



Research Article

Artificial Intelligence Liability and Legal Personality in the Age of Autonomous Systems

Nelson Agbor* 

School of Law, Criminology and Criminal Justice, University of Northampton, Northampton, United Kingdom

Abstract

Artificial intelligence (AI) is rapidly transforming modern society, with increasingly autonomous systems making decisions that affect healthcare, finance, transport, commerce, criminal justice, and public administration. As AI systems evolve from merely executing programmed instructions to learning, adapting, and acting with limited human intervention, traditional legal doctrines of liability are under growing strain. Existing legal frameworks generally attribute responsibility to human actors, including programmers, manufacturers, operators, and users. However, these approaches become increasingly inadequate when harm results from autonomous decision-making that cannot easily be traced to a single human actor. This article critically examines whether AI should be recognised as possessing a limited form of legal personality capable of giving rise to legal liability. Drawing on doctrinal legal research and comparative and interdisciplinary analysis, the study evaluates existing theories of legal personality, corporate personhood, agency, product liability, and negligence, as well as emerging international regulatory approaches, including the European Union AI Act. It analyses whether the concept of legal personality should evolve to accommodate highly autonomous AI systems while preserving the fundamental objectives of accountability, justice, and effective compensation for victims. The article argues that granting AI unrestricted legal personality would undermine established principles of legal responsibility and obscure human accountability. Nevertheless, the law should recognise a functional and limited legal status for specified categories of highly autonomous AI operating within tightly regulated environments. The article concludes that the future of AI regulation depends not on treating machines as equivalent to natural persons but on developing an adaptive legal framework that balances innovation, accountability, public trust, and the rule of law in an increasingly autonomous digital society.

Keywords

Artificial Intelligence, Autonomous Systems, Legal Personality, AI Liability Tort Law, AI Governance, Algorithmic Accountability, Comparative AI Regulation

*Correspondence: Nelson Agbor (nelson.agbor@northampton.ac.uk), Nelson Agbor (nelsonagbor@yahoo.com)

Received: 3 September 2026; **Accepted:** 14 September 2026; **Published:** 28 September 2026



Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

1. Introduction

1.1. Background to Artificial Intelligence and Autonomous Systems

Artificial intelligence (AI) has emerged as one of the most transformative technological developments of the twenty-first century. Once confined to theoretical computer science and speculative fiction, AI has rapidly evolved into a pervasive force in contemporary society, influencing virtually every sector of economic, political, and social life [47]. Advances in machine learning, deep learning, neural networks, natural language processing, computer vision, and autonomous robotics have enabled AI systems to perform tasks that once required human cognition, including reasoning, prediction, decision-making, language generation, and adaptive learning. Increasingly sophisticated AI applications now operate across healthcare, finance, transportation, education, policing, defence, manufacturing, legal services, and public administration, often making decisions with significant consequences for individuals and society¹. Unlike traditional software, many modern AI systems can learn from data, adapt their behaviour over time, and produce outcomes that may not have been explicitly programmed by their developers [51]. The growing integration of autonomous technologies into everyday decision-making has fundamentally altered traditional assumptions about legal accountability. Historically, legal systems have operated on the premise that harmful conduct can ultimately be attributed to identifiable human actors or legally recognised organisations. However, highly autonomous AI systems increasingly operate in ways that make causal attribution considerably more complex [20].

1.2. The Emerging Challenge of AI Liability

The rapid advancement of AI has exposed significant deficiencies in existing systems of civil, criminal, administrative, and regulatory liability. As AI systems become increasingly autonomous, traditional legal concepts of fault, negligence, intention, causation, foreseeability, and accountability become harder to apply. In many cases, harmful outcomes cannot be readily attributed to a single identifiable human decision-maker. For example, an autonomous vehicle may cause a fatal collision even when operating in accordance with its learning algorithms [4]. A medical diagnostic AI may misidentify a life-threatening condition, leading to delayed treatment. A financial algorithm may manipulate markets through unintended interactions with competing systems [42]. Traditional liability models generally assume that harmful conduct origi-

nates with an identifiable legal subject possessing legal capacity. Tort law seeks to establish negligence or a breach of duty; criminal law generally requires both a prohibited act and a culpable mental state; contract law depends on legally recognised parties capable of assuming obligations; and product liability focuses primarily on defects attributable to manufacturers. These established doctrines become increasingly strained when AI systems independently generate decisions that neither developers nor users anticipated [46]. The so-called "responsibility gap" has therefore become a central concern in AI scholarship. As autonomous systems become more sophisticated, the gap between human decision-making and machine-generated outcomes widens [11]².

1.3. Research Problem

The principal problem addressed in this article is the growing mismatch between traditional legal doctrines of liability and the increasingly autonomous behaviour of contemporary AI systems. Existing legal frameworks largely assume that every legally significant act can ultimately be attributed to either a natural person or an established juristic person, such as a corporation. This assumption becomes increasingly problematic when AI systems generate decisions independently through continuous learning processes that neither developers nor operators fully understand or control [34]. Current approaches often attempt to allocate liability among programmers, manufacturers, owners, users, or employers. While appropriate in many circumstances, these approaches become less satisfactory as AI systems gain greater operational autonomy and decision-making capability [4]. Furthermore, legal uncertainty risks undermining both innovation and public confidence. Businesses need predictable liability rules before deploying advanced AI technologies, while individuals affected by AI-generated decisions need accessible legal remedies when harm occurs. The absence of coherent legal principles for highly autonomous systems threatens both objectives. Although several jurisdictions have proposed new regulatory frameworks for AI safety, transparency, and risk management, there is comparatively little consensus on whether AI itself should ever possess legal personality or whether entirely new liability models are required [31].

1.4. Research Questions

This article seeks to answer the following research questions:

- 1) How do existing legal doctrines conceptualise legal personality and legal responsibility?

¹This capacity to adapt and evolve distinguishes contemporary AI from earlier automated technologies. Autonomous vehicles, algorithmic trading systems, diagnostic medical software, generative AI models, autonomous drones, and predictive policing algorithms demonstrate varying degrees of operational independence, raising important legal questions about responsibility when these systems cause harm

²It raises fundamental jurisprudential questions about the nature of legal responsibility. Specifically, it invites reconsideration of whether AI should remain merely an object of regulation or whether sufficiently autonomous systems ought, in limited circumstances, to be recognised as legal subjects capable of bearing certain legal responsibilities.

- 2) Why do traditional liability frameworks struggle to regulate increasingly autonomous AI systems?
- 3) Should highly autonomous AI systems be recognised as having a limited form of legal personality?
- 4) What theoretical justifications support or oppose granting legal personality to AI?
- 5) How have different jurisdictions addressed questions of AI liability and accountability?
- 6) Which regulatory model best balances innovation, legal certainty, accountability, and the protection of fundamental rights³?

1.5. Research Objectives

The primary objective of this article is to critically assess whether contemporary legal systems should reconsider the concept of legal personality in light of increasingly autonomous AI.

To achieve this objective, the article seeks to:

- 1) examine the historical and theoretical foundations of legal personality;
- 2) analyse the limitations of existing tort, contract, criminal, and product liability frameworks when applied to AI.
- 3) evaluate competing scholarly arguments concerning AI legal personality.
- 4) compare emerging regulatory responses across major jurisdictions.
- 5) assess the practical implications of recognising AI as a limited legal person.
- 6) propose an alternative framework that ensures accountability and supports responsible technological innovation.

1.6. Research Methodology

This study adopts a qualitative doctrinal legal research methodology. Doctrinal research is particularly appropriate because the article primarily examines legal principles, statutory frameworks, judicial decisions, regulatory developments, and jurisprudential theories concerning legal personality and liability. The research systematically analyses primary legal sources, including legislation, case law, international regulatory instruments, and policy documents, as well as secondary academic literature in legal scholarship, philosophy, computer science, and technology governance [53]. The article also employs comparative legal analysis, examining developments in the European Union, the United Kingdom, the United States, and selected international organisations. This approach enables the identification of common regulatory trends, divergences, and emerging best practices in AI governance and accountability. In addition, the research incorporates normative

legal analysis. Rather than merely describing existing law, the article critically evaluates whether current legal frameworks adequately address the challenges posed by autonomous AI systems and proposes reforms grounded in broader principles of justice, accountability, legal certainty, proportionality, and human rights [5].

1.7. Scope and Limitations

This article examines questions of legal personality and liability arising from autonomous AI systems operating in civil, commercial, and regulatory contexts. It focuses on systems capable of making decisions with varying degrees of human intervention, including autonomous vehicles, medical diagnostic AI, algorithmic decision-making systems, generative AI technologies, and autonomous robotics. The analysis primarily addresses private law liability, though criminal law and regulatory accountability are considered where relevant. The comparative discussion focuses predominantly on developments within the European Union, the United Kingdom, the United States, and selected international initiatives, reflecting their significant influence on global AI governance. The article does not seek to resolve broader philosophical debates about machine consciousness, sentience, or artificial moral agency⁴.

1.8. Original Contribution of the Study

This article contributes to the growing body of scholarship on AI governance by integrating legal theory, comparative regulation, and practical liability analysis within a unified jurisprudential framework. Rather than treating legal personality as a purely theoretical question, the article examines its practical implications for accountability, compensation, regulatory enforcement, and public confidence in autonomous technologies. The article also contributes by critically assessing whether existing legal concepts remain sufficiently flexible to regulate future generations of AI systems. Rather than adopting polarised positions that AI should either be granted legal personality or treated as legal property, the article argues for a more nuanced functional approach that distinguishes between different levels of autonomy and corresponding forms of legal responsibility. Furthermore, the study seeks to bridge doctrinal legal scholarship and emerging technological realities by proposing a liability model that allocates responsibility proportionately among developers, deployers, operators, manufacturers, insurers, and, where legally appropriate, highly autonomous AI systems operating within carefully defined regulatory boundaries⁵.

³Collectively, these questions aim to clarify whether the existing legal framework can continue to regulate future generations of AI or whether more fundamental doctrinal reform is required.

⁴The study also recognises the rapidly evolving nature of AI technologies and reg-

ulatory frameworks. Legislative reforms continue to emerge globally, so future developments may require reassessment of some conclusions presented herein.

⁵By integrating jurisprudence, comparative law, technology regulation, and public policy, the article provides a comprehensive framework to inform future legislative reform and judicial interpretation.

2. The Evolution of Artificial Intelligence and Autonomous Decision-Making

2.1. Defining Artificial Intelligence

Artificial intelligence (AI) broadly refers to computer systems capable of performing tasks that typically require human intelligence. These tasks include learning, reasoning, problem-solving, language processing, perception, prediction, and decision-making. Unlike conventional software, which follows predetermined instructions, many modern AI systems use machine learning algorithms to identify patterns in large datasets and improve their performance over time without explicit reprogramming [30]. The distinguishing feature of contemporary AI is therefore not merely automation but adaptive intelligence. This capacity to process vast quantities of information and generate increasingly sophisticated outputs has made AI a central component of modern governance, commerce, healthcare, education, and legal practice⁶.

2.2. Categories of AI Systems

AI systems may be classified by their capabilities and levels of autonomy. Narrow AI, often called weak AI, is designed to perform specific tasks such as facial recognition, language translation, fraud detection, or legal document review [14]. These systems dominate current commercial applications and typically operate within predefined parameters [50]. By contrast, Artificial General Intelligence (AGI) remains a theoretical concept, referring to machines capable of performing any intellectual task a human can undertake across multiple domains. Beyond AGI lies Artificial Superintelligence (ASI), a hypothetical stage at which AI would exceed human cognitive abilities in virtually every field [23]. From a regulatory perspective, AI systems are also classified by the degree of risk they pose. Risk-based classifications distinguish among minimal-risk applications; limited-risk systems subject to transparency obligations; high-risk systems operating in sectors such as healthcare, policing, employment, and transportation; and prohibited AI practices that threaten fundamental rights [38].

2.3. Autonomous Systems and Machine Learning

The defining characteristic of modern AI is its growing autonomy. Machine learning enables systems to analyse data, identify relationships, and improve predictive accuracy through iterative training rather than fixed programming. Deep learning, a subset of machine learning, employs multi-layered artificial neural networks capable of recognising complex patterns in large datasets. Reinforcement learning further

enables AI systems to optimise behaviour through continuous interaction with their environment by rewarding successful outcomes and penalising undesirable ones [48]. These technologies enable autonomous systems to perform functions with minimal human intervention. Autonomous vehicles continuously interpret road conditions and make real-time driving decisions. Medical diagnostic systems analyse radiological images and recommend treatment options. Financial algorithms execute transactions within milliseconds, while generative AI systems produce text, images, software code, and legal analysis with minimal user input [17].

2.4. From Automation to Autonomous Agency

The progression from simple automation to autonomous agency is among the most significant technological developments facing contemporary legal systems. Traditional automated systems execute predefined commands and remain entirely dependent on human programming. Autonomous AI systems, however, possess varying degrees of independence in interpreting information, selecting alternatives, and adapting to changing circumstances [37]. Although AI lacks consciousness, emotions, or genuine free will, its operational independence often gives the impression of agency. Many systems now produce outcomes that are difficult for their designers to predict because complex machine-learning models continuously evolve as they are exposed to new data. Consequently, decisions may arise from computational processes that remain opaque even to those who created the algorithms, a phenomenon commonly described as the "black box" problem [56]. This transition challenges conventional legal assumptions that every legally relevant act can ultimately be traced to a specific human decision-maker. The increasing operational independence of AI therefore raises a fundamental jurisprudential question: at what point does technological autonomy require legal doctrines on responsibility to evolve?⁷[56].

2.5. Contemporary Uses of AI in Society

AI has become deeply embedded in virtually every aspect of contemporary life. In healthcare, AI supports disease diagnosis, predictive analytics, drug discovery, and robotic surgery. Financial institutions rely on algorithmic trading, fraud detection, credit assessment, and risk management systems. In transport, autonomous vehicles and intelligent traffic management systems promise improved safety and efficiency while introducing novel legal risks [29]. The legal profession increasingly uses AI for legal research, document review, contract analysis, predictive litigation analytics, and generative drafting. Public authorities use AI in immigration decision-making, welfare administration, taxation, policing, and border

⁶As AI systems continue to evolve, legal scholars have increasingly questioned whether existing legal doctrines remain adequate to regulate technologies that display varying degrees of autonomy and independent decision-making.

⁷While AI remains a legal object under current law, its growing capacity for autonomous decision-making has intensified calls for new legal frameworks that address accountability without undermining technological innovation

security. Educational institutions integrate AI into personalised learning environments, automated assessment, and academic administration⁸. While these innovations enhance productivity and economic growth, they also raise significant legal and ethical concerns about discrimination, privacy, intellectual property, misinformation, cybersecurity, transparency, and accountability [20].

2.6. The Growing Risk of AI-Caused Harm

The expansion of autonomous AI systems has significantly increased the risk of legal harm. AI-generated decisions may cause physical injury, economic loss, reputational damage, privacy violations, discriminatory outcomes, or infringements of fundamental rights. Autonomous vehicles may be involved in fatal accidents; medical AI may misdiagnose patients; predictive policing algorithms may reinforce systemic biases; financial systems may trigger market instability; and generative AI may disseminate defamatory or misleading content on a global scale [6]. A defining characteristic of AI-related harm is the complexity of causal attribution. Unlike conventional products, autonomous AI frequently operates through dynamic interactions among developers, data providers, deployers, users, and continuously evolving algorithms. Consequently, identifying the legally responsible actor is increasingly difficult. Existing doctrines of negligence, product liability, and vicarious liability often struggle to accommodate circumstances in which harmful outcomes arise from self-learning computational processes rather than direct human instruction. These challenges expose what many scholars call the "accountability gap" in AI governance [21].

3. Theoretical Foundations of Legal Personality

3.1. The Concept of Legal Personality

Legal personality is a foundational concept in jurisprudence, determining which entities can hold rights, incur obligations, and participate in legal relations. A legal person is an entity recognised by law as having the capacity to hold rights, incur duties, own property, enter into contractual relationships, sue and be sued, and bear legal responsibility. The concept is therefore a legal construct rather than a biological or moral one. While all human beings are recognised as natural persons, the law has long extended legal personality to artificial entities, including corporations, partnerships, charities, local authorities, universities, and certain public institutions. These entities possess legal personality not because they possess consciousness or moral agency, but because such recognition facilitates

legal certainty, economic efficiency, and the orderly administration of justice [32]. The distinction between legal personality and moral personhood is particularly significant in discussions of artificial intelligence (AI). Moral personhood traditionally depends on characteristics such as consciousness, rationality, intentionality, autonomy, and moral responsibility. By contrast, legal personality has historically been granted for functional and pragmatic reasons rather than philosophical ones. A corporation neither thinks nor feels, yet it enjoys legal rights and bears legal obligations because the law considers such recognition necessary to achieve identifiable legal objectives. Consequently, the legal system has repeatedly shown that legal personality is a flexible instrument capable of adapting to changing social, political, and economic realities⁹.

3.2. Historical Development of Legal Personality

The concept of legal personality has evolved alongside organised legal systems. In Roman law, legal capacity was initially confined to natural persons, although certain collective entities, such as municipalities and religious bodies, gradually acquired recognised legal status. Medieval canon law further expanded the concept by recognising monasteries, churches, and universities as juridical entities capable of owning property and conducting legal affairs independently of their individual members. The Industrial Revolution significantly accelerated the expansion of legal personality through the rise of incorporated businesses. The emergence of the modern corporation reflected the practical necessity of allowing organisations to own assets, enter into contracts, and assume liabilities independently of shareholders. This development reached its doctrinal maturity in the principle of separate corporate personality, under which an incorporated company became legally distinct from its members [23].

3.3. Natural Persons and Juristic Persons

Legal systems traditionally distinguish between natural persons and juristic (or artificial) persons. Natural persons acquire legal personality automatically at birth and possess the full range of legal rights and obligations recognised by law, subject to age, capacity, and other legal limitations. They are capable of criminal responsibility, civil liability, contractual obligations, and constitutional rights. Juristic persons, by contrast, derive their legal existence entirely from law. Their personality is created by legislation, judicial recognition, or incorporation and exists only to the extent permitted by the legal system. For example, corporations may own property, employ workers, enter into contracts, litigate, and incur liability independently of their shareholders. Their legal personality enables courts to attribute rights and responsibilities directly to

⁸Meanwhile, generative AI systems have transformed creative industries by producing written content, artwork, music, software code, and audiovisual materials.

⁹The issue is not whether AI is human, but whether existing legal categories remain

capable of accommodating technologies whose actions increasingly influence legal rights and obligations.

the organisation rather than exclusively to individual members [7]. This distinction is significant because AI cannot presently be categorised as either a natural or a conventional juristic person. Unlike humans, AI lacks biological existence, consciousness, and moral agency. Unlike corporations, AI is not incorporated and has neither shareholders nor governing organs [24].

3.4. Theories of Legal Personality

Legal scholarship has developed several theories explaining why the law grants legal personality to certain entities. Although these theories predate AI, they provide valuable analytical frameworks for assessing whether autonomous systems could, in principle, qualify for legal recognition [8].

3.4.1. Fiction Theory

Fiction Theory, primarily associated with Friedrich Carl von Savigny, holds that only human beings are genuine legal persons. According to this view, corporations and other artificial entities possess personality only because the law creates a legal fiction for practical purposes. Their rights and obligations ultimately derive from the legal system rather than from any independent existence. Applied to AI, Fiction Theory suggests that legal personality could be conferred on autonomous systems only through explicit legislative recognition. AI would not become a person by virtue of its technological capabilities, but solely because lawmakers deemed such recognition beneficial to the administration of the law [25].

3.4.2. Concession Theory

The Concession Theory likewise holds that legal personality exists only by virtue of state recognition. Under this approach, the state determines which entities may acquire legal status and defines the scope of their rights and obligations. This theory emphasises legislative sovereignty and public policy. Applied to AI, it implies that any legal personality granted to autonomous systems would depend entirely on democratic legislative choice rather than on technological development alone. Recognition would therefore remain conditional, limited, and revocable in light of public interest considerations.

3.4.3. Realist Theory

The Realist Theory challenges the view that legal personality is merely fictional. It holds that collective entities possess genuine social existence independent of legal recognition, as they function as organised institutions with identifiable interests and decision-making structures. Legal personality merely acknowledges this underlying social reality. Applied to AI, this theory raises more difficult questions. Although advanced AI systems increasingly perform socially significant functions and interact independently with individuals and institutions, they remain technologically dependent on human-created infrastructure. Whether this operational autonomy amounts to

genuine social existence remains contested [25].

3.4.4. Purpose Theory

The Purpose Theory regards legal personality as an instrument for achieving specific legal objectives rather than as recognition of intrinsic characteristics. Under this approach, legal personality exists because it facilitates efficient administration, accountability, and the protection of legal interests. This functional perspective is particularly relevant to AI because it shifts attention away from philosophical debates about consciousness and instead asks whether recognising limited legal personality would improve legal certainty, allocate liability more effectively, and strengthen regulatory oversight. Consequently, Purpose Theory perhaps provides the strongest jurisprudential foundation for careful consideration of limited forms of AI legal personality.

3.5. Rights, Duties and Legal Capacity

Legal personality comprises not only the possession of rights but also the assumption of corresponding legal duties. A legal person must ordinarily have legal capacity to participate in legal relationships, including owning property, entering into contracts, bringing legal proceedings, complying with statutory obligations, and bearing responsibility for unlawful conduct. Importantly, legal systems frequently distinguish between the possession of rights and the extent of legal capacity. Minors, persons lacking mental capacity, and corporations all possess varying degrees of legal capacity, depending on statutory provisions and judicial interpretation [49]. This distinction has significant implications for AI. Even if highly autonomous systems were granted some form of legal personality, that recognition need not mirror the comprehensive legal status of natural persons [44].

3.6. Can Legal Personality Exist Without Consciousness

Perhaps the strongest objection to recognising AI as a legal person is that machines lack consciousness, emotions, intentionality, and moral agency. Traditional theories of criminal responsibility, ethical accountability, and human dignity often assume that genuine responsibility requires conscious choice. AI systems, however, process information through computational algorithms rather than subjective awareness, and therefore cannot presently experience intention, guilt, remorse, or moral blameworthiness. Nevertheless, history shows that legal personality has never depended exclusively on consciousness. Corporations, charitable trusts, government agencies, municipalities, and international organisations all possess legal personality despite lacking independent minds or emotions [28]. Their legal status exists because it enables the law to regulate complex social and economic relationships effectively. The more pressing question is whether recognising limited legal

personality for highly autonomous AI would improve accountability, more effectively compensate victims, and promote responsible innovation without undermining established legal principles [8].

4. Existing Liability Frameworks for Artificial Intelligence

4.1. Tort Liability

Tort law has traditionally been the principal means by which individuals obtain compensation for harm caused by the wrongful acts or omissions of others. Liability generally depends on establishing that the defendant owed a duty of care, breached that duty, and thereby caused foreseeable damage to the claimant. These principles have proved sufficiently flexible to accommodate many technological developments; however, the emergence of increasingly autonomous AI systems has exposed significant limitations in their application. Where AI systems function merely as tools under direct human control, conventional negligence principles remain largely adequate. Developers may be liable for negligent programming, manufacturers for defective design, operators for misuse, and organisations for failing to implement appropriate safeguards. Courts may struggle to determine whether the harm resulted from negligent programming, inadequate supervision, poor-quality training data, unforeseeable machine-learning outcomes, or the system's autonomous operation [43].

4.2. Contractual Liability

Contract law governs the legal obligations parties voluntarily assume and provides remedies when contractual terms are breached. AI is increasingly integrated into commercial transactions through automated contracting, algorithmic procurement, smart contracts, digital assistants, and autonomous commercial decision-making. Businesses routinely use AI to negotiate prices, manage inventories, process customer requests, and fulfil contractual obligations with minimal human intervention. Despite these developments, AI cannot presently be a contracting party because it lacks legal personality and contractual capacity. Contracts involving AI remain legally attributable to the individuals or organisations deploying the technology. Consequently, liability ordinarily falls to the contracting party rather than to the AI system performing the relevant functions [30]. However, autonomous AI increasingly challenges established contractual doctrines. Questions arise when AI systems generate contractual terms not anticipated by either party, make unauthorised commercial decisions, or execute transactions that produce unintended legal consequences. Smart contracts on blockchain platforms further complicate matters by automatically executing contractual obligations without direct human oversight. Existing contract

law generally resolves these issues by attributing responsibility to the deploying organisation, yet increasing AI autonomy may eventually strain this approach as human intervention becomes minimal. While contract law continues to regulate commercial AI deployment effectively in many contexts, future autonomous systems may require a more sophisticated allocation of contractual responsibility [18].

4.3. Criminal Liability

Criminal liability poses perhaps the greatest challenge for AI regulation because criminal responsibility traditionally depends on two essential elements: the commission of a prohibited act (*actus reus*) and the presence of a culpable mental state (*mens rea*). Criminal law presupposes intentional, reckless, or negligent human conduct accompanied by moral blameworthiness. Artificial intelligence cannot presently satisfy these requirements. AI possesses neither consciousness nor criminal intent and cannot appreciate the moral or legal consequences of its conduct. Consequently, current legal systems cannot prosecute AI systems themselves. Instead, criminal liability remains attributable to developers, manufacturers, operators, employers, or users where their conduct satisfies established principles of criminal responsibility [26]. Nevertheless, increasingly autonomous AI creates novel challenges. Autonomous vehicles involved in fatal collisions, AI-assisted medical errors, algorithmic financial manipulation, and autonomous weapons systems all raise difficult questions about the attribution of criminal fault [31].

4.4. Product Liability

Product liability has become one of the most significant legal mechanisms governing AI-related harm. Traditionally, manufacturers are strictly liable when defective products cause injury, irrespective of negligence. Product liability therefore shifts attention away from individual fault and towards the safety of products placed on the market. AI technologies frequently fall within the scope of product liability when software is integrated into physical products such as autonomous vehicles, medical devices, industrial robots, or consumer electronics. When defects arise from flawed design, manufacturing errors, inadequate warnings, or foreseeable misuse, existing product liability frameworks often provide effective remedies for injured parties [32]. However, self-learning AI poses significant challenges for traditional product liability doctrine. Unlike conventional products, AI systems may evolve after entering the market through continuous learning and software updates. Harm may arise not from an original manufacturing defect but from behavioural changes that emerge long after deployment. Determining whether such changes constitute product or software defects, or operational failures, becomes increasingly difficult [23].

4.5. Vicarious Liability

Vicarious liability holds employers and organisations responsible for wrongful acts committed by employees acting within the scope of their employment. The doctrine reflects broader public policy objectives by ensuring that organisations benefiting from particular activities also bear the associated legal risks. As organisations increasingly deploy AI in employment contexts, questions arise as to whether AI-generated decisions should also trigger vicarious liability. Employers remain responsible for discriminatory recruitment software, automated dismissal systems, algorithmic workplace monitoring, and AI-assisted employment decisions because these technologies operate on the organisation's behalf. Nevertheless, the analogy becomes less convincing as AI systems gain greater operational independence. Unlike employees, AI lacks consciousness, contractual employment, and legal personality. Consequently, applying traditional vicarious liability principles to autonomous systems is conceptually strained. Although organisations should ordinarily remain responsible for the technologies they deploy, future AI systems capable of substantial independent decision-making may require alternative liability models that better reflect the distribution of control among developers, deployers, and operators [17].

4.6. Corporate Liability and AI

Corporate liability offers another useful framework for understanding AI accountability. Corporations possess legal personality and may incur both civil and criminal liability independently of individual shareholders. Legal systems therefore attribute organisational responsibility, even though corporations lack human consciousness. Some scholars argue that AI could eventually receive analogous legal treatment. Since corporations already function as artificial legal persons, extending a carefully limited legal personality to highly autonomous AI may appear conceptually consistent. However, important differences remain. Corporations possess internal governance structures, directors, shareholders, regulatory oversight, and identifiable financial assets against which judgments may be enforced. AI systems currently lack these institutional characteristics. While corporate liability demonstrates the flexibility of legal personality, it does not automatically justify recognising AI as a separate legal subject. Rather, corporate liability shows that legal systems have previously created artificial persons to enhance accountability and commercial certainty [16].

4.7. The Limits of Existing Legal Frameworks

The foregoing analysis shows that existing liability frameworks continue to regulate many AI-related disputes effectively. Tort law compensates victims for negligence, contract law governs commercial relationships, criminal law punishes

culpable human conduct, product liability addresses defective technologies, vicarious liability allocates organisational responsibility, and corporate liability illustrates the adaptability of legal personality. Collectively, these doctrines provide substantial protection when AI functions primarily as an advanced technological tool [52]. However, these frameworks share a common assumption: every legally significant act can ultimately be attributed to a recognised legal person. As AI systems become increasingly autonomous, this assumption becomes less convincing. Existing doctrines often struggle to identify a single responsible actor when harmful outcomes arise from complex interactions among developers, data providers, deployers, users, and self-learning algorithms. The resulting accountability gap risks undermining both effective victim compensation and legal certainty for innovators. Existing liability doctrines remain indispensable, but they appear increasingly inadequate to regulate highly autonomous AI operating with limited human oversight [35].

5. Should Artificial Intelligence Possess Legal Personality

5.1. Arguments Supporting AI Legal Personality

The proposal to recognise artificial intelligence (AI) as possessing legal personality has attracted growing scholarly attention as autonomous systems become more sophisticated. Proponents argue that existing legal frameworks are increasingly unable to address situations in which AI systems independently make decisions that cause legal harm. They contend that recognising a limited form of legal personality would improve legal certainty, facilitate the attribution of liability, and ensure that victims are not left without effective remedies. Supporters further argue that legal personality is a legal construct rather than a reflection of biological or moral status. Since corporations, charities, municipalities, and other artificial entities already possess legal personality despite lacking consciousness, there is no conceptual reason why the law could not recognise highly autonomous AI systems for specific regulatory purposes [12]. Under this approach, AI would not enjoy the full rights of natural persons but would possess a carefully defined legal status that would enable it to bear civil obligations, maintain compulsory insurance, own designated assets, or participate in limited legal proceedings¹⁰.

5.2. Arguments Against AI Legal Personality

Despite these arguments, substantial opposition remains. Critics contend that legal personality should not be extended

¹⁰Such recognition, it is argued, would strengthen accountability while encouraging responsible technological innovation.

to AI because machines lack the essential characteristics traditionally associated with responsibility, including consciousness, intentionality, free will, moral judgement, and the capacity to understand legal obligations. Unlike corporations, which are governed by human directors and shareholders, AI systems possess neither independent institutional structures nor genuine moral decision-making autonomy. Opponents also warn that recognising AI as a legal person could weaken, rather than strengthen, accountability. Developers, manufacturers, operators, and commercial organisations might seek to shift liability onto AI systems to avoid responsibility for defective products or negligent deployment [41].

5.3. Electronic Personhood: Origins and Development

The concept of "electronic personhood" emerged from broader debates about regulating autonomous robots and AI systems. It envisages a limited legal status applicable only to highly autonomous technologies operating with minimal human intervention. Rather than equating AI with human beings, electronic personhood seeks to establish a functional legal category through which certain autonomous systems may bear specified legal obligations. The proposal has sparked significant academic and regulatory debate because it seeks to address the growing accountability gap created by increasingly autonomous technologies¹¹. Advocates suggest that electronic personhood could operate alongside mandatory insurance, registration requirements, and regulatory oversight, thereby ensuring effective compensation where conventional liability rules prove inadequate [38].

5.4. Lessons from Corporate Personality

Corporate personality is perhaps the most frequently cited analogy in discussions of AI legal status. A corporation possesses separate legal personality despite lacking physical existence, consciousness, or moral agency. It may own property, enter into contracts, sue and be sued, and incur both civil and criminal liability independently of its shareholders [15]. This demonstrates that legal personality has historically been created to serve practical legal objectives rather than philosophical ideals. However, important distinctions remain. Corporations operate through identifiable governance structures, including directors, shareholders, financial assets, and statutory obligations, which enable courts to enforce judgments effectively. AI systems lack these institutional characteristics. Consequently, while corporate personality demonstrates the flexibility of legal doctrine, it cannot be simply replicated for AI without substantial modification [22].

5.5. Comparative Analysis with Animals, Ships and Trusts

Comparative legal analogies further illustrate the adaptability of legal personality. Although animals are increasingly recognised as deserving legal protection, they generally remain legal objects rather than legal persons. Ships, however, have historically been treated as independent juridical entities in certain maritime proceedings, allowing actions to be brought directly against the vessel. Similarly, trusts operate through legal arrangements that separate beneficial from legal ownership, despite lacking independent consciousness. These examples demonstrate that legal systems have often developed specialised constructs to address unique practical circumstances. AI therefore need not fit neatly within existing categories of natural or corporate personality [3].

5.6. Moral Agency versus Legal Agency

A critical distinction in the AI debate is that between moral and legal agency. Moral agency presupposes the capacity to understand ethical principles, exercise free will, and bear moral blame for one's actions. Contemporary AI systems clearly do not satisfy these criteria. Their decisions result from computational processes rather than from conscious reflection or moral reasoning. Legal agency, however, is considerably broader. Many legal entities perform legally significant functions without moral consciousness. Consequently, legal personality need not depend on moral agency if its primary objective is to facilitate effective regulation and accountability. The more pressing question is therefore whether recognising limited legal agency for certain autonomous AI systems would improve legal certainty and victim compensation without diminishing the responsibility of the human actors involved in their creation, deployment, and supervision [2].

5.7. Practical Consequences of Recognising AI as a Legal Person

Recognising limited legal personality for AI would have significant practical consequences. It could facilitate clearer allocation of civil liability, support compulsory insurance schemes, improve regulatory oversight, and enhance public confidence in autonomous technologies. It might also encourage developers to embed stronger governance, transparency, and safety mechanisms into AI systems. However, such recognition also poses substantial risks. If poorly designed, AI legal personality could become a mechanism for corporations to evade liability by attributing harmful outcomes to autonomous systems rather than to organisational failures. For this reason, any future recognition should be narrowly confined to specified regulatory purposes and should never displace the contin-

¹¹Nevertheless, concerns remain that the concept risks obscuring rather than clari-

fying responsibility unless accompanied by robust safeguards that preserve the liability of developers, manufacturers, and deployers.

uing liability of developers, manufacturers, deployers, or operators [13].

6. Comparative Regulatory Approaches

6.1. The European Union's AI Regulatory Framework

The European Union (EU) has emerged as the global leader in developing a comprehensive regulatory framework for artificial intelligence. Its approach is grounded in a risk-based model that classifies AI systems by the level of risk they pose to individuals, society, and fundamental rights. AI applications that pose unacceptable risks are prohibited, while high-risk systems in sectors such as healthcare, education, employment, law enforcement, border management, and critical infrastructure are subject to stringent regulatory obligations. These obligations include conformity assessments, transparency requirements, human oversight, risk management systems, and post-market monitoring. Importantly, the EU framework does not recognise AI as having legal personality. Instead, accountability remains firmly attached to the developers, providers, deployers, importers, and distributors of AI systems. This reflects the EU's commitment to ensuring that technological innovation remains subject to meaningful human responsibility while safeguarding fundamental rights and consumer protection [24].

6.2. The United Kingdom's Approach to AI Governance

The United Kingdom has adopted a more flexible, innovation-oriented approach to AI regulation. Rather than introducing a single comprehensive AI statute, the UK favours a principles-based framework, implemented by existing sectoral regulators. Core regulatory principles include safety, transparency, fairness, accountability, contestability, and proportionality. Regulators are expected to apply these principles within their respective sectors while fostering technological innovation. The UK's approach emphasises that existing legal doctrines, including negligence, product liability, data protection, equality law, and consumer protection, remain capable of addressing many AI-related disputes [43].

6.3. The United States' Regulatory Position

The United States has generally favoured a decentralised, market-driven approach to AI governance. Federal regulation remains fragmented, with sector-specific agencies overseeing AI across healthcare, financial services, transportation, defence, and consumer protection. States have also begun intro-

ducing legislation addressing algorithmic discrimination, privacy, and automated decision-making. American regulatory policy generally prioritises innovation while relying on existing tort law, product liability, contract law, competition law, and consumer protection statutes to address AI-related harms. Although academic debate on AI legal personality continues, legislative attention has focused primarily on ensuring transparency, reducing algorithmic bias, strengthening cybersecurity, and encouraging responsible AI development, rather than creating a new category of legal person [39].

6.4. International Developments

Beyond domestic legal systems, international organisations have increasingly recognised the need for coordinated AI governance. Because AI technologies operate across national borders, fragmented regulatory approaches risk creating uncertainty for businesses, developers, and consumers, and undermine effective accountability. International initiatives have therefore emphasised the importance of trustworthy AI, transparency, fairness, human oversight, privacy protection, and respect for human rights. Although regulatory approaches differ considerably, there is broad consensus that AI should remain subject to meaningful human control and that legal responsibility should not disappear simply because decision-making processes become increasingly automated [19].

6.5. Emerging Standards from International Organisations

Several international organisations have developed principles to guide the responsible development and deployment of AI. Common themes include human-centred innovation, transparency, explainability, accountability, non-discrimination, security, and effective governance. These standards encourage governments to adopt regulatory frameworks that protect fundamental rights while supporting scientific and technological progress. Importantly, these emerging international standards consistently place responsibility on human actors and institutions rather than on AI itself¹². Developers, deployers, regulators, and commercial organisations are expected to implement appropriate governance mechanisms, conduct impact assessments, ensure ongoing monitoring, and provide accessible remedies where AI causes harm [44].

6.6. Comparative Lessons for Future AI Liability

The comparative analysis reveals considerable variation in regulatory techniques but substantial agreement on the underlying principles of AI governance. The European Union favours comprehensive legislative regulation grounded in risk management, while the United Kingdom adopts a flexible

¹²This reinforces the prevailing international consensus that accountability should

remain human-centred despite increasing technological autonomy

principles-based model and the United States relies more heavily on existing legal doctrines and sector-specific oversight. Nevertheless, all three jurisdictions reject the proposition that AI should presently possess independent legal personality. A common feature across these approaches is the preservation of human accountability [45]. Legislators consistently seek to ensure that developers, manufacturers, deployers, operators, and organisations remain legally responsible for the deployment and consequences of AI systems. However, the comparative experience also demonstrates growing recognition that existing liability doctrines may become increasingly strained as AI systems acquire greater operational autonomy [28].

7. Case Studies and Judicial Developments

7.1. Autonomous Vehicles

Autonomous vehicles are among the clearest examples of the legal challenges posed by AI. Modern self-driving systems rely on machine learning, sensors, cameras, radar, and real-time data processing to make independent driving decisions. While these technologies promise to reduce human error and improve road safety, several high-profile accidents involving autonomous vehicles have shown that AI systems can also cause serious injury or death. The principal legal difficulty concerns the attribution of responsibility. When an autonomous vehicle causes an accident, liability may fall on the manufacturer, software developer, vehicle owner, maintenance provider, or human operator [36]. Existing negligence and product liability rules often struggle to determine which party exercised sufficient control over the AI system at the time of the accident¹³.

7.2. Medical Artificial Intelligence

AI has transformed healthcare by improving diagnostic accuracy, supporting clinical decision-making, facilitating drug discovery, and assisting with robotic surgery. Diagnostic algorithms can analyse radiological images, predict disease progression, and recommend treatment options with remarkable speed and accuracy. Nevertheless, AI-generated medical errors can cause severe harm to patients. When an AI system misdiagnoses cancer, recommends inappropriate treatment, or fails to detect life-threatening conditions, determining legal responsibility is particularly challenging. Liability may fall to software developers, healthcare institutions, medical practitioners, or device manufacturers. Courts must determine whether clinicians reasonably relied on AI recommendations or whether independent professional judgement should always prevail [27].

7.3. Generative Artificial Intelligence and Copyright

Generative AI has posed significant challenges for intellectual property law. Large language models and image-generation systems can produce articles, artwork, software code, music, and audiovisual content that closely resemble existing copyrighted works. This has led to numerous disputes over copyright infringement, ownership of AI-generated works, and the lawful use of copyrighted materials in AI training. Courts and legislators continue to grapple with questions about whether AI-generated outputs infringe existing intellectual property rights and whether developers bear responsibility for content produced autonomously by their systems [45]. These disputes demonstrate that conventional copyright doctrines require careful adaptation to balance innovation with the protection of creators' rights.

7.4. Algorithmic Discrimination

The deployment of AI across recruitment, lending, policing, healthcare, education, and immigration has exposed the risk of algorithmic discrimination. Machine learning systems trained on biased historical datasets may unintentionally reproduce or amplify existing social inequalities, resulting in discriminatory outcomes based on race, gender, disability, age, or socioeconomic status. Judicial and regulatory developments increasingly emphasise that organisations cannot avoid liability by attributing discriminatory decisions solely to algorithms. Instead, employers, financial institutions, public authorities, and technology companies remain responsible for ensuring that AI systems comply with equality and human rights legislation.

7.5. AI in Financial Services

Financial institutions increasingly use AI to detect fraud, assess creditworthiness, execute algorithmic trading, manage investment portfolios, and evaluate financial risk. These technologies improve efficiency but also pose systemic legal risks. Autonomous trading algorithms may contribute to market instability, while automated lending systems may produce discriminatory or inaccurate credit assessments. Regulatory authorities have responded by tightening requirements on transparency, explainability, governance, and operational resilience. Financial case studies show that legal responsibility generally remains with regulated institutions rather than with AI systems themselves [40].

7.6. Autonomous Weapons Systems

Perhaps the most controversial application of AI concerns autonomous weapons systems capable of identifying and en-

¹³These cases therefore illustrate the growing inadequacy of traditional liability models

in situations where machine learning significantly influences decision-making.

gaging targets with minimal human intervention. Such technologies raise profound legal and ethical questions under international humanitarian law, international human rights law, and international criminal law. When autonomous weapons unlawfully kill civilians or violate the principles of distinction, proportionality, or precaution, identifying legal responsibility becomes exceptionally difficult. Potential liability may fall to military commanders, software developers, manufacturers, governments, or political leaders [9].

7.7. Judicial Responses to AI-Related Liability

Although AI-specific jurisprudence remains in its early stages, judicial responses reveal a consistent pattern across multiple jurisdictions. Courts have generally declined to recognise AI as an independent legal person and continue to allocate responsibility to identifiable human actors and organisations. Developers, manufacturers, employers, healthcare providers, commercial enterprises, and public authorities remain legally accountable for the deployment and operation of AI systems. At the same time, judicial reasoning increasingly recognises the unique challenges posed by autonomous decision-making, algorithmic opacity, and complex causal relationships. Courts have emphasised the importance of transparency, explainability, human oversight, and foreseeable risk management when assessing liability. These emerging judicial trends suggest that, while existing legal doctrines remain applicable, they require careful adaptation to the distinctive characteristics of modern AI [10].

8. Towards a New Model of AI Liability

8.1. The Inadequacy of Traditional Legal Doctrines

The preceding analysis shows that existing legal doctrines provide an important foundation for regulating artificial intelligence (AI), yet they are increasingly strained by the rise of highly autonomous systems. Tort, contract, criminal, product liability, and vicarious liability all assume that harmful conduct can ultimately be attributed to an identifiable legal person. As AI systems become more capable of learning, adapting, and making independent decisions, this assumption becomes less convincing. The resulting accountability gap creates uncertainty for developers, businesses, regulators, and individuals harmed by AI-generated decisions¹⁴ [52].

8.2. A Functional Model of AI Responsibility

This article proposes a functional model of AI responsibility

based on the degree of autonomy exercised by the AI system, rather than on the fiction that AI possesses human characteristics. Under this approach, legal responsibility should be proportionate to the level of operational independence demonstrated by the technology. Low-risk AI functioning solely as a decision-support tool should remain subject to conventional liability rules. By contrast, highly autonomous systems operating with minimal human intervention should attract enhanced regulatory obligations and clearer mechanisms for allocating responsibility. Importantly, this model does not advocate recognising AI as having full legal personality. Instead, it supports a limited functional legal status, under which such recognition improves legal certainty, facilitates compensation, and strengthens regulatory oversight without displacing human responsibility [54].

8.3. Shared Liability Between Developers, Operators and Users

Given the complexity of modern AI ecosystems, liability should ordinarily be shared among the principal participants responsible for designing, deploying, maintaining, and operating AI systems. Developers should remain responsible for negligent programming, inadequate testing, insecure software architecture, and foreseeable algorithmic defects. Manufacturers should bear responsibility for unsafe products placed on the market, while deployers and operators should remain accountable for inappropriate implementation, inadequate supervision, misuse, or failure to monitor system performance. Users may also incur liability if they knowingly disregard operational guidance or use AI for unlawful purposes. This shared liability model more accurately reflects the distributed nature of AI governance and avoids the unrealistic expectation that a single actor can always exercise complete control over increasingly autonomous systems [53].

8.4. Strict Liability for High-Risk AI Systems

For particularly hazardous AI applications, fault-based liability may prove insufficient. This article therefore supports the introduction of strict liability for high-risk AI systems operating in sectors where failures could cause significant physical, economic, or societal harm. These sectors include autonomous transportation, healthcare, critical infrastructure, financial markets, law enforcement, and defence. Under a strict liability regime, claimants would not need to establish negligence but would need only to demonstrate that the AI system caused the relevant harm. Organisations deploying high-risk AI would therefore assume responsibility for the risks associated with introducing such technologies into society [33].

¹⁴Accordingly, rather than abandoning traditional doctrines, legal systems should develop a complementary framework

that reflects the distinctive characteristics of autonomous technologies while preserving meaningful human accountability.

8.5. Mandatory Insurance and Compensation Funds

To complement strict liability, governments should require mandatory insurance for operators and providers of high-risk AI systems. As with compulsory motor vehicle insurance, mandatory AI insurance would ensure victims receive timely compensation, irrespective of the financial capacity of individual developers or deployers. In addition, legislatures should consider establishing publicly supervised compensation funds for catastrophic AI-related harms where conventional litigation is inadequate. Such funds could provide rapid financial assistance while preserving the right to pursue further claims against responsible parties. These mechanisms would enhance access to justice and reduce lengthy, costly litigation in technically complex disputes involving autonomous technologies [21].

8.6. Regulatory Oversight and Compliance Mechanisms

Effective AI liability cannot rest solely on private litigation. Comprehensive regulatory oversight is essential to prevent harm. Regulatory authorities should therefore require developers and deployers of high-risk AI systems to conduct risk and algorithmic impact assessments, independent audits, cybersecurity testing, and continuous post-deployment monitoring. Transparency obligations should ensure that significant AI decisions remain explainable and amenable to meaningful human review. Organisations should maintain detailed records of AI development, training data, operational updates, and decision-making processes to facilitate judicial review and regulatory investigations in the event of disputes [55]. Robust compliance mechanisms not only strengthen accountability but also foster public trust in AI technologies by demonstrating that innovation remains subject to effective legal supervision.

8.7. Ethical Principles and Human Rights Safeguards

Any future AI liability framework must ultimately remain grounded in fundamental ethical principles and the protection of human rights. AI should be designed and deployed in a manner that respects human dignity, equality, privacy, non-discrimination, due process, and access to effective remedies. Legal responsibility should reinforce, rather than diminish, these values. Accordingly, recognising any limited functional legal status for AI should never allow developers, manufacturers, or organisations to evade accountability. Human oversight must remain central to decisions affecting life, liberty, health, employment, immigration, criminal justice, and other

areas involving fundamental rights. A human-centred approach to AI governance ensures that technological innovation serves society rather than undermining the rule of law¹⁵. Taken together, the proposed model combines shared liability, strict liability for high-risk applications, compulsory insurance, enhanced regulatory oversight, and robust human rights protections [1].

9. Conclusion

9.1. Summary of Findings

This article has examined whether existing legal doctrines remain capable of regulating increasingly autonomous artificial intelligence (AI) systems. It has demonstrated that although traditional frameworks of tort, contract, criminal, product, and corporate liability continue to provide an important legal foundation, they are increasingly strained by AI systems that learn, adapt, and make decisions with limited human intervention. The resulting accountability gap creates significant uncertainty in attributing legal responsibility.

9.2. The Future of Legal Personality

The analysis shows that legal personality is a flexible legal construct that has evolved in response to changing societal needs. However, the article concludes that AI should not presently be recognised as having full legal personality. Instead, any future recognition should be limited, functional, and carefully regulated to improve legal certainty without diminishing human accountability.

9.3. Recommendations for Legislators and Policymakers

Legislators should adopt comprehensive, risk-based AI governance frameworks that include strict liability for high-risk systems, mandatory insurance, transparency obligations, algorithmic impact assessments, and effective regulatory oversight. International cooperation should also be strengthened to promote harmonised standards for AI accountability.

9.4. Recommendations for Courts and Regulators

Courts should continue to interpret existing legal doctrines purposively, recognising the distinctive characteristics of autonomous AI. Regulators should require continuous monitoring, explainability, human oversight, and independent auditing to ensure that AI systems remain safe, transparent, and aligned with fundamental rights.

¹⁵This approach offers a balanced framework that encourages responsible innova-

tion while ensuring that increasingly autonomous AI systems remain subject to effective legal accountability and judicial control.

9.5. Areas for Future Research

Future research should examine the legal implications of Artificial General Intelligence (AGI), decentralised autonomous systems, cross-border AI governance, and the interplay among AI liability, human rights, and international law. As AI technology continues to evolve, legal scholarship must remain equally dynamic to ensure that innovation advances alongside accountability, justice, and the rule of law.

Abbreviations

AI	Artificial Intelligence
AGI	Artificial General Intelligence
ASI	Artificial Superintelligence

Author Contributions

Nelson Agbor: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Resources, Supervision, Visualization, Writing – original draft

Conflicts of Interest

The author declares no conflicts of interest.

References

- [1] Aizenberg, E. and Van Den Hoven, J., 2020. Designing for human rights in AI. *Big Data & Society*, 7(2), p. 2053951720949566.
- [2] Arvan, M., 2022. Varieties of artificial moral agency and the new control problem.
- [3] Baeyaert, J., 2025. Beyond Personhood: The Evolution of Legal Personhood and Its Implications for AI Recognition. *Technology and Regulation*, 2025, pp. 355-386.
- [4] Barocas, S., Hardt, M. and Narayanan, A., 2023. *Fairness and machine learning: Limitations and opportunities*. MIT Press.
- [5] Bayles, M. D., 1987. *Principles of law: A normative analysis* (p. 1). D. Reidel: distrib. Kluwer Academic Publishers.
- [6] Bengio, Y., 2024. Government interventions to avert future catastrophic AI risks. *Harvard Data Science Review*, 5.
- [7] Beran, K., 2020. *The concept of juristic person*. Wolters Kluwer.
- [8] Blumenthal, S. L., 2016. *Law and the modern mind: Consciousness and responsibility in American legal culture*. Harvard University Press.
- [9] Bode, I. and Huelss, H., 2022. *Autonomous weapons systems and international norms*. McGill-Queen's Press-MQUP.
- [10] Buiten, M., De Streel, A. and Peitz, M., 2023. The law and economics of AI liability. *Computer Law & Security Review*, 48, p. 105794.
- [11] Cane, P., 2017. *Key ideas in tort law*. Bloomsbury Publishing.
- [12] Cerka, P., Grigienė, J. and Sirbikytė, G., 2017. Is it possible to grant legal personality to artificial intelligence software systems? *Computer Law & Security Review*, 33(5), pp. 685-699.
- [13] Chesterman, S., 2020. Artificial intelligence and the limits of legal personality. *International & Comparative Law Quarterly*, 69(4), pp. 819-844.
- [14] Chesterman, S., 2020. Artificial intelligence and the problem of autonomy. *Notre Dame Journal on Emerging Technologies*, 1, pp. 210-250.
- [15] Dewey, J., 1926. The historic background of corporate legal personality. *The Yale Law Journal*, 35(6), pp. 655-673.
- [16] Diamantis, M., 2019. The extended corporate mind: When corporations use AI to break the law.
- [17] Diamantis, M. E., 2023. Vicarious Liability for AI. *Indiana Law Journal*, 99(1), p. 7.
- [18] Ebers, M., Zou, M. and Poncibò, C., 2022. Contracting and contract law in the age of artificial intelligence.
- [19] Emery-Xu, N., Jordan, R. and Trager, R., 2025. International governance of advancing artificial intelligence. *AI & SOCIETY*, 40(4), pp. 3019-3044.
- [20] Enarsson, T., Enqvist, L. and Naartijävi, M., 2022. Approaching the human in the loop—legal perspectives on hybrid human/algorithmic decision-making in three contexts. *Information & Communications Technology Law*, 31(1), pp. 123-153.
- [21] Faure, M. and Li, S., 2022. Artificial intelligence and (compulsory) insurance. *Journal of European Tort Law*, 13(1), pp. 1-24.
- [22] Friedenberg, J., 2020. *The future of the self: An interdisciplinary approach to personhood and identity in the digital age*. Univ of California Press.
- [23] Griffin, F., 2021. Artificial intelligence and liability in health care.
- [24] Gstrein, O. J., Haleem, N. and Zwitter, A., 2024. General-purpose AI regulation and the European Union AI Act. *Internet Policy Review*, 13(3), pp. 1-26.
- [25] Gupta, R. and Nazir, M., Liability in the Age of AI: Perspectives on Criminal and Civil Responsibility for AI-Induced Harm. In *Artificial Intelligence for Legal System* (pp. 21-35). Chapman and Hall/CRC.
- [26] Hallevy, G., 2015. *Liability for crimes involving artificial intelligence systems* (Vol. 257). New York, NY, USA: Springer International Publishing.
- [27] Hamet, P. and Tremblay, J., 2017. Artificial intelligence in medicine. *Metabolism*, 69, pp. S36-S40.

- [28] Heiss, S., 2021. Towards Optimal Liability for Artificial Intelligence: Lessons from the European Union's Proposals of 2020.
- [29] Hess, A. and Kjeldsen, J. E., 2025. *Ethos, Technology, and AI in Contemporary Society*. Routledge.
- [30] Jackson, P. C., 2019. *Introduction to artificial intelligence*. Courier Dover Publications.
- [31] Khanna, D., 2026. *Governing Intelligence: Strategies for Managing Risk, Compliance, and Trust in the Age of Generative AI*. Geh Press.
- [32] Klabbbers, J., 2017. The concept of legal personality. In *International Legal Personality* (pp. 3-34). Routledge.
- [33] Kretschmer, M., Kretschmer, T., Peukert, A. and Peukert, C., 2023. The risks of risk-based AI regulation: taking liability seriously. *arXiv preprint arXiv: 2311.14684*.
- [34] Kooli, C., 2023. Chatbots in education and research: A critical examination of ethical implications and solutions. *Sustainability*, 15(7), p. 5614.
- [35] Kurki, V. A., 2019. *A theory of legal personhood*. Oxford University Press.
- [36] Lindberg, G., Carrero, I., Mallor, F., Estévez, J., Battaglini, M. and Vinuesa, R., 2023. Autonomous driving: present and emerging trends of technology, ethics, and law. *Handbook on Artificial Intelligence and Transport*, pp. 596-616.
- [37] Magnusson Sjöberg, C., 2019. Legal automation: AI and law revisited. In *Legal tech, smart contracts and blockchain* (pp. 173-187). Singapore: Springer Singapore.
- [38] Mazzini, G. and Bagni, F., 2023. Considerations on the regulation of AI systems in the financial sector by the AI Act. *Frontiers in Artificial Intelligence*, 6, p. 1277544.
- [39] Onoja, M. O., Onyenze, C. C. and Akintoye, A. A., 2025. Cross-border data privacy and AI governance: A comparative study between the UK and the US. *Well Testing Journal*, 34(S3), pp. 345-368.
- [40] Ostmann, F. and Dorobantu, C., 2021. AI in financial services.
- [41] Papakonstantinou, V. and De Hert, P., 2020. Refusing to award legal personality to AI: Why the European Parliament got it wrong. *European Law Blog*, 20.
- [42] Porwal, P. D., 2025. Ethics and Laws: Governing Generative AI's Role in Financial Systems. *Generative Artificial Intelligence in Finance: Large Language Models, Interfaces, and Industry Use Cases to Transform Accounting and Finance Processes*, pp. 283-298.
- [43] Rachum-Twaig, O., 2019. Whose robot is it anyway? Liability for artificial-intelligence-based robots. *University of Illinois Law Review*, 2020.
- [44] Rodrigues, R., 2020. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 4, p. 100005.
- [45] Samuelson, P., 2023. Generative AI meets copyright. *Science*, 381(6654), pp. 158-161.
- [46] Simons, K. W., 2002. Dimensions of negligence in criminal and tort law. *Available at SSRN 323401*.
- [47] Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., Hirschberg, J., Kalyanakrishnan, S., Kamar, E., Kraus, S. and Leyton-Brown, K., 2022. Artificial intelligence and life in 2030: the one-hundred-year study on artificial intelligence. *arXiv preprint arXiv: 2211.06318*.
- [48] Tatineni, S., 2024. *Integrating Artificial Intelligence with DevOps: Advanced Techniques, Predictive Analytics, and Automation for Real-Time Optimisation and Security in Modern Software Development*. Libertatem Media Private Limited.
- [49] Terry, H. T., 1903. Legal duties and rights. *The Yale Law Journal*, 12(4), pp. 185-212.
- [50] Togelius, J., 2024. *Artificial general intelligence*. Mit Press.
- [51] Tulli, S. K. C., 2024. Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *International Journal of Acta Informatica*, 3(1), pp. 35-58.
- [52] Wachter, S., 2024. Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond. *Yale Journal of Law and Technology*, 26(3).
- [53] Wacks, R., 2021. *Understanding jurisprudence: An introduction to legal theory*. Oxford University Press.
- [54] Wallingford, E., 2025. *Liabilities and Modern Artificial Intelligence: A Tri-Phase Model*. Taylor & Francis.
- [55] Wiener, J. B., 2013. The diffusion of regulatory oversight. *The Globalisation of Cost-Benefit Analysis in Environmental Policy*, pp. 123-41.
- [56] Wischmeyer, T., 2019. Artificial intelligence and transparency: opening the black box. In *Regulating artificial intelligence* (pp. 75-101). Cham: Springer International Publishing.