https://doi.org/10.38044/2686-9136-2025-6-17

ARTICLES

ARTIFICIAL INTELLIGENCE AND LIABILITY: EXPLORING LEGAL CHALLENGES AND RESPONSIBILITY IN AI DECISION-MAKING AND AUTONOMOUS SYSTEMS

Kolawole O. Afuwape

O.P. Jindal Global University
Sonipat Narela Road, Jagdishpur Village, Sonipat, India, 131001

Abstract

The rapid integration of artificial intelligence (AI) across a wide range of economic sectors, including transportation, healthcare, and finance, has significantly transformed decision-making processes and operational efficiency. At the same time, increasing reliance on AI has generated new legal challenges, particularly with respect to accountability and sanctions. Central issues include decisional responsibility, algorithmic transparency, and data regulation, especially in relation to bias. Traditional legal frameworks, which were developed to govern human conduct, are poorly equipped to address the self-learning capabilities, unpredictability, and opacity of AI systems. This paper examines the emerging concept of shared responsibility within multi-stakeholder AI ecosystems, in which liability may extend across developers, manufacturers, operators, and users. It analyzes product liability principles and the allocation of accountability in cases where AI systems cause harm. Particular emphasis is placed on the need to adapt legal frameworks to keep pace with the rapid evolution of AI technologies, ensuring flexibility, resilience, and alignment with international legal standards. The European Union's AI Act is examined as a case study illustrating efforts to address accountability gaps while promoting ethical guidelines to strengthen public trust. Through the use of case studies and hypothetical scenarios, this paper highlights the importance of transparency and fairness in managing the legal implications of AI. Finally, it advocates for closer collaboration between computer science and law to bridge gaps in AI literacy, product development, and regulation. By addressing contemporary challenges and proposing legal responses, this paper offers a coherent framework for managing liability in the age of artificial intelligence.

Keywords

artificial intelligence, autonomous systems, accountability, transparency, explainable AI, XAI, algorithmic bias, ethical AI, product liability, shared responsibility

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study has no sponsorship.

For citation Afuwape, K. O. (2025). Artificial intelligence and liability: Exploring legal challenges and responsibility in AI decision-making and autonomous systems. *Digital Law Journal, 6*(4), 82–100. https://doi.org/10.38044/2686-9136-2025-6-17

Submitted: 28 Jun. 2025, accepted: 16 Nov. 2025, published: 30 Dec. 2025

СТАТЬИ

ОТВЕТСТВЕННОСТЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРАВОВЫЕ ВЫЗОВЫ В ПРОЦЕССЕ ПРИНЯТИЯ РЕШЕНИЙ С ПОМОЩЬЮ ИИ И АВТОНОМНЫХ СИСТЕМ

К. О. Афувапе

Глобальный университет им. О. П. Джиндала
131001, Индия, Сонипат, п. Джагдишпур, ш. Сонипат Нарела

Аннотация

Быстрая интеграция искусственного интеллекта (ИИ) в широкий спектр секторов экономики, включая транспорт, здравоохранение и финансы, значительно изменила процессы принятия решений и операционную эффективность. В то же время растущая зависимость от ИИ породила новые правовые проблемы, особенно в отношении ответственности. К центральным вопросам относятся ответственность за принятие решений, прозрачность алгоритмов и регулирование данных, особенно в связи с предвзятостью. Традиционные правовые рамки, разработанные для регулирования поведения людей, плохо приспособлены для решения проблем, связанных с самообучающимися способностями, непредсказуемостью и непрозрачностью систем ИИ. В данной статье рассматривается новая концепция совместной ответственности в многосторонних экосистемах ИИ, в которых ответственность может распространяться на разработчиков, производителей, операторов и пользователей. Анализируются принципы ответственности за качество продукции и распределение ответственности в случаях, когда системы ИИ причиняют вред. Особое внимание уделяется необходимости адаптации правовых рамок к быстрому развитию технологий ИИ, обеспечению гибкости, устойчивости и соответствия международным правовым стандартам. Закон Европейского союза об ИИ рассматривается в качестве примера, иллюстрирующего усилия по устранению пробелов в ответственности при одновременном продвижении этических принципов для укрепления доверия общественности. С помощью конкретных примеров и гипотетических сценариев в данной статье подчеркивается важность прозрачности и справедливости в правовом регулировании ИИ. В заключение статья выступает за более тесное сотрудничество между компьютерными науками и правом с целью устранения пробелов в знаниях об ИИ, разработке продуктов и регулировании. Рассматривая современные вызовы и предлагая правовые решения, данная статья предлагает последовательную структуру для регулирования ответственности в эпоху искусственного интеллекта.

Ключевые слова

искусственный интеллект, автономные системы, подотчетность, прозрачность, объяснимый ИИ, алгоритмическая предвзятость, этический ИИ, ответственность за качество продукции, совместная ответственность

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Афувапе, К. О. (2025). Ответственность искусственного интеллекта: правовые вызовы в процессе принятия решений с помощью ИИ и автономных систем. *Цифровое право, 6*(4), 82–100. https://doi.org/10.38044/2686-9136-2025-6-17

Поступила: 28.06.2025, принята в печать: 16.11.2025, опубликована: 30.12.2025

Introduction—Overview of AI

Artificial intelligence (AI) possesses characteristics that emulate human intelligence through numerical and computational systems (Zhang & Lu, 2021). These systems are capable of forming representations, learning from data, making predictions, conducting analyses, drawing conclusions, and, in some cases, applying self-corrections. AI is designed to address a wide range of tasks, including medical prediction, planning, image visualization, voice recognition, and the acquisition of specific skills. AI systems rely on training datasets to improve predictive accuracy and to assist in solving complex problems with a high degree of precision (Kumar et al., 2023, pp. 8459–8486).

To a certain extent, AI may be understood as a scientific field concerned with the learning capabilities of intelligent machines, primarily intelligent computer programs, which generate outcomes in a manner comparable to human cognitive and attentional processes (Khaleel et al., 2024, pp. 1–21). As a rule, AI involves sequential processes of data accumulation, the creation of effective structures for utilizing acquired data, the production of definite or approximate outcomes, self-evaluation, and subsequent adjustment. Overall, AI is used to assess and advance machine-learning techniques that aim to replicate aspects of human cognition (Dong et al., 2020, pp. 1–10). AI technologies are increasingly employed to perform more accurate analyses and to generate practical and economic value. From this perspective, a range of statistical models, along with computational intelligence methods, are integrated into AI systems.

AI has seen remarkable and rapid development over the past two decades. Its subdomains—such as machine learning (ML), natural language processing (NLP), and computer vision—are progressively converging and expanding across numerous sectors of society. Artificial intelligence is increasingly embedded in human activities and, in certain contexts, is replacing human decision-making processes (Chukwuani et al., 2020, pp. 444–449). Although AI originates within computer science, it is closely connected to many other disciplines, including mathematics, cognitive science and philosophy, biology, business and logistics, engineering and manufacturing, transportation, healthcare, education, and government (Adnan et al., 2024).

The deployment of AI has enhanced productivity while reducing costs, and its effects contribute to economic development, social transformation, and individual welfare (Adigwe et al., 2024,

pp. 126–146). AI aims to create digital computers or computer-operated robots capable of performing intellectual and cognitive tasks typically associated with humans, without external assistance (Markauskaite et al., 2022). These cognitive functions include acquiring knowledge, reasoning, problem-solving, perception and comprehension, and speech. A foundational aspect of AI is knowledge engineering, whereby machines are constructed using data and information about the human world so that they can act in human-like ways (McCarthy, 2022, pp. 66–90). Another major branch of AI is machine learning, in which predefined algorithms and statistical models are used to minimize or converge errors without explicit, task-specific programming (Telikani, 2021, pp. 1–35). This approach is based on the premise that machines can learn from data, identify problems, and determine solutions with minimal human intervention.

This paper offers specific recommendations to support the argument that data protection and privacy laws are essential for improving the transparency and accountability of AI systems. Nevertheless, significant issues, debates, and ongoing controversies surround the practical implementation of these rights, particularly regarding the extent to which they can be enforced and the manner of their enforcement. Moreover, current data protection laws exhibit notable limitations in their coverage of, and applicability to, AI systems. In particular, this paper demonstrates how de-identification techniques intended to circumvent legal obligations by removing personal identifiers are undermined by AI technologies, which are capable of directly re-identifying data or indirectly inferring sensitive attributes from datasets that have been anonymized.

Results

The findings indicate that the autonomous actions of AI systems cannot be adequately regulated through traditional legal frameworks that are grounded in human agency. Such autonomous action requires distinct and domain-specific regulatory consideration, particularly in sectors such as healthcare, transportation, and finance. This paper highlights the potential problem of overlapping and shared interests among AI developers, users, and manufacturers. To address these challenges, it proposes a hybrid model of liability that combines elements of strict liability with algorithmic transparency requirements. The paper concludes that global accountability is central to necessary legal reforms and suggests that, without such reforms, society will be reluctant to rely on AI technologies or to adopt them at a rapid pace.

Role of AI in Autonomous Systems and Decision-Making

Autonomous Decision-Making Systems (ADMS) are advanced computing systems capable of receiving and responding to information in both digital and physical forms, and of generating outputs that may either support or substitute human decision-making processes (Dwivedi et al., 2023). ADMS can be defined as processes that, with or without the use of AI techniques, take inputs and data received or collected from the environment and, based on predefined objectives, produce a wide range of outputs.[1]

Autonomous AI represents a subcategory of artificial intelligence in which systems and tools have developed to the point where they can operate largely independently of human input (Atakishiyev et al., 2024, pp. 51182–51221). The actions performed by autonomous AI systems range from relatively simple operations to complex data analysis tasks (Bathla et al., 2022). In this respect, autonomous AI

[1] Anderson, A., Vadari, S., Wall, L., Sharma, P., & Reiman, A. (2023). *Distributed rules-based deconfliction of ADMS applications: Part 2: Conceptual implementation.* Pacific Northwest National Laboratory. https://doi.org/10.2172/1996255

brings real-world AI systems closer to the portrayals commonly found in fictional representations of artificial intelligence (Lucci et al., 2022, p. 850).

When effectively implemented, AI systems composed of multiple interacting components can significantly enhance the operational capacity of businesses and other organizations (Dalsaniya & Patel, 2022, pp. 322–337). Some components are software-based and provide specific functionalities, such as algorithms that analyze collected data, while other components are embedded within systems to capture data from the environment and supply it to analytical processes. The term "AI" may apply to systems that still require continuous human intervention,[2] as well as to more advanced architectures—such as reinforcement learning, machine learning, and deep learning platforms—that are capable of processing and correlating large datasets with limited human involvement (ZainEldin et al., 2024).

Self-governing or autonomous AI represents one of the most advanced forms of contemporary AI. However, since many AI applications widely used today are not fully self-sufficient, they are commonly described as narrow AI (Perwej et al., 2024, pp. 1–32). Narrow AI refers to systems designed to perform specific tasks that generally require human oversight or guidance (Hopgood, 2021, p. 514). In contrast, artificial general intelligence (AGI) refers to a hypothetical or fictional concept in which AI systems are fully autonomous, capable of operating independently of any human operator, and able to outperform human intelligence across all domains (Mikki, 2024).

Current AI systems, including those described as autonomous, do not yet meet the criteria of AGI. Rather, autonomous AI constitutes an intermediate stage in the progression toward that theoretical goal. While such systems may rely on equipment and infrastructures that still require human intervention for data collection and system support (Paesano, 2023, pp. 1694–1723), they also incorporate advanced learning structures—such as reinforcement learning, machine learning, and deep learning—that enable the classification and analysis of large datasets with minimal direct human interaction. As such, autonomous AI is among the most complex AI concepts developed to date, marking a significant step toward greater machine independence while remaining distinct from fully autonomous artificial general intelligence.

Specialists define narrow AI as the many AI systems and tools currently in use that cannot perform certain tasks independently without human guidance (Hopgood, 2021, p. 514). By contrast, artificial general intelligence refers to an AI that can operate fully autonomously, independent of any human operator, and surpass human intelligence in all respects. Autonomous AI fits neither category, but it represents a significant step toward the development of artificial general intelligence.

An autonomous AI system requires the following two components:

- **Data collection instruments**, commonly referred to as sensors, which are physical devices used to gather data from the environment.[3]
- **Algorithms**. For a system to autonomously achieve a goal defined by a human, the collected data must be processed by computer algorithms (Lehmann et al., 2023). In the ideal case, where all components are smoothly integrated, an autonomous AI agent can operate independently of human input, make its own decisions, and perform tasks autonomously. An autonomous AI

[2] Moruzzi, C., & Margarido, S. (2024). Customizing the balance between user and system agency in human-AI co-creative processes. In *Proceedings of the 15th International Conference on Computational Creativity, ICCC'24, Jonköping, Sweden* (pp. 108–117). Association for Computational Creativity. https://www.research.ed.ac.uk/en/publications/customizing-the-balance-between-user-and-system-agency-in-human-a/

[3] Saari, M. (2024). *Software hardware combination for IoT sensor data gathering and prototyping: Architecture model, framework, and process model*. Tampere University. https://trepo.tuni.fi/handle/10024/154585

agent may be understood as a tool that receives a goal from a human and develops a strategy for achieving that goal through a set of tasks and actions (Sado et al., 2023, pp. 1–41).

It is evident that several potential benefits can be derived from ADMS-based systems (Salvini et al., 2023), although attitudes toward the acceptability of ADMS vary depending on the application and the end user (Aysolmaz et al., 2023). Human decision-making capacity is inherently limited and varies across individuals, as a single person can respond effectively to only a restricted number of stimuli at any given time (Sosnowski & Brosnan, 2023, pp. 1103–1117). By contrast, once an ADMS has been trained, it can be replicated indefinitely.[4] Beyond computational efficiency, the use of ADMS may offer additional benefits, including improvements in safety, cost reduction, efficiency, and accuracy (Attaran, 2020, pp. 158–172).

The potential risks associated with Automated Decision-Making Systems (ADMS), and the serious consequences they may impose on individuals in critical sectors such as healthcare, military operations, finance, and justice, highlight the need to integrate human oversight into automated decision-making frameworks (Leslie & Perini, 2024). Such integration is often presented as an essential means of ensuring accountability and effective supervision. However, the concept of meaningful human control gives rise to a paradox. On the one hand, systems are designed to make decisions independently in order to reduce or eliminate human involvement, thereby enhancing safety, lowering costs, and improving the prediction of behavior. On the other hand, there is a growing demand to monitor autonomous systems to ensure ethical outcomes, for example, by addressing concerns related to fairness.

Particularly troubling is the phenomenon of quasi-automation, in which humans are formally involved but function largely as a superficial source of validation, while the system performs the substantive decision-making tasks. In many organizations, insufficient staff training or a lack of adequate time allocated for decision-making have been identified as common issues. This problem was notably demonstrated in 2018, when Amazon faced criticism over an AI-based recruitment tool that ranked job candidates, which was found to be biased against women and black applicants.[5] The algorithm ranked applicants on a scale from one to five based on their résumés but systematically rated female candidates poorly because it had been trained on historical data reflecting male dominance in the technology sector. As will be discussed later in this paper, recruiters retained partial responsibility for shortlisting, interviewing, and hiring new employees, but they rarely reviewed the full pool of applicants due to the sheer volume of applications, which caused candidate lists to be processed very quickly. This example illustrates the need for clearly defined parameters to establish meaningful human control over ADMS (Saeik et al., 2021).

Legal Framework for AI in the EU

The European Commission has developed a number of legislative instruments in response to the rapid emergence and widespread deployment of diverse AI technologies across multiple sectors, as well as the ethical concerns and risks associated with their use. In 2021, the European Commission

[4] Smith, S., Patwary, M., Norick, B., LeGresley, P., Rajbhandari, S., Casper, J., Liu, Z., Prabhumoye, S., Zerveas, G., Korthikanti, V., Zhang, E., Child, R., Aminabadi, R. Y., Bernauer, J., Song, X., Shoeybi, M., He, Y., Houston, M., Tiwary, S., & Catanzaro, B. (2022). *Using DeepSpeed and Megatron to Train Megatron-Turing NLG 530B, A Large-Scale Generative Language Model* (arXiv:2201.11990). arXiv. https://doi.org/10.48550/arXiv.2201.11990

[5] Njoto, S. M. (2020). Gendered Bots? Bias in the use of Artificial Intelligence in Recruitment (pp. 11–15). *The Policy Lab, The University of Melbourne.* https://www.academia.edu/43650660/Gendered_Bots_Bias_in_the_use_of_Artificial_Intelligence_in_Recruitment

proposed the AI Act,[6] which establishes a comprehensive legal framework for the development, deployment, and use of AI systems across various sectors within the EU and its internal market (Schmidt et al., 2024). On July 12, 2024, the AI Act was published in the Official Journal of the European Union, marking it as the first horizontal legal framework specifically aimed at regulating artificial intelligence across the EU.[7] The AI Act became applicable on August 1, 2024, and will enter into full effect on August 2, 2026, unless specific provisions listed in Article 113 apply.[8]

As of February 2025, the EU AI Liability Directive—initially proposed by the European Commission to address legal challenges related to the attribution of responsibility in cases involving AI systems—has been formally withdrawn from the Commission's legislative agenda[9] (Grozdanovski, 2025, pp. 1–24). Despite early momentum, including the adoption of a position by the European Parliament's Committee on Legal Affairs (JURI Committee), proposals to extend the Directive's scope, and broader parliamentary interest, the Directive encountered strong opposition from EU member countries. Critics argued that it duplicated provisions already addressed by the newly adopted Product Liability Directive.[10] This withdrawal reflects institutional reluctance to create overlapping legal regimes and underscores the EU's preference to regulate AI liability and responsibility through existing legislation, particularly through the AI Act, and to rely on its overall regulatory effectiveness (Greenstein & Zamboni, 2025, pp. 1–41). The absence of a harmonized, specifically tailored AI liability regime creates a regulatory gap, especially in cases involving non-material harm and complex decision-making chains, which may undermine legal certainty and consumer protection in AI-related contexts.

Several EU legal acts and regulations are relevant to the governance of AI, including the EU Artificial Intelligence Act (AI Act),[11] the Digital Markets Act (DMA),[12] the Cyber Resilience Act (CRA),[13] the Data Act,[14] the Digital Services Act,[15] and the General Data Protection Regulation (GDPR),[16] all of which influence the regulation and deployment of AI systems within the EU.

6 Regulation 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, 2024 O.J. (L 1689) 1 [hereafter AI Act].

7 Ibid., art. 3(1).

8 Zwitter, A., Gstrein, O. J., & Haleem, N. (2024). *General-purpose AI regulation and the European Union AI Act.* Social Science Research Network. https://doi.org/10.2139/ssrn.4916400

9 AI Liability Directive. (n.d.). *The Artificial Intelligence Liability Directive.* https://www.ai-liability-directive.com/

10 Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products, 1985 O.J. (L 210) 29.

11 AI Act, art. 3(1), 2024 O.J. (L 1689) 46.

12 Regulation 2022/1925, of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 OJ (L 265).

13 Regulation 2024/2847, of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), 2024 O.J. (L 2024/2847) 1.

14 Regulation 2023/2854, of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation 2017/2394 and Directive 2020/1828 (Data Act), 2023 O.J. (L 2023/2854) 1.

15 Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

16 Regulation 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, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

The AI Act defines an "AI system" as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." A "general-purpose AI model" is defined as an AI model, including those trained on large datasets using self-supervision at scale, that demonstrates significant generality and is capable of competently performing a wide range of distinct tasks, regardless of how it is placed on the market, and that can be integrated into a variety of downstream systems or applications, excluding models used solely for research, development, or prototyping prior to market placement. The term "general-purpose AI system" refers to an AI system derived from a general-purpose AI model that can be used either as a standalone product or as part of other systems.

Pursuant to Article 3(66),[17] the AI Act has extraterritorial applicability to the following actors:

- any provider that places an AI system or a general-purpose AI model on the EU market, uses it for its own purposes, or otherwise makes it available, irrespective of whether the provider is established within the EU or in a third country;
- any deployer of AI systems that is established or located within the EU;
- any provider or deployer of an AI system established or located in a third country, where the output generated by the AI system is used within the EU.

The AI Liability Directive primarily addressed non-contractual, fault-based civil liability claims within the EU and was expected to adopt the same definition of AI as that used in the AI Act (Nikolinakos, 2024, pp. 477–621).

Under the AI Act, any developer of an AI system or general-purpose AI model, as well as any natural or legal entity, public authority, agency, or other body that develops and places such systems or models on the EU market, is classified as a "provider".[18]

A "distributor" is defined as any natural or legal entity in the supply chain other than a provider or importer who makes an AI system available on the EU market, but a provider or importer does not become a distributor solely by placing an AI system on the market.[19]

An "importer" is any natural or legal entity within the EU that places an AI system on the EU market which is marketed under the name or trademark of an entity established in a third country.[20]

The proposed AI Liability Directive sought to revise civil liability rules to make it easier for victims of AI-related harm to prove fault and obtain compensation. It aimed to enhance legal certainty by introducing mechanisms such as disclosure obligations and rebuttable presumptions to address the technical complexity and opacity of AI systems. However, the European Commission withdrew the Directive in early 2025 due to concerns about over-regulation and a lack of legislative progress. Although the Directive is no longer proceeding through the formal legislative process, its underlying objective of complementing the AI Act by addressing AI-related liability concerns remains relevant.

The AI Liability Directive was intended to ensure that individuals harmed by AI systems would have access to compensation equivalent to that available to victims of other forms of technological harm within the EU (Nikolinakos, 2024). Existing fault-based liability regimes are often ill-suited to address damage caused by AI-driven products and services. Victims may encounter significant

[17] AI Act, art. 3(66), 2024 O.J. (L 1689) 50.

[18] Ibid., art. 3(3).

[19] Ibid., art. 3(7).

[20] Ibid., art. 3(6).

practical and financial barriers when attempting to demonstrate fault and establish causation, largely due to the opaque, complex, and self-learning nature of AI systems.

Risk Categorization

The categorization of AI systems by risk level and the corresponding regulatory requirements under the EU Artificial Intelligence Act are set out in the following provisions:

- Article 5—Prohibited AI Practices, which lists AI systems and practices that are outright banned, such as manipulative subliminal techniques, social scoring by public authorities, and certain uses of biometric technologies.
- Article 6—High-Risk AI Systems, which defines what constitutes a high-risk AI system, including AI applications used in areas such as critical infrastructure, education, employment, law enforcement, migration, and the administration of justice.
- Article 7—Amendments to the List of High-Risk AI Systems, which establishes the mechanism through which the European Commission may update or expand the list of high-risk AI applications.

Under the AI Act, any undertaking that provides an AI system as a service, produces a product incorporating an AI system, deploys an AI system, imports an AI system, distributes an AI system, or acts as an authorized representative of an operator is classified as an "operator," regardless of legal form. Both individual providers and contractors specializing in general-purpose AI models are subject to obligations relating to technical documentation and transparency. They are also required to consult with the European Commission and national competent authorities and to comply with national legislation concerning copyright and related rights. Compliance may be demonstrated, *inter alia*, through adherence to approved codes of practice.

Additional obligations apply to providers of general-purpose AI models that pose systemic risk. These include requirements to conduct standardized model evaluations, identify and manage systemic risks, monitor incidents, and implement appropriate cybersecurity measures.

The AI Act further provides for the development of codes of conduct for AI systems, with the European Commission expressing the expectation that providers will adopt such codes on a voluntary basis (Cantero Gamito & Marsden, 2024). By contrast, the AI Liability Directive does not impose any comparable compliance obligations (Hacker, 2023).

Legal Personification of AI

The products and actions of artificial intelligence cannot easily be accommodated within existing legal categories, whether as property or as persons. Many scholars compare the current role of artificial intelligence in law to the historical concept of a "quasi-person", a legal status previously used to address entities that did not fit neatly into established legal classifications (Amelin et al., 2022, pp. 294–302). A number of authors have drawn analogies between the present legal treatment of artificial intelligence and earlier encounters with quasi-personhood in legal doctrine (Mecaj, 2022, pp. 180–196).

A related issue arises from the position of other legal scholars who argue that if discussions concerning the behavior of AI and its moral and ethical dimensions are to be treated as meaningful and coherent, then it may also be appropriate to consider the legal recognition of the personality of artificial intelligence. In this context, legal personality is viewed as a significant stage in the realization of constitutional rights. Once an AI system is granted legal personality under the law, it would, in principle, become a bearer of constitutional rights (Bublitz, 2024, pp. 1095–1106).

Complexities of Multi-Stakeholder Liability

Explainable AI (XAI) and Interpretability

Cognitive approaches to transparency and accountability in AI systems focus on the application of technological processes, tools, and practices that make artificial intelligence systems comprehensible, explainable, and traceable to organizational stakeholders (Göksal & Solarte Vasquez, 2024). These approaches seek to facilitate an understanding of how an AI system arrives at a particular conclusion and to provide mechanisms for challenging outcomes or identifying points at which the system may have failed. As a result, Explainable AI (XAI) has emerged as an important subfield concerned with making AI systems interpretable to human users (Holzinger et al., 2023, pp. 16–24).

When AI is deployed in serious and high-impact application contexts, there are strong societal imperatives to understand how AI systems function, to critically assess and challenge their outcomes, and to demand justification for AI-driven decisions and actions. In this regard, the EU's General Data Protection Regulation (GDPR) incorporates a so-called "right to explanation" and establishes principles governing solely automated decision-making that has significant effects on individuals (Bayamlıoğlu, 2022, pp. 1058–1078).

Legal and Regulatory Frameworks

Legal and regulatory frameworks play a crucial role in promoting transparency and establishing effective accountability within information systems that rely on artificial intelligence (Díaz-Rodríguez et al., 2023). Privacy laws contribute to fair data processing by requiring organizations to disclose how data is used and by enabling individuals to participate in and influence decisions concerning the use of their personal information (Mijwil et al., 2023, pp. 8–13). These laws also support accountability, as the GDPR grants data subjects the right to bring legal action against organizations for unlawful automated decision-making. Similarly, anti-discrimination laws facilitate accountability by prohibiting the development and deployment of AI systems that produce discriminatory outcomes, while also providing individuals with legal remedies for unfair treatment.

A recent case involving Clearview AI illustrates these concerns. The American facial recognition company was accused by the American Civil Liberties Union (ACLU) of violating Illinois' Biometric Information Privacy Act (BIPA) (Ahmed, 2023, pp. 66–95). The company reportedly collected billions of images from Facebook and other websites to build a facial recognition database without users' consent. This case raises significant questions regarding the use of AI systems that rely heavily on personal data.

Such challenges and regulatory gaps are often viewed as best addressed through incremental reforms to data protection law combined with the development of new AI governance frameworks. These measures may include expanding the definition of "personal data" to encompass inferred data, introducing privacy impact assessments and algorithmic audits for high-risk AI systems, and requiring comprehensive model documentation and reporting.

As artificial intelligence has become increasingly embedded in consumer products and services, growing scrutiny has emerged regarding accountability when AI systems cause harm to individuals (Patel, 2024, pp. 1–17). Traditional product liability regimes hold manufacturers responsible for harm caused by manufacturing defects, design flaws, or inadequate warnings. However, the autonomous and self-learning characteristics of AI systems make them difficult to assess under conventional product liability frameworks (Sayre & Glover, 2024, pp. 357–394). Defining what constitutes a "defect" in an AI system presents particular challenges (Hacker, 2023). This raises complex questions,

such as whether biased outputs generated by an AI system should be considered defects (Lesenciuc, 2024, pp. 9–22). If an AI system functions as intended and harm results from the optimization goals embedded in its design, such harm may be interpreted as a design defect (Li et al., 2023, pp. 1–46). Distinguishing between a flaw and an unavoidable or inherent risk associated with the intended use of AI remains inherently difficult.

Furthermore, under established product liability doctrines, the "component parts" rule generally excludes component suppliers from liability for harm caused by the final integrated product (Beck & Jacobson, 2017, pp. 143–210). The incorporation of AI systems further complicates liability attribution, as emergent properties may arise from interactions among multiple AI components (Díaz-Rodríguez et al., 2023). This makes it challenging to assign responsibility among the various actors involved in data provision, model development, and system integration.

The EU AI Liability Directive adopted a progressive yet cautious approach to addressing evidentiary challenges posed by multi-purpose AI systems by proposing two key mechanisms: the right to disclosure of evidence and a shift in the burden of proof. These measures were intended to rebalance procedural inequalities between claimants and powerful AI developers by empowering courts to order the disclosure of relevant technical information, such as system logs and training data, from high-risk AI providers. At the same time, national courts would have been permitted to presume causality where claimants could demonstrate that an AI system's failure plausibly caused the harm suffered, thereby easing evidentiary burdens in civil liability claims. While these mechanisms would have enhanced access to justice for victims, they also raised concerns about excessive disclosure of proprietary algorithms and the potential chilling effect on innovation. The Directive's emphasis on procedural fairness reflected the EU's preference for soft harmonization rather than strict liability. However, its withdrawal has created a regulatory gap in addressing evidentiary asymmetries in AI-related litigation (Ziosi et al., 2023).

As a result, plaintiffs may continue to face significant difficulties in obtaining sufficient evidence to prove that an AI system caused alleged harm, particularly because relevant algorithms and operational processes are often protected as proprietary information and not easily discoverable. This also complicates the apportionment of damages, as harms caused by AI systems may consist not of isolated losses but of cumulative minor inconveniences or diffuse negative externalities. Legislative reform may therefore be necessary to clarify procedural mechanisms in AI-related litigation. Such reforms could include requiring AI companies to establish integrated AI incident response teams to address liability claims or to maintain detailed data logs, testing records, and validation documentation for AI systems implicated in harm.

Guidelines on Business Ethics

There are multiple approaches to ethical AI, which are reflected in a range of core principles and bodies of work. One prominent example is the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, which has developed a set of principles for ethical AI known as the IEEE standards for AI (Jedličková, 2024, pp. 1–14). These principles can serve as a foundation for developing AI systems that are safe and socially relevant, in line with widely accepted societal values. Issues of bias and non-bias are critical considerations in the advancement of AI systems, along with principles of fairness and equality.

Improving collaboration among academia, industry, and government can contribute to greater transparency in AI systems and help ensure accountability for the outcomes they produce (Sharma, 2024). The integration of perspectives from disciplines such as computer science, law, ethics, and the

social sciences can provide the expertise needed to address the complex and multi-layered challenges of AI governance.[21]

This paper advocates for the development of collaborative governance models, emphasizing that this should be understood as a long-term process that demands sustained and coordinated effort. AI governance requires the participation of a broad range of societal actors, including policymakers, industry and business representatives, non-governmental organizations, and the general public (Zaidan & Ibrahim, 2024, pp. 1–18). Such inclusive involvement will help ensure that current and future AI systems are developed and deployed in accordance with diverse perspectives and expectations. In this way, collaborative governance supports responses to the complexity and multidimensional nature of AI governance challenges. The establishment of independent regulatory agencies for AI implementation is also proposed as a means of ensuring oversight and improving efficiency that encompasses multiple stakeholders.

Balancing Competing Interests

One of the central challenges of AI governance is the need to balance competing interests, including privacy, intellectual property rights, and transparency (Walter, 2024). Particular tension exists between the demand for transparency in AI processing and the protection of user privacy, indicating that while transparency is important, it should not be pursued in a manner that infringes upon individual privacy rights (Ramya et al., 2025, pp. 85–110). Various approaches have been proposed to address this discord, such as the use of differential privacy techniques, which aim to preserve individual privacy while maintaining a degree of transparency. These approaches highlight the difficulty of protecting proprietary innovations while simultaneously promoting transparency.

Because machine learning algorithms are often protected as intellectual property, companies are generally reluctant to disclose them, which can result in reduced transparency. To address these competing concerns, legal and policy recommendations have been proposed that would permit access to AI systems by third-party auditors under conditions that preserve confidentiality and anonymity.

Facebook* faced a class action lawsuit in which it was accused of violating the Illinois Biometric Information Privacy Act (BIPA)[22] by using facial recognition technology to collect and store its users' biometric data without their consent. In 2020, the company settled the case for $650 million (Nieves, 2021, pp. 1–20). This outcome was subsequently affirmed by the United States Court of Appeals for the Ninth Circuit in the well-known *Patel v. Facebook, Inc.* case.[23] In addition, in 2023, the Illinois Supreme Court issued another significant decision concerning BIPA enforcement. In *Cothron v. White Castle System, Inc.*,[24] the Court reaffirmed its prior jurisprudence by holding that each instance of biometric data collection without required consent constitutes a separate BIPA violation. This ruling has substantial implications for the calculation of damages and poses significant legal risks to organizations that fail to comply with the statute.

[21] Teixeira, N., & Pacione, M. (2024). *Implications of Artificial Intelligence on Leadership in Complex Organizations: An Exploration of the Near Future* [MRP]. OCAD University. https://openresearch.ocadu.ca/id/eprint/4190/

* Ed. note: By decision of the authorities of the Russian Federation, *Meta Platforms*, Inc. has been declared an extremist organization, and its activities are prohibited on the territory of Russia.

[22] Biometric Information Privacy Act of 2009, 740 ILCS 14/1–14/99 (Ill.).

[23] 932 F.3d 1264 (9th Cir. 2019).

[24] 2023 IL 128004.

Legal Challenges in AI Decision Making

A fault-based liability system, which requires proof of negligence or intent, is ill-suited to AI systems that operate autonomously or rely on opaque machine-learning processes and are, in many cases, beyond the direct control or even full understanding of users and developers alike (Botero Arcila, 2024). The evidentiary burden imposed by such a system would create unnecessary obstacles for victims, particularly in high-stakes sectors such as autonomous transportation or healthcare, where AI malfunctions may result in catastrophic harm. By contrast, a strict liability regime, which does not require proof of fault, is more compatible with the unpredictability and risk profile of advanced AI systems, especially those classified as high-risk under the AI Act.[25] However, the blanket application of strict liability may stifle innovation and impose disproportionate burdens on small-scale developers.

An alternative approach offering a more balanced solution is a hybrid liability model that combines strict liability for operators or deployers of high-risk AI systems with fault-based liability for designers and developers (Popa Tache & Vâlcu, 2025, pp. 281–305). Under this model, primary responsibility rests with the "AI owner" or deploying entity—such as a hospital, logistics provider, or digital platform—that determines how and where the system is used. Secondary liability may be attributed to developers or manufacturers where defects in design, training, or system updates can be demonstrated. Regulators may further support this framework by imposing obligations related to transparency, risk assessment, and insurance coverage. Ultimately, the construction of AI liability regimes must protect victims without imposing undue constraints on responsible innovation by ensuring accountability across the entire AI value chain and adapting legal frameworks to the distinctive risks and opacity associated with intelligent systems (Zekos, 2023, pp. 293–359).

Policy Recommendation on the Need for a Visionary Legal Framework for AI

There is an urgent need to establish a progressive legal framework that addresses liability for high-intelligence AI systems involved in decision-making in critical sectors such as healthcare, transportation, security, and commerce. Existing liability regimes, which are largely premised on human agency, are inadequate to address the challenges posed by autonomous and opaque AI-driven decision-making. The central legal questions that require resolution include identifying who should bear liability when harm is caused through the use of AI and determining how causation and fault should be established in a manner that balances innovation with justice. Addressing these issues is essential to ensure that the legal system evolves alongside technological development rather than lagging behind it.

The law should clearly distinguish between actors across the AI value chain in order to allocate liability appropriately. A recommended approach is a tiered liability model, under which strict liability is imposed on deployers and operators of high-risk AI systems—namely, those entities that choose to integrate such systems into real-world contexts, oversee their operation, and derive benefits from their use. These actors are generally best positioned to assess contextual risks and to implement appropriate protective measures. Conversely, liability for AI developers and model providers should be based on fault, with particular emphasis placed on whether reasonable care was exercised with respect to transparency, safety, and diligence in the design, training, and updating of AI systems. This approach encourages prudent behavior while avoiding undue constraints on innovation.

[25] Buiten, M., De Streel, A., & Peitz, M. (2021). *EU Liability Rules for the Age of Artificial Intelligence*. Social Science Research Network. https://doi.org/10.2139/ssrn.3817520

To address the difficulties associated with establishing causation and fault, traditional evidentiary rules must be adapted. AI systems are often described as "black boxes," making it difficult to trace specific outcomes to particular design or operational decisions. Accordingly, the legal framework should adopt a presumption of causality whereby, if an AI system causes harm, courts presume a causal link between the system and the injury. The burden would then shift to the operator or developer to demonstrate that appropriate care was taken to prevent this harm. Such a shift acknowledges the practical impossibility faced by victims in unpacking complex AI operations while incentivizing risk prevention by AI stakeholders.

In addition, the legal framework should mandate transparency, auditability, and traceability throughout the development and deployment of AI systems. Regulators should require that high-risk AI systems implement robust logging mechanisms, including comprehensive decision logs and metadata audit trails, to enable the reconstruction of system behavior in the context of liability proceedings. These technical requirements should be formalized through binding regulations similar to safety standards found in sectors such as pharmaceuticals or aviation. Establishing such shared evidentiary infrastructure would facilitate reasoned adjudication of responsibility and encourage openness in system design.

Given the distributed and collaborative nature of AI development, the framework should also incorporate mechanisms for shared liability in situations where responsibility cannot be clearly attributed to a single actor. For example, assigning joint and several liability may be appropriate in cases where commercial AI systems incorporate open-source models or third-party application programming interfaces. In cases where attribution remains particularly difficult, the establishment of AI compensation funds or mandatory insurance schemes for high-risk AI activities could provide effective remedies for victims while maintaining trust in the AI ecosystem and avoiding deterrence of investment.

From a governance perspective, there should be a central AI regulatory or supervisory authority with a mandate to enforce liability rules, issue binding safety certifications, and resolve disputes. This body should coordinate with sector-specific regulators and data protection authorities to ensure consistency in standards and enforcement. It should also maintain a public registry of certified high-risk AI systems and compliance audit reports, thereby enhancing transparency, accountability, and public oversight. Such an institution would serve both preventive and adjudicatory functions.

A forward-looking, dynamic, and socio-technically sensitive AI liability framework must take into account the technological complexity inherent in artificial intelligence. It should define liability across the entire AI lifecycle, reconceptualize evidentiary rules to address informational opacity, establish enforceable transparency and monitoring obligations, and provide effective compensation mechanisms. Crucially, it should also be aligned at the international level to avoid regulatory fragmentation and to support the safe, fair, and innovative development of AI on a global scale. Public policy should reinforce these objectives by embedding them within AI ecosystems and ensuring that legislative efforts continue to safeguard fundamental rights alongside technological progress.

Conclusion

This paper confirms that the emergence of AI-based decision-making and autonomous systems fundamentally disrupts existing liability frameworks, which were developed on the assumption of human actors and deterministic causation. Its central finding is that traditional tort, contract, and product liability regimes are inadequate in situations where autonomous systems operate with a high degree of independence, giving rise to significant challenges in assigning accountability when harm occurs.

A further key observation is that responsibility for AI-related harm cannot be easily attributed to a single actor. Instead, liability is often distributed among developers, manufacturers, deployers, and users. This diffusion of responsibility underscores the need for more refined mechanisms to allocate liability, particularly in high-risk sectors such as healthcare, transportation, and finance, where autonomous decision-making may generate systemic risks.

The study also highlights the limited effectiveness of fault-based liability mechanisms when applied in isolation and suggests that strict liability and risk-distribution models may be more effective in ensuring compensation and deterrence. Comparative analysis indicates that jurisdictions such as the European Union are moving toward more harmonized regulatory approaches, including the AI Liability Directive and reforms to product liability frameworks, while the United States has largely retained a sector-specific regulatory model.

Finally, the paper argues for a reconciliation of innovation and accountability through the implementation of transparency, explainability, and auditability requirements in AI systems. Liability regimes will need to evolve toward hybrid models that integrate fault-based, strict, and enterprise liability in order to ensure legal certainty and maintain public trust in autonomous technologies.

References

1. Dalsaniya, A., & Patel, K. (2022). Enhancing process automation with AI: The role of intelligent automation in business efficiency. *International Journal of Science and Research Archive*, *5*(2), 322–337. https://doi.org/10.30574/ijsra.2022.5.2.0083
2. Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the future: The interplay of artificial intelligence, innovation, and competitiveness and its effect on the global economy. *Asian Journal of Economics, Business and Accounting*, *24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269
3. Adnan, M., Xiao, B., Ali, M. U., Bibi, S., Yu, H., Xiao, P., Zhao, P., Wang, H., & An, X. (2024). Human inventions and its environmental challenges, especially artificial intelligence: New challenges require new thinking. *Environmental Challenges*, (16), Article 100976. https://doi.org/10.1016/j.envc.2024.100976
4. Ahmed, I. (2023). ACLU v. Clearview Ai, Inc., 2021 Ill. Cir. LEXIS 292. *DePaul Journal of Art, Technology & Intellectual Property Law*, *33*(1), 66–95.
5. Amelin, R., Channov, S., Dobrobaba, M., Kalinina, L., & Kholodnaya, E. (2022). Transformation of legal personality in the context of the development of modern digital technologies. *International Journal of Computer Science & Network Security, 22*(11), 294–302.
6. Atakishiyev, S., Salameh, M., Yao, H., & Goebel, R. (2024). Explainable artificial intelligence for autonomous driving: A comprehensive overview and field guide for future research directions. *IEEE Access*, (12), 101603–101625. https://doi.org/10.1109/ACCESS.2024.3431437

7. Attaran, M. (2020). Digital technology enablers and their implications for supply chain management. *Supply Chain Forum: An International Journal*, *21*(3), 158–172. https://doi.org/10.1080/16258312.2020.1751568
8. Aysolmaz, B., Müller, R., & Meacham, D. (2023). The public perceptions of algorithmic decision-making systems: Results from a large-scale survey. *Telematics and Informatics*, *79*, Article 101954. https://doi.org/10.1016/j.tele.2023.101954
9. Bathla, G., Bhadane, K., Singh, R. K., Kumar, R., Aluvalu, R., Krishnamurthi, R., Kumar, A., Thakur, R. N., & Basheer, S. (2022). Autonomous vehicles and intelligent automation: Applications, challenges, and opportunities. *Mobile Information Systems*, *2022*, Article 7632892. https://doi.org/10.1155/2022/7632892
10. Beck, J., & Jacobson, M. (2017). 3D printing: What could happen to products liability when users (and everyone else in between) become manufacturers. *Minnesota Journal of Law, Science and Technology*, *18*(1), 143–210.
11. Botero Arcila, B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, Article 106012. https://doi.org/10.1016/j.clsr.2024.106012
12. Bublitz, J. C. (2024). Might artificial intelligence become part of the person, and what are the key ethical and legal implications? *AI & SOCIETY*, *39*(3), 1095–1106. https://doi.org/10.1007/s00146-022-01584-y
13. Cantero Gamito, M., & Marsden, C. T. (2024). Artificial intelligence co-regulation? The role of standards in the EU AI Act. *International Journal of Law and Information Technology*, *32*, Article eaae011. https://doi.org/10.1093/ijlit/eaae011
14. Chukwuani, V. N., & Egiyi, M. A. (2020). Automation of accounting processes: Impact of artificial intelligence. *International Journal of Research and Innovation in Social Science*, *4*(8), 444–449.
15. Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López De Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, Article 101896. https://doi.org/10.1016/j.inffus.2023.101896
16. Dong, Y., Hou, J., Zhang, N., & Zhang, M. (2020). Research on how human intelligence, consciousness, and cognitive computing affect the development of artificial intelligence. *Complexity*, *2020*, 1–10. https://doi.org/10.1155/2020/1680845
17. Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., … Wright, R. (2023). Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, *71*, Article 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642
18. Göksal, Ş.-İ., & Solarte-Vasquez, M. C. (2024). The blockchain-based trustworthy artificial intelligence supported by stakeholders-in-the-loop model. *Scientific Papers of the University of Pardubice, Series D: Faculty of Economics and Administration*, *32*(2). https://doi.org/10.46585/sp32022083
19. Greenstein, S., & Zamboni, M. (2025). Navigating the legislative dilemma: Evaluating the EU AI Act's approach to regulating emerging technologies. *The Theory and Practice of Legislation*, *13*(3), 312–352. https://doi.org/10.1080/20508840.2025.2513177
20. Grozdanovski, L. (2025). Non-discrimination law, the GDPR, the AI act and the—Now withdrawn—AI liability directive proposal offering gateways to pre-trial knowledge of algorithmic discrimination. *AI and Ethics*, *5*(5), 5039–5062. https://doi.org/10.1007/s43681-025-00754-0
21. Hacker, P. (2023). The European AI liability directives – Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, *51*, Article 105871. https://doi.org/10.1016/j.clsr.2023.105871

22. Holzinger, A., Keiblinger, K., Holub, P., Zatloukal, K., & Müller, H. (2023). AI for life: Trends in artificial intelligence for biotechnology. *New Biotechnology*, *74*, 16–24. https://doi.org/10.1016/j.nbt.2023.02.001
23. Hopgood, A. A. (2021). *Intelligent systems for engineers & scientists: A practical guide to artificial intelligence*. CRC Press Inc. https://doi.org/10.1201/9781003226277
24. Jedličková, A. (2025). Ethical approaches in designing autonomous and intelligent systems: A comprehensive survey towards responsible development. *AI & Society*, *40*(4), 2703–2716. https://doi.org/10.1007/s00146-024-02040-9
25. Khaleel, M., Jebrel, A., & Shwehdy, D. M. (2024). Artificial intelligence in computer science. *International Journal of Electrical Engineering and Sustainability*, *2*(2), 1–21. https://doi.org/10.5281/zenodo.13836932
26. Kumar, Y., Koul, A., Singla, R., & Ijaz, M. F. (2023). Artificial intelligence in disease diagnosis: A systematic literature review, synthesizing framework and future research agenda. *Journal of Ambient Intelligence and Humanized Computing*, *14*(7), 8459–8486. https://doi.org/10.1007/s12652-021-03612-z
27. Lehmann, J., Schorz, S., Rache, A., Häußermann, T., Rädle, M., & Reichwald, J. (2023). Establishing reliable research data management by integrating measurement devices utilizing intelligent digital twins. *Sensors*, *23*(1), Article 468. https://doi.org/10.3390/s23010468
28. Lesenciuc, A. (2024). Defective truth. AI or HI ideological imprints and political biases? *Romanian Journal of Information Technology and Automatic Control*, *34*(3), 9–22. https://doi.org/10.33436/v34i3y202401
29. Leslie, D., & Perini, A. M. (2024). Future shock: Generative AI and the international AI policy and governance crisis. *Harvard Data Science Review*, (Special Issue 5). https://doi.org/10.1162/99608f92.88b4cc98
30. Li, B., Qi, P., Liu, B., Di, S., Liu, J., Pei, J., Yi, J., & Zhou, B. (2023). Trustworthy AI: From principles to practices. *ACM Computing Surveys*, *55*(9), Article 177. https://doi.org/10.1145/3555803
31. Lucci, S., Musa, S., & Kopec, D. (2022). *Artificial intelligence in the 21st century* (3rd ed.). Mercury Learning and Information. https://doi.org/10.1515/9781683922520
32. Markauskaite, L., Marrone, R., Poquet, O., Knight, S., Martinez-Maldonado, R., Howard, S., Tondeur, J., De Laat, M., Buckingham Shum, S., Gašević, D., & Siemens, G. (2022). Rethinking the entwinement between artificial intelligence and human learning: What capabilities do learners need for a world with AI? *Computers and Education: Artificial Intelligence*, *3*, Article 100056. https://doi.org/10.1016/j.caeai.2022.100056
33. McCarthy, J. (2022). Artificial intelligence, logic, and formalising common sense. In *Machine learning and the city* (pp. 69–90). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119815075.ch6
34. Mecaj, S. E. (2022). Artificial intelligence and legal challenges. *Revista Opinião Jurídica (Fortaleza)*, *20*(34), 181–196. https://doi.org/10.12662/2447-6641oj.v20i34.p180-196.2022
35. Mijwil, M., Aljanabi, M., & ChatGPT. (2023). Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime. *Iraqi Journal for Computer Science and Mathematics*, *4*(1). https://doi.org/10.52866/ijcsm.2023.01.01.0019
36. Mikki, S. (2024). Generalized neuromorphism and artificial intelligence: Dynamics in memory space. *Symmetry*, *16*(4), Article 492. https://doi.org/10.3390/sym16040492
37. Nieves, A. M. (2021). Facial recognition technology: Can we tame the wild west? *Journal of Law and Technology at Texas, 5*, 1–20.
38. Nikolinakos, N. Th. (2024). Reforming the EU civil liability framework applicable to artificial intelligence and other emerging digital technologies: Defective products—The revised Product Liability Directive. In N. Th. Nikolinakos (Ed.), *Adapting the EU civil liability regime to the digital age: Artificial intelligence, robotics, and other emerging technologies* (pp. 477–621). Springer International Publishing. https://doi.org/10.1007/978-3-031-67969-8_9
39. Paesano, A. (2021). Artificial intelligence and creative activities inside organizational behavior. *International Journal of Organizational Analysis*, *31*(5), 1694–1723. https://doi.org/10.1108/IJOA-09-2020-2421

40. Patel, K. (2024). Ethical reflections on data-centric AI: Balancing benefits and risks. *International Journal of Artificial Intelligence Research and Development (Ijaird)*, *2*(1), 1–17.
41. Perwej, Y., Akhtar, N., & Agarwal, D. (2024). The emerging technologies of Artificial Intelligence of Things (AIoT): Current scenario, challenges, and opportunities. In *Convergence of artificial intelligence and internet of things for industrial automation* (pp. 1–32). CRC Press.
42. Popa Tache, C. E., & Vâlcu, E. N. (2025). Artificial intelligence and corporate liability towards a new legal-ethical contract in the dynamics of emerging global human rights convergences. *Juridical Tribune-Review of Comparative and International Law*, *15*(2), 281-305.
43. Ramya, R., Priya, S., Thamizhikkavi, P., & Anand, M. (2025). The pillars of AI ethics: Transparency, accountability, and privacy. In *Responsible implementations of generative AI for multidisciplinary use* (pp. 85–110). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9173-0.ch004
44. Sado, F., Loo, C. K., Liew, W. S., Kerzel, M., & Wermter, S. (2023). Explainable goal-driven agents and robots: A comprehensive review. *ACM Computing Surveys*, *55*(10), Article 211. https://doi.org/10.1145/3564240
45. Saeik, F., Avgeris, M., Spatharakis, D., Santi, N., Dechouniotis, D., Violos, J., Leivadeas, A., Athanasopoulos, N., Mitton, N., & Papavassiliou, S. (2021). Task offloading in edge and cloud computing: A survey on mathematical, artificial intelligence and control theory solutions. *Computer Networks*, *195*, Article 108177. https://doi.org/10.1016/j.comnet.2021.108177
46. Salvini, P., Reinmund, T., Hardin, B., Grieman, K., Ten Holter, C., Johnson, A., Kunze, L., Winfield, A., & Jirotka, M. (2023). Human involvement in autonomous decision-making systems. Lessons learned from three case studies in aviation, social care and road vehicles. *Frontiers in Political Science*, *5*, Article 1238461. https://doi.org/10.3389/fpos.2023.1238461
47. Sayre, M., & Glover, K. (2024). Machines make mistakes too: Planning for AI liability in contracting. *Journal of Law, Technology, & the Internet*, *15*(2), 357–394.
48. Schmidt, J., Schutte, N. M., Buttigieg, S., Novillo-Ortiz, D., Sutherland, E., Anderson, M., de Witte, B., Peolsson, M., Unim, B., Pavlova, M., Stern, A. D., Mossialos, E., & van Kessel, R. (2024). Mapping the regulatory landscape for artificial intelligence in health within the European Union. *NPJ Digital Medicine*, *7*(1), Article 229. https://doi.org/10.1038/s41746-024-01221-6
49. Sharma, S. (2024). Benefits or concerns of AI: A multistakeholder responsibility. *Futures*, *157*, Article 103328. https://doi.org/10.1016/j.futures.2024.103328
50. Sosnowski, M. J., & Brosnan, S. F. (2023). Under pressure: The interaction between high-stakes contexts and individual differences in decision-making in humans and non-human species. *Animal Cognition*, *26*(4), 1103–1117. https://doi.org/10.1007/s10071-023-01768-z
51. Taeihagh, A., Ramesh, M., & Howlett, M. (2021). Assessing the regulatory challenges of emerging disruptive technologies. *Regulation & Governance*, *15*(4), 1009–1019. https://doi.org/10.1111/rego.12392
52. Telikani, A., Tahmassebi, A., & Gandomi, A. (2021). Evolutionary machine learning: A survey. *ACM Computing Surveys*, *54*, 1–35. https://doi.org/10.1145/3467477
53. Walter, Y. (2024). Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*, *4*(1), Article 14. https://doi.org/10.1007/s44163-024-00109-4
54. Zaidan, E., & Ibrahim, I. A. (2024). AI governance in a complex and rapidly changing regulatory landscape: A global perspective. *Humanities and Social Sciences Communications*, *11*(1), Article 1121. https://doi.org/10.1057/s41599-024-03560-x
55. ZainEldin, H., Gamel, S. A., Talaat, F. M., Aljohani, M., Baghdadi, N. A., Malki, A., Badawy, M., & Elhosseini, M. A. (2024). Silent no more: A comprehensive review of artificial intelligence, deep learning, and machine learn-

ing in facilitating deaf and mute communication. *Artificial Intelligence Review*, *57*(7), Article 188. https://doi.org/10.1007/s10462-024-10816-0

56. Zekos, G. I. (2023). *Artificial intelligence and competition: Economic and legal perspectives in the digital age*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-48083-6
57. Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. *Journal of Industrial Information Integration*, *23*, Article 100224. https://doi.org/10.1016/j.jii.2021.100224
58. Ziosi, M., Mökander, J., Novelli, C., Casolari, F., Taddeo, M., & Floridi, L. (2023). The EU AI liability directive (AILD): Bridging information gaps. *European Journal of Law and Technology*, *14*(3).

Information about the author:

Kolawole O. Afuwape — LL.M. (University of Dundee, Scotland, United Kingdom), LL.M. (Lagos State University, Nigeria), Lecturer, Jindal Global Law School, Sonipat, India.
afuwapekolawole@gmail.com
ORCID: https://orcid.org/0009-0001-5686-230X

Сведения об авторе:

Афувапе К. О. — магистр права (Университет Данди, Шотландия, Соединенное Королевство), магистр права (Государственный университет Лагоса, Нигерия), преподаватель, Глобальный университет им. О. П. Джиндала, Сонипат, Индия.
afuwapekolawole@gmail.com
ORCID: https://orcid.org/0009-0001-5686-230X