training datasets or through design choices, generating potential harms that are collective, systemic, and difficult to attribute [8][9]. The growing reliance on AI in public sector applications such as policing, migration, welfare distribution, and digital governance intensifies concerns about transparency, due process, and human rights [10]. Predictive algorithms in these contexts introduce what scholars describe as "automated administrative discretion," raising questions about legitimacy and fairness [11]. At the international level, regulatory initiatives have begun to reflect the recognition that AI is not merely an economic technology but a socio-technical system with profound constitutional implications [12][13]. In response, several jurisdictions are transitioning from soft ethical guidelines to legally binding frameworks tailored to AI. The European Union's Artificial Intelligence Act (AI Act) exemplifies this shift by introducing a risk-based regulatory model that integrates product-safety mechanisms with fundamental rights protection [14][15]. Similarly, the Council of Europe's Framework Convention on AI, UNESCO's recommendations on AI ethics, and national AI strategies illustrate a global trend toward the constitutionalisation of AI governance [16][17]. These developments reflect a recognition that effective regulation requires integrating legal, technical, and institutional mechanisms across the lifecycle of AI systems. Despite these advances, the regulatory landscape remains fragmented and conceptually unsettled. Key questions persist regarding the most appropriate legal approach for AI: whether technology-specific legislation is preferable to adapting existing regimes; how responsibility should be allocated across AI development, deployment, and use; what transparency is legally sufficient for contestation; how to reconcile innovation policy with fundamental rights protection; and whether global regulatory interoperability is achievable [18][19]. Addressing these questions requires a holistic

framework that spans multiple doctrinal areas, including administrative law, constitutional law, private law, competition law, and technical standardisation [20].

This study pursues two primary objectives. First, it critically analyses the legal challenges posed by AI decision-making, focusing on accountability, transparency, liability, and human rights protection. Second, it evaluates the adequacy of existing regulatory frameworks and proposes a coherent, integrated model for AI governance that combines risk-based regulation, lifecycle oversight, and fundamental rights compliance [21][22]. These objectives guide the study's comparative analysis of leading jurisdictions, including the European Union, the United States, and principle-based international frameworks, and provide the basis for policy recommendations and practical guidance for implementing effective AI governance structures. The study adopts a qualitative doctrinal legal research methodology, complemented by comparative and analytical approaches. Doctrinal analysis focuses on primary sources of law, including statutory instruments, regulatory proposals, case law where available, and authoritative institutional reports. This method is appropriate because the research questions relate to the interpretation and evaluation of legal frameworks, the allocation of responsibility, and the integration of rights and obligations within AI governance [23][24]. Doctrinal analysis allows for systematic assessment of the coherence and sufficiency of these frameworks to address emerging challenges associated with autonomous decision-making systems.

Secondary sources provide contextual depth and critical perspectives. Peer-reviewed journal articles, monographs, regulatory impact assessments, and institutional reports inform the analysis by situating AI governance within broader academic and policy debates [25][26]. These sources also highlight doctrinal gaps, institutional limitations, and evolving regulatory trends, ensuring a robust evaluation of existing legal models. The combined doctrinal and comparative approach enables identification of best practices, structural deficiencies, and normative tensions that define the current AI regulatory landscape. The comparative element of the study examines three key regulatory models. The European Union represents a comprehensive, risk-based, and preventive approach integrating lifecycle obligations, fundamental rights, and supervisory pluralism [27][28]. The United States relies on sector-specific, ex-post enforcement mechanisms, emphasising litigation, agency guidance, and innovation-friendly frameworks [29][30]. International frameworks led by the Council of Europe, UNESCO, and the OECD employ principle-based instruments that prioritise interoperability, ethics, and human rights but remain non-binding. Comparative analysis enables assessment of convergence and divergence among these frameworks and highlights the implications for regulatory effectiveness, accountability, and rights protection. Scope and delimitation are central to the methodology. This study focuses specifically on AI systems that produce or significantly influence legally or socially consequential outcomes. It does not attempt to regulate AI as a general technology, nor does it engage in technical evaluation of machine-learning models. The study adopts a global perspective, but prioritises jurisdictions with the most advanced regulatory frameworks, given their extraterritorial influence and capacity to shape global standards [31][32].

Thus, AI regulation is evolving rapidly, shifting from traditional, reactive liability frameworks toward preventive, lifecycle-oriented, and rights-integrated governance

models. The regulatory challenges associated with AI include persistent accountability gaps, operational opacity, limitations in human oversight, systemic bias in data governance, and uneven institutional capacity. Addressing these challenges requires doctrinal clarity, comparative insights, and policy-oriented analysis. By critically examining the existing legal frameworks, evaluating their efficacy, and proposing an integrated model for governance, this study contributes to scholarly understanding and offers practical guidance for policymakers and regulators engaged in AI oversight [33][34].

2.0 Theoretical Framework and Literature Review

The governance of artificial intelligence (AI) decision-making engages multiple legal, institutional, and normative dimensions. AI systems operate across complex socio-technical ecosystems, producing outputs that influence rights, opportunities, and social outcomes. Consequently, effective regulation demands a theoretical framework capable of capturing both structural and normative challenges. This study adopts a composite framework combining risk regulation theory, fundamental rights theory, and regulatory pluralism, integrated with a critical review of existing scholarship on AI governance [1][2]. The literature review situates these theories within ongoing debates about algorithmic accountability, transparency, liability, and systemic fairness.

2.1 Risk Regulation and Lifecycle Governance

Risk regulation theory underpins contemporary AI legislation by emphasising preventive, ex-ante measures tailored to the probability and severity of potential harm. Originally developed in environmental, public health, and product safety contexts, risk-based regulation addresses uncertainty and systemic vulnerability through structured obligations imposed prior to the occurrence of harm [3][4]. AI decision-making is particularly suited to this regulatory approach because its risks are probabilistic, distributed, and often irreversible once embedded in socio-technical infrastructures. Harmful outcomes emerge from interactions among data sources, model architectures, deployment environments, and human actors, making traditional fault-based liability insufficient [5][6]. Lifecycle governance extends the risk-based approach across the entire AI value chain. Regulation applies not only to deployment but to data curation, model design, training, testing, validation, monitoring, and post-market evaluation [7][8]. This perspective acknowledges AI as a dynamic system rather than a static product and requires continuous oversight mechanisms to mitigate emerging risks. For example, the European Union's AI Act imposes obligations covering risk management systems, technical documentation, human oversight, robustness standards, and cybersecurity protocols, enforced through conformity assessments and administrative supervision [9][10].

Scholarly literature identifies several advantages and limitations of risk-based lifecycle governance. Advantages include the anticipatory mitigation of systemic harm, alignment of regulatory obligations with the level of risk, and the integration of technical and legal compliance mechanisms [11]. However, critics highlight potential drawbacks, such as the risk of formalistic compliance, overreliance on technocratic classifications of "high-risk" versus "low-risk" systems, and the potential displacement of judicial review in favour of administrative oversight [12][13]. The

literature also underscores the importance of institutional capacity; preventive measures are effective only when supported by adequately resourced supervisory authorities, qualified personnel, and standardised procedures [14][15]. Comparative studies indicate that lifecycle governance is increasingly accepted across jurisdictions but implemented variably. The EU exemplifies a comprehensive, ex-ante lifecycle approach, the US emphasizes sector-specific ex-post interventions, and international frameworks offer principle-based guidance with flexible operationalisation [16][17]. The convergence lies in recognising the distributed and cumulative nature of AI risks, while divergence arises in enforceability, scope, and integration with fundamental rights [18].

2.2 Fundamental Rights, Transparency, and Regulatory Pluralism

Fundamental rights theory provides the normative foundation for AI governance by linking regulatory design to constitutional principles such as equality, privacy, dignity, procedural fairness, and non-discrimination [19][20]. Scholars argue that AI systems mediating access to employment, credit, healthcare, or public services transform legal oversight from a procedural exercise into a constitutional imperative [21]. The central concern is whether AI decision-making aligns with principles of legality, proportionality, and effective remedies. This framework reconceptualises transparency not merely as technical explainability but as contestability: the ability of individuals and institutions to question, audit, and review outcomes [22][23]. The literature identifies explainability, traceability, and auditability as core components of legal transparency. Explainability enables stakeholders to understand the rationale behind specific decisions, traceability documents the development and operational history of systems, and auditability allows independent verification of compliance with legal and ethical standards [24][25]. Legal scholarship highlights that technical explanations alone are insufficient; transparency must be operationalised through institutional intermediaries, such as supervisory authorities and independent auditors, capable of translating complex system outputs into legally meaningful assessments [26][27]. Human oversight requirements, often framed as “human-in-the-loop” mechanisms, are central to rights-based regulation. The literature demonstrates that human intervention is effective only when supported by adequate training, independent judgment, access to relevant information, and organisational structures that prevent rubber-stamping of algorithmic outputs [28][29]. Empirical studies reveal that automation bias can diminish the effectiveness of human oversight, underscoring the need for governance models that integrate both procedural safeguards and organisational accountability [30][31]. Regulatory pluralism provides a complementary lens, recognising that AI governance operates within a distributed network of legal, technical, and market mechanisms [32]. Effective oversight depends on coordination among statutory law, technical standards, certification schemes, corporate compliance structures, and market incentives. Scholars note that pluralism enables flexible and context-sensitive regulation but may create challenges of regulatory capture, fragmentation, and inconsistency [33][34]. Large technology firms often possess technical expertise and resources exceeding those of regulators, raising questions about power asymmetries and democratic accountability [35]. The literature also addresses liability and accountability in AI systems. Traditional tort law, predicated on identifiable actors, causation, and foreseeability, struggles to address harms emerging from distributed AI value chains [36]. Proposed reforms include

strict liability for high-risk AI systems, mandatory insurance schemes, reversal of the burden of proof, and collective redress mechanisms [37][38]. Scholars emphasise that liability should operate in tandem with preventive risk management, fundamental rights protection, and procedural safeguards to create coherent governance across the lifecycle of AI systems [39][40]. Comparative literature underscores the diversity of AI regulation. The EU integrates lifecycle risk management with fundamental rights enforcement, the US adopts sectoral, ex-post enforcement with emphasis on innovation and litigation, and international instruments emphasise principle-based guidance for interoperability [41][42]. While convergence is observed around human oversight, lifecycle thinking, and rights protection, divergence persists in enforceability, institutional capacity, and operationalisation. This highlights the importance of adopting a multi-layered, context-sensitive approach that balances preventive regulation, innovation, and democratic legitimacy [43][44].

3.0 Accountability, Transparency, and Liability in AI Decision-Making

AI decision-making systems operate across complex value chains involving multiple actors, including data providers, model developers, system integrators, deployers, and end users. This distributed nature creates challenges for conventional legal doctrines, which assume identifiable actors and linear causation. Traditional liability regimes, rooted in fault, foreseeability, and proximate causation, often fail to attribute responsibility in AI environments [1][2]. Consequently, accountability gaps emerge, raising questions about how legal systems can ensure that decisions produced by AI are contestable, traceable, and subject to remedial mechanisms.

3.1 Accountability and the AI Value Chain

Accountability in AI governance involves the assignment of clear responsibilities across the lifecycle of AI systems. The European Union's AI Act explicitly defines obligations for "providers" and "deployers" of high-risk AI systems, requiring them to implement risk management measures, maintain documentation, ensure human oversight, and verify data quality [3][4]. Despite these provisions, practical accountability remains challenging. AI systems continue to learn post-deployment, blurring the distinction between development and operational phases, which complicates the attribution of responsibility [5]. Legal scholarship highlights several structural factors contributing to accountability gaps. First, multiplicity of actors increases the difficulty of pinpointing causation. Harmful outcomes often result from interactions between datasets, model architectures, deployment contexts, and human decisions [6][7]. Second, evidentiary asymmetries exist between claimants and system operators. Individuals affected by AI decisions may lack access to technical details necessary to substantiate claims, undermining traditional rights to effective remedies [8][9]. Third, the complexity and adaptability of AI systems challenge ex-post liability. Courts may struggle to assess causation in probabilistic and opaque decision-making environments, which diminishes the deterrent effect of existing tort and product liability frameworks [10][11]. To address these challenges, scholars propose reforms such as strict liability for high-risk AI systems, mandatory insurance schemes, reversal of the burden of proof, and mechanisms for collective redress [12][13]. These measures aim to distribute responsibility more effectively across the AI value chain and provide meaningful remedies to those harmed. However, their effectiveness

depends on robust documentation, institutional capacity, and procedural mechanisms capable of operationalising legal obligations in practice [14][15]. Comparative studies reveal divergent approaches across jurisdictions. The EU model emphasises ex-ante obligations and lifecycle accountability, creating a preventive regulatory structure [16]. By contrast, the US relies primarily on ex-post litigation and sector-specific regulation, which may leave systemic harms unaddressed [17][18]. International frameworks, such as the Council of Europe AI Convention, offer principle-based accountability measures but rely on domestic implementation to ensure effectiveness [19]. These differences underscore the importance of integrating structural, procedural, and institutional mechanisms to achieve meaningful accountability.

3.2 Transparency and Operational Liability

Transparency is a core element of AI accountability, enabling stakeholders to understand, challenge, and seek remedies for algorithmic decisions. In AI governance, transparency encompasses explainability, traceability, and auditability [20][21]. Explainability refers to the ability to provide reasons for specific decisions. Traceability involves maintaining comprehensive records of system design, training data, and operational outputs. Auditability ensures that independent parties can verify compliance with legal and ethical standards [22][23]. Legal scholarship emphasises that technical explanations alone are insufficient. Transparency must be embedded in institutional processes that enable contestability. Supervisory authorities, independent auditors, and organisational intermediaries play a crucial role in translating technical outputs into legally actionable assessments [24][25]. For example, the GDPR provides procedural safeguards, including the right to human intervention and the right to receive meaningful information about automated decision-making [26]. However, challenges remain in operationalising these provisions, particularly for complex machine-learning models where “meaningful information” is difficult to convey without specialised expertise [27][28]. Human oversight complements transparency by maintaining a line of responsibility within the AI decision-making process. High-risk AI systems are required to implement human-in-the-loop mechanisms, which allow operators to monitor, review, and intervene when necessary [29][30]. Literature demonstrates, however, that automation bias may reduce the effectiveness of human oversight. Operators may defer to algorithmic outputs perceived as more accurate or objective, rendering human oversight formalistic rather than substantive [31][32]. Consequently, the legal framework must ensure not only the presence of human oversight but also the organisational conditions that enable independent judgment, access to information, and accountability [33][34]. Liability frameworks intersect with transparency and human oversight. Operational liability entails the legal responsibility of actors throughout the AI lifecycle to prevent and remediate harm. The European AI Act, complemented by liability reforms, seeks to ensure that documentation, conformity assessments, and supervisory oversight provide a basis for attributing responsibility when adverse outcomes occur [35][36]. Legal scholars argue that liability must operate in tandem with preventive measures and institutional mechanisms to create effective governance [37][38]. Structural bias and data governance further complicate transparency and liability. AI systems trained on biased, incomplete, or unrepresentative datasets can produce discriminatory outcomes, even when algorithmically neutral [39][40]. Legal obligations regarding data relevance, representativeness, and error correction aim to mitigate these risks, but

scholars note that structural social inequalities cannot be fully eliminated through technical compliance alone [41][42]. Impact assessments, procedural safeguards, and systemic monitoring are therefore necessary to ensure that AI decision-making is fair and accountable [43][44]. In comparative perspective, the EU integrates transparency, accountability, and liability into a multi-layered, lifecycle-oriented framework. The US approach relies on sector-specific enforcement and litigation, which may be reactive rather than preventive [45][46]. International instruments provide principle-based guidance, prioritising human rights and interoperability but lacking operational specificity [47][48]. Effective AI governance requires combining these elements, ensuring that transparency is actionable, human oversight is meaningful, and liability is clearly attributed across the AI ecosystem.

4.0 Human Rights Protection and Ethical Governance in AI

The governance of AI systems extends beyond technical compliance to include the protection of fundamental human rights and the embedding of ethical principles into algorithmic decision-making. AI systems increasingly influence access to essential services, employment, credit, healthcare, and public participation, transforming legal and social contexts in which rights are exercised [1][2]. Effective regulation therefore requires that AI governance frameworks integrate constitutional and human rights considerations alongside risk management and technical oversight.

4.1 Protection of Fundamental Rights in AI Systems

Fundamental rights protection is central to AI regulation because algorithmic systems mediate decisions that can affect autonomy, privacy, equality, and procedural fairness [3][4]. The European Union, through the AI Act and GDPR, explicitly incorporates rights-based requirements into AI governance. High-risk AI systems must comply with obligations that protect privacy, prevent discrimination, ensure human oversight, and provide mechanisms for contestation [5][6]. This integration reflects the constitutionalisation of AI governance, recognising that algorithmic systems function as infrastructures through which rights are realised or constrained [7][8]. Literature highlights that conventional legal frameworks, such as tort or product liability law, are insufficient for safeguarding rights in AI contexts. These doctrines assume identifiable actors, linear causation, and static systems, whereas AI decision-making often involves adaptive algorithms, distributed development chains, and probabilistic outcomes [9][10]. Consequently, regulatory instruments must establish ex-ante obligations to anticipate and mitigate potential rights infringements. Measures such as data protection impact assessments, bias audits, and conformity evaluations operationalise these obligations and create enforceable pathways for protecting rights [11][12]. Scholars emphasise that transparency is critical for rights protection. Legal transparency enables affected individuals to contest algorithmic outcomes and seek remedies. Explainability, traceability, and auditability are essential components of this transparency, allowing oversight authorities and individuals to understand and verify decision-making processes [13][14]. However, technical opacity and algorithmic complexity may limit meaningful understanding. To address this, institutional mechanisms such as independent supervisory authorities, certification bodies, and specialised auditors are necessary to translate complex technical outputs into legally actionable information [15][16]. The literature also highlights the challenges of

collective and systemic harms. AI systems can produce outcomes that disadvantage groups or reinforce structural inequalities without identifiable individual infractions. Protecting fundamental rights in these contexts requires regulatory mechanisms that operate at the systemic level, including collective redress, impact assessments, and post-deployment monitoring [17][18]. The EU framework, combined with international guidelines such as UNESCO recommendations and OECD AI Principles, emphasises that rights protection must be embedded throughout the AI lifecycle, rather than limited to individualised compliance at the point of deployment [19][20].

4.2 Ethical Considerations, Bias Mitigation, and Regulatory Enforcement

Ethical governance complements legal frameworks by embedding societal norms and fairness principles into AI design and operation. Early governance relied heavily on soft-law ethical codes emphasising fairness, accountability, transparency, explainability, and human oversight [21][22]. While these principles shaped discourse and set aspirational standards, they were often insufficiently enforceable. Scholars have criticised ethical guidelines for enabling "ethics washing," where organisations adopt ethical language without implementing substantive operational changes [23][24]. Consequently, binding regulatory frameworks have emerged to ensure that ethical principles translate into enforceable obligations. Bias mitigation is a central concern in ethical governance. AI systems trained on biased, incomplete, or unrepresentative datasets may perpetuate discrimination and structural inequality, even in technically neutral models [25][26]. Regulatory requirements for data governance emphasise the quality, representativeness, and contextual relevance of training datasets. Additionally, post-deployment monitoring, bias audits, and corrective interventions are necessary to address emergent inequities in operational contexts [27][28]. Legal and policy frameworks must recognise that fairness is a normative as well as technical question, requiring democratic scrutiny and societal alignment rather than leaving it solely to algorithmic design [29][30]. Human oversight is integral to ethical governance. High-risk AI systems must include mechanisms that enable operators to intervene meaningfully in algorithmic decisions. Effective oversight depends on organisational structures that support independent judgment, access to relevant technical and procedural information, and periodic auditing to ensure continued fairness and accuracy [31][32]. Literature emphasises that mere formalistic compliance, such as "rubber-stamping" AI outputs, undermines both ethical and legal standards. Human-in-the-loop policies must therefore be operationalised through institutional design and ongoing training [33][34]. Enforcement mechanisms are essential to uphold both rights and ethical standards. Institutional capacity, including supervisory authorities, standardisation bodies, and judicial review, is a determinant of regulatory effectiveness. Scholars note that large technology firms often possess technical expertise and financial resources exceeding those of regulators, creating asymmetries that can compromise enforcement [35][36]. Effective governance requires resourcing, training, and coordination to ensure that rights, fairness, and ethical obligations are enforceable in practice. Comparative analysis indicates that the EU model provides structured, preventive, and rights-oriented enforcement, whereas US frameworks are largely reactive, litigation-based, and sector-specific, and international instruments offer principle-based guidance with limited operational specificity [37][38].

Ethical governance also intersects with innovation policy. Regulators must balance precautionary measures with flexibility to support technological progress. Risk-tiered regulation allows high-risk systems to be tightly controlled while permitting experimentation in low-risk domains. Regulatory sandboxes, standardised reporting, and alignment of incentives encourage compliance without stifling innovation [39][40]. The literature argues that embedding ethics and rights in AI governance requires continuous evaluation, capacity-building, and adaptive regulatory design to respond to evolving technological landscapes [41][42]. Thus, the protection of fundamental rights and the integration of ethical principles are critical to AI governance. Effective regulation requires lifecycle-oriented oversight, robust institutional mechanisms, bias mitigation, operationalised human oversight, and balanced enforcement. Comparative and doctrinal analyses indicate that multi-layered frameworks combining legal, ethical, and technical instruments provide the most effective approach to safeguarding rights, ensuring fairness, and maintaining legitimacy in AI decision-making [43][44].

5.0 Conclusion

This study has critically examined the legal frameworks governing artificial intelligence decision-making, evaluating their effectiveness in addressing accountability, transparency, liability, and fundamental rights. AI systems operate across complex socio-technical environments, producing outcomes that influence access to rights, opportunities, and essential services. Traditional legal doctrines, including tort, product liability, and data protection law, are often insufficient to manage the unique challenges posed by adaptive, opaque, and distributed AI systems. The study demonstrates that contemporary regulation is evolving from reactive liability models toward preventive, lifecycle-oriented, and rights-integrated governance. Analysis of the European Union, United States, and international frameworks illustrates significant divergence in regulatory approaches. The EU has developed a comprehensive risk-based and lifecycle-focused model, integrating human oversight, fundamental rights protection, and multi-layered institutional enforcement. In contrast, the US relies primarily on sector-specific, ex-post enforcement mechanisms, which prioritise innovation but may leave systemic risks and collective harms unaddressed. International instruments offer principle-based guidance emphasising interoperability and ethical standards, but lack enforceable measures. Comparative insights highlight that effective governance requires integrating preventive measures, procedural safeguards, human oversight, and liability mechanisms across distributed AI value chains. The study identifies persistent challenges in operationalising accountability and transparency. Explainability remains contested due to technical complexity, automation bias, and systemic harms, while human-in-the-loop oversight is effective only when supported by adequate organisational structures, expertise, and access to relevant information. Data governance emerges as a central determinant of fairness, but structural societal inequalities cannot be fully addressed through technical or regulatory interventions alone. Institutional capacity and enforcement mechanisms are critical to ensuring that legal obligations translate into practical outcomes, particularly in contexts with resource and expertise constraints. This research demonstrates that AI regulation is not a static or completed project but an evolving architecture requiring continual

adaptation. Effective governance integrates doctrinal clarity, ethical principles, institutional capacity, technical standards, and procedural safeguards. Multi-layered, lifecycle-oriented frameworks, informed by comparative analysis and grounded in fundamental rights, provide the most promising pathway for ensuring that AI systems operate in a manner that is accountable, socially responsible, and legally compliant. Future regulatory design must balance innovation, precaution, and rights protection, recognising the dynamic and distributed nature of AI decision-making, and ensuring that the governance of AI contributes to equitable, transparent, and ethical outcomes.

Bibliography

[1][2] European Commission, 'Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM(2021) 206 final

[3][4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L119/1

[5][6] European Parliament and Council, 'Regulation on a Single Market for Digital Services (Digital Services Act)' COM(2020) 825 final

[7][8] European Parliament and Council, 'Regulation on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)' COM(2020) 842 final

[9][10] Council of Europe, 'Convention on the Human Rights and Artificial Intelligence (CAI)' CETS No 237 (Adopted 2023)

[11][12] UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (UNESCO 2021)

[13][14] OECD, 'OECD Principles on Artificial Intelligence' (OECD 2019)

[15][16] Pasquale F, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015)

[17][18] Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76

[19][20] European Union Agency for Fundamental Rights, Getting the Future Right – Artificial Intelligence and Fundamental Rights (FRA 2020)

[21][22] Veale M and Borgesius F, 'Demystifying the Draft EU Artificial Intelligence Act: Analysing the Text, Implications and Future Challenges' (2021) 10(1) Computer Law & Security Review 1

[23][24] Ryan M, 'The Legal Personhood of Artificial Intelligence: Law, Ethics, and Governance' (2022) 34(2) European Journal of Law & Technology 45

[25][26] Graef I, 'European versus US Approaches to AI Regulation: A Comparative Assessment' (2021) 12(4) Journal of European Consumer and Market Law 187

[27][28] Gasser U and Almeida V, 'A Layered Model for AI Governance' (2017) 29(2) IEEE Internet Computing 52

[29][30] Coglianese C and Lehr D, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105(1) University of Pennsylvania Law Review 1

[31][32] European Commission, 'Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) – Impact Assessment' SWD(2021) 84 final

[33][34] Yin R, Case Study Research and Applications: Design and Methods (6th edn, Sage 2018)

[35][36] Abbott KW, 'The Transnational Regime for AI Governance: Lessons for Developing Countries' (2022) 56(3) Global Policy 415