

The Legal Challenges of Regulating Artificial Intelligence in Commercial Transactions

Chineze Hildagard Desmond-Ihekaire, Ph.D, FCARB.

Department of Public and Private Law, Faculty of Law, Federal University Otuoke, Bayelsa State, Nigeria Email: mailme2ng@yahoo.com, desmond-ihekaitech@fuotooke.edu.ng

ABSTRACT

As commerce increasingly integrates digital technologies, Artificial Intelligence (AI) plays a pivotal role in enhancing mercantile efficiency, decision-making, and customer engagement. This paper explores the transformative and far-reaching impact of AI on commercial transactions, emphasizing its growing significance in modern business environments as well as its legal challenges. This study adopted the doctrinal research method, analyzing existing literature and real-world applications to evaluate how AI technologies affect contract formation, performance, and enforcement in commercial settings. Findings indicate that AI systems contribute to faster, more accurate transaction processing, especially through smart contracts and predictive analytics. However, their use also raises legal and ethical concerns, particularly regarding liability, privacy, and contract enforceability when autonomous response systems and automated decision-making technologies are involved. Current legal systems often struggle to keep pace with the rapid development of AI technologies, creating regulatory and legislative gaps. The paper concludes that while AI holds great potential to revolutionize commercial transactions, its adoption must be accompanied by robust legal reforms and governance structures. It recommends that governments should consider drafting AI-specific laws that define liability, standards of care, and operational boundaries for AI systems. These laws must clearly assign responsibility for harms caused by autonomous systems and ensure that legal accountability cannot be evaded due to the complexity of AI decision-making.

Keywords: Artificial Intelligence; Consumer Protection; Digital Contract; Automated Decision making; Challenges.

1. INTRODUCTION

Artificial intelligence (AI)¹ is everywhere¹ and its development, deployment and use is moving forward rapidly and contributing to the global economy and efficiency in concluding transactions across the globe. The rapid integration of Artificial Intelligence (AI) into the commercial sector has ushered in a new era of digital commerce, revolutionizing how businesses operate, negotiate, and conduct transactions. AI technologies are now pivotal in automating customer service, analyzing market data, detecting fraud, managing supply chains, and even executing contracts

¹ M A Boden, *AI: Its Nature and Future* (Oxford University Press, UK 2016).

through smart systems. From AI-powered chatbots to algorithmic trading platforms and intelligent procurement systems, these innovations promise increased efficiency, cost reduction, and enhanced decision-making accuracy.² However, as AI systems become more autonomous and influential in shaping commercial activities, they present profound legal and regulatory challenges that traditional legal frameworks struggle to accommodate.

The rapid advancements in artificial intelligence (AI) have led to an increased need for establishing appropriate regulation. The use of AI has resulted in a range of ethical, legal, and social dilemmas, including new challenges in several areas such as data privacy and protection, employment, economic competition, health care, intellectual property, security and ethical issues particularly in legal profession. At the national and supranational levels, governments are seeking to establish a framework of laws and soft laws to regulate the use of AI in contexts ranging from misinformation and disinformation to the use of AI in warfare and economic competition. Organizations now face an increasing legal responsibility to demonstrate that their AI is used in a way that respects the public's rights and best interests. Furthermore, they need to balance often conflicting needs and expectations towards ensuring fairness, safety, transparency, and privacy.³

At the heart of these challenges is the inherently different nature of AI. Unlike conventional software, many AI systems particularly those based on machine learning are capable of self-improvement and decision-making without direct human input. This independence raises complex questions about legal liability, accountability, contract validity, data privacy, and regulatory oversight. For instance, if an AI system concludes a commercial transaction that results in financial loss or contractual breach, current legal doctrines do not provide clear answers regarding who bears responsibility the developer, the user, or the organization that deployed the AI.⁴ The law, historically based on human agency and intention and fault, is clearly ill-equipped to respond to the decentralized and often opaque functioning of intelligent algorithms.

Further complicating the regulatory landscape is the global, borderless nature of AI-powered commerce. Commercial transactions often involve parties, platforms, and data flows that span multiple jurisdictions, each with its own legal standards, enforcement mechanisms, and regulatory approaches. The lack of harmonized international regulations on AI exacerbates legal uncertainty, particularly in areas such as dispute resolution, taxation, intellectual property, and data sovereignty.⁵ This creates jurisdictional issues especially regarding forum for instituting proceedings in cases of breach.

The lack of appropriate or uniform regulation of AI has several social and economic implications. Autonomous AI agents and systems are capable of making decisions with potential lethality. Furthermore if AI is left unregulated, they may reproduce the human biases and discrimination that are contained in training datasets. In such a scenario, AI agents would become a source of

² E Brynjolfsson and A McAfee, 'The Business of Artificial Intelligence: What it Can—and Cannot—Do for Your Organization' [2017] (7) *Harvard Business Review*, 3-11. <<https://starlab-alliance.com/wp-content/uploads/2017/09/The-Business-of-Artificial-Intelligence.pdf>> accessed 11 May 2025.

³ H Batra, *Regulating Artificial Intelligence: Challenges and Perspectives* <<https://www.linkedin.com/pulse/regulating-artificial-intelligence-challenges-hemant-batra-batra-ejbcc>> accessed 11 May 2025.

⁴ R Calo, 'Robotics and the Lessons of Cyberlaw' [2015] (103)(3) *California Law Review*, 513–563.

⁵ B Wagner, 'Ethics as an Escape from Regulation. From "Ethics-washing" to Ethics-shopping?' in E Bayamlioglu and others, *Being Profiled: Cogitas Ergo Sum. 10 Years of 'Profiling the European Citizen* (Amsterdam: Amsterdam University Press 2018) 84–88.

increasing dis empowerment of already marginalized communities by denying fair access to areas such as health systems, education, and employment both in the present and in the future. These developments have led to an international movement toward the development of ethical principles that should guide the governance and regulation of AI.⁶ The Nigerian Bar Association on its own part have in a communique issued at the end of her Annual General Conference in August 2025 by her president Afam Osigwe SAN stated that notwithstanding the adoption of AI as a legal tool its limitations should be acknowledge. Thus in in paragraph 3.3 LXVII it was stated that “The legal profession must embrace technological tools today to augment legal framework, but caution must be exercised to prevent breaches of confidentiality and violations of ethical standards”.

2. CONCEPTUAL FRAMEWORK

2.1 Artificial Intelligence

The term Artificial intelligence (AI) refers to computer systems capable of performing complex tasks that historically only a human could do, such as reasoning, making decisions, or solving problems.⁷

AI has also been defined as the capability of a computer or machine to imitate human cognitive functions such as learning, reasoning, problem solving, and decision- making⁸. It can also be described as a digital computer or computer-controlled robot that performs tasks commonly performed by humans for instance visual perception, speech, recognition, decision-making, translation and interpretation between languages. Furthermore, Artificial Intelligence (AI) according to Nwakunor⁹ is the computer-controlled robots that think intelligently [like humans. These robots are controlled electronically with the aid of the computer by mimicking the competencies of the human mind. AI keeps records and analyses of every action being made by the user. As a result of innovation in science and technology, AI is used in all facets of life for human development and comfort. For example, in the educational sector, AI is used to teach children who are in playgroup, preparatory and kindergarten classes using robots as teaching aids in the classrooms to impart knowledge to them. Artificial Intelligence, often referred to as the intelligence demonstrated by machines, encompasses a spectrum of technologies that enable systems to perform tasks that traditionally required human intelligence.¹⁰

The OECD’s AI Expert Group conceptualized an AI system as: “A machine-based system that can for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments”.¹¹ IBM however defined AI as: “The capability of a

⁶ Batra (n 2)

⁷ Coursera, ‘What is Artificial Intelligence? Definition, Uses and Types’ <<https://www.coursera.org/articles/what-is-artificial-intelligence#>> accessed 11 May 2025.

⁸ Wikipedia Artificial Intelligence <https://en.wikipedia.org> accessed on 16/05/2026

⁹ J A Nwakunor, ‘Leveraging Artificial Intelligence to Enhance Brand Management’ *The Guardian Newspaper* (29 June, 2021) 3.

¹⁰ K Owebor and others, ‘Multi-criteria Optimisation of Integrated Power Systems for Low-Environmental Impact’ [2022] (44)(2) *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, 3459-3476; R Mouchou and others, ‘Developments in the Application of Nano Materials for Photovoltaic Solar Cell Design, Based on Industry 4.0 Integration Scheme’ in *Advances in Artificial Intelligence, Software and Systems Engineering* (Proceedings of the AHFE 2021 Virtual Conferences on Human Factors in Software and Systems Engineering, Artificial Intelligence and Social Computing, and Energy, July 25- 29, 2021, USA Springer International Publishing) 510-521.

¹¹ OECD, *Artificial Intelligence in Society* (Paris: OECD Publishing, 2019) 785.

computer program to perform tasks or reasoning processes that we usually associate to intelligence in human beings.¹²

2.2 Commercial Transactions

At its core, a commercial transaction refers to the exchange of goods, services, or money between two or more parties for business or trade. These transactions can take various forms, including the sale of goods, provision of services, leasing agreements, and financial transactions, among others. Commercial transactions underpin the functioning of economies worldwide, driving growth, innovation, and prosperity.¹³

There are many forms of commercial transactions, including those that occur between two separate businesses, consumers and businesses, businesses and government entities and between internal divisions of a company to name a few. Commercial transactions can happen on a large scale or small scale. In short, commercial transactions are at the heart of doing business.¹⁴ In the construction of commercial transactions, protection of consumers is at the heart of every regulatory intervention.¹⁵

Commercial transactions serve as the foundation of international trade, facilitating the exchange of goods and services across borders. They enable businesses to access new markets, source materials and products efficiently, and forge mutually beneficial partnerships with suppliers and customers worldwide. By fostering trust, transparency, and accountability, commercial transactions contribute to the smooth functioning of global supply chains and the growth of the global economy.¹⁶

2.3 Smart Contracts

Smart contracts is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform. As discussed further below, the code can either be the sole manifestation of the agreement between the parties or might complement a traditional text-based contract and execute certain provisions, such as transferring funds from Party A to Party B.¹⁷ The code itself is replicated across multiple nodes of a blockchain and, therefore, benefits from the security, permanence and immutability that a blockchain offers. That replication also means that as each new block is added to the blockchain, the code is, in effect, executed. If the parties have indicated, by initiating a transaction, that certain parameters have been met, the code will execute the step triggered by those parameters. If no such transaction has been initiated, the code will not take any steps.¹⁸

The integral components of a smart contract are termed objects. There are essentially three objects in a smart contract – the signatories, who are the parties involved in the smart contracts that use

¹² F Rossi, *Artificial Intelligence: Potential Benefits and Ethical Considerations* (European Parliament Legal Affairs Publication, 2019) 17.

¹³ K Ashraf, 'Understanding the Essence of Commercial Transactions in International Trade', <<https://www.linkedin.com/pulse/understanding-essence-commercial-transactions-trade-kareem-ashraf-vqj8e>> accessed 11 May 2025.

¹⁴ Clayborne & Wagner, 'Commercial Transactions', <<https://claybornewagner.com/commercial-transactions/>> accessed 11 May 2025.

¹⁵ J Campbell and others, 'Consumer Financial Protection' [2011] (25) *Journal of Economic Perspectives*, 1.

¹⁶ Ashraf (n 12)

¹⁷ S D Levi and A B Lipton, 'An Introduction to Smart Contracts and Their Potential and Inherent Limitations', <<https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>> accessed 11 May 2025.

¹⁸ *Ibid.*

digital signatures to approve or disapprove the contractual terms; the subject of the agreement or contract; and the specific terms. Smart contracts incorporate critical tools for bookkeeping and eliminate the possibility of infiltration of accounting records. They also enable shareholders to take part in decision-making in a transparent way. Also, they help in trade clearing, where the funds are transferred once the amounts of trade settlements are calculated.¹⁹

Smart contracts could eliminate the so-called procure-to-pay gaps. When a product arrives and is scanned at a warehouse, a smart contract could immediately trigger requests for the required approvals and once obtained, immediately transfer funds from the buyer to the seller. Sellers would get paid faster and no longer need to engage in dunning, and buyers would reduce their account payable costs. This could impact on working capital requirements and simplify finance operations for both parties. On the enforcement side, a smart contract could be programmed to shut off access to an internet-connected asset if a payment is not received. For example, access to certain content might automatically be denied if payment was not received.²⁰

2.4 Liability

Liability refers to legal responsibility for one's actions or omissions, in particular the responsibility to compensate a third party harmed by those actions. If something goes awry, liability clauses in contracts determine whether it is you or another party who will be held accountable.²¹ For example, who will cover the cost of damages? Who will pay any outstanding debts or compensation? The legal consequences of these actions are collectively known as liability, and the party found liable is often required to make amends by paying damages to the aggrieved party.²²

This liability arises when someone's conduct whether intentional or negligent causes injury, financial loss, or other adverse consequences. In legal terms, "acts" can refer to both affirmative actions (e.g., committing a tort or breach of contract) and failures to act when there is a legal duty to do so (e.g., negligence or omission). The extent of liability depends on the nature of the act, applicable laws, and whether the actions were lawful or unlawful.²³ In the context of AI, liability questions arise when AI systems cause harm or errors in commercial settings, and the law must determine who is responsible. The dearth of laws on who, how and in what circumstances liability will inure on harm caused by the use of AI have posed several challenges in commercial transactions.

2.5 Data Protection

Cambridge Dictionary defines data as "information, especially facts or numbers, collected to be examined and considered and used to help decision-making or information in an electronic form that can be stored and used by a computer."²⁴ Data protection is the practice of safeguarding sensitive information from data loss and corruption. Its goal is to protect data and ensure its availability and compliance with regulatory requirements. An effective data protection strategy does more than simply protect data. It also replicates and restores data in the event of loss or

¹⁹ CFI Team, 'Smart Contracts', <<https://corporatefinanceinstitute.com/resources/valuation/smart-contracts/>> accessed 11 May 2025.

²⁰ Levi and Lipton (n 16)

²¹ S Goundan, 'What Is Liability', <<https://sprintlaw.com.au/articles/what-is-liability/>> accessed 11 May 2025.

²² *Ibid.*

²³ Liability for acts: Overview, definition, and example <<https://www.cobrief.app/resources/legal-glossary/liability-for-acts-overview-definition-and-example/>> accessed 11 May 2025.

²⁴ Cambridge Advanced Learner's Dictionary, *Data* (Cambridge University Press) <<https://dictionary.cambridge.org/dictionary/english/data>> accessed 11 May 2025.

damage. This is because the main principles of data protection are to safeguard data and support data availability. Availability means ensuring users can access data for business operations, even if data is damaged, lost or corrupted, such as in a data breach or malware attack.²⁵

Data protection and privacy is an extension of the fundamental right of citizens to privacy. Section 37 of the 1999 Constitution (as Amended) protects the rights of citizens to their privacy and the privacy of their homes, correspondence, telephone conversations and telegraphic communication.²⁶

3. THE NATURE OF AI IN COMMERCIAL TRANSACTIONS

AI technologies in commerce range from chatbots and virtual assistants to algorithmic trading systems and autonomous procurement tools. These systems often operate with minimal human oversight, making decisions based on vast datasets and pre-programmed objectives. In some cases, AI systems are even authorized to negotiate contracts or execute transactions on behalf of businesses. This automation challenges traditional assumptions about consent, intention, and liability in contractual agreements.²⁷ Commercial contracts can be complex. In today's digital age, AI and automation continue to revolutionize various industries and commercial law is no exception. AI provides enhanced contract analysis and risk management capabilities and its systems can review contracts for potential risks, non-compliance, and inconsistencies. Furthermore, AI-based contract negotiation tools offer a collaborative environment where parties can engage in real-time discussions and secure faster agreement.²⁸

One of the most significant impacts of AI in commercial transactions is in contract analytics and management. AI-powered tools can analyze vast numbers of contracts to extract key information, assess risks, and even suggest optimal terms, significantly reducing the time and cost associated with traditional legal reviews.²⁹ These tools are increasingly being used by legal departments and law firms to streamline operations.

AI is also enhancing customer experience in commercial transactions. Intelligent chatbots and virtual assistants provide real-time support to customers, handle inquiries, and even complete sales. These systems learn from user interactions to deliver increasingly personalized services.³⁰ For example, AI-driven recommendation systems used by e-commerce platforms analyze customer behavior and transaction history to suggest products likely to be purchased. This makes advertising simpler and more effect as the appropriate goods can be offered to those interested in such goods. In commercial sectors, AI is optimising procurement strategies, predicting supply chain disruptions, and automating vendor management. AI-driven analytics enable organizations to negotiate better contracts, identify cost-saving opportunities, and enhance supplier

²⁵ A Badman and M Kosinski, 'What is Data Protection?' <<https://www.ibm.com/think/topics/data-protection>> accessed 11 May 2025.

²⁶ CFRN 1999 (as amended) s 37

²⁷ K Werbach and N Cornell, 'Contracts ex Machina' [2017] (67)(2) *Duke Law Journal*, 313–382.

²⁸ S Jones, 'Embracing Artificial Intelligence in Commercial Contracts Whilst Navigating the Risks', <<https://www.mondaq.com/uk/contracts-and-commercial-law/1365290/embracing-artificial-intelligence-in-commercial-contracts-whilst-navigating-the-risks>> accessed 11 May 2025.

²⁹ H Surden, 'Artificial Intelligence and Law: An Overview' [2019] (35)(4) *Georgia State University Law Review*, 1305–1339.

³⁰ A Kaplan and M Haenlein, 'Siri, Siri, in my hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence' [2019] (62)(1) *Business Horizons*, 15–25.

relationships.³¹ Where AI is optimized consumer satisfaction is achieved through effective communication.

Despite the many benefits, the integration of AI into commercial transactions also raises legal and ethical concerns. Issues of accountability, data privacy, and the enforceability of AI-generated contracts remain unresolved. Especially where the system malfunctions to enter into contemplated transactions.

4. LEGAL CHALLENGES OF REGULATING AI IN COMMERCIAL TRANSACTIONS.

The growing integration of Artificial Intelligence (AI) in commercial transactions presents significant legal challenges, as traditional regulatory frameworks struggle to keep pace with the speed and complexity of AI technologies. These challenges encompass issues of liability, contract enforceability, data privacy, and the opacity of AI decision-making processes.

i. Liability and Accountability

One of the most pressing legal issues is determining who is liable when an AI system causes harm, makes a mistake, or breaches a contract. Traditional tort and contract laws assume a human actor who can be held responsible. In contrast, AI systems operate based on machine learning and often exhibit behavior that is not directly traceable to any single human decision. However, the appointment of AI systems as directors raises questions about their legal personalities and liability.³² For instance, if an AI system executes a transaction based on biased or flawed data, who should bear responsibility the developer, the operator, or the user? Current legal systems generally do not recognize AI entities as having legal person-hood, thus placing liability on the nearest human agent or organization.³³ This creates a legal grey area that can discourage adoption or complicate dispute resolution.

In Nigerian law for instance, only natural persons and juristic persons are competent to sue or be sued. See the case of *Ataguba & Co V Gura Nigeria Ltd*³⁴ where the Supreme Court held as follows “ as a general principle, only natural persons, that is, human beings and artificial person’s such as body corporate are competent to sue or be sued. That is human beings, this includes human beings, companies incorporated under the CAMA and unincorporated associations like registered trade unions and partnerships. See also the case of *Fawehinmi V Nigerian Bar Association (No.2)*³⁵ Where it was held that no action can be brought by or against any party other than a natural person or persons unless such a party has been given by statute, expressly or impliedly, a legal personality. This position has further been given judicial imprimatur by the Supreme Court of Nigeria in *Social -Political Development V Ministry of FCT*³⁶ where it held thus” a non-juristic person cannot sue or be sued”. It should be observed that most laws fixes liability on persons based on fault, negligence and or intention which AI is not capable of forming. Thus, the deployment of AI systems complicates accountability due to involvement of multiple hardware

³¹ A Kaufmann, ‘The Rise of AI in Commercial and Legal Sectors: Opportunities, Challenges, and Risks’ <<https://www.linkedin.com/pulse/rise-ai-commercial-legal-sectors-opportunities-risks-andrew-kaufmann-y5v1e>> accessed 11 May 2025.

³² O C Aduma and N G Ikpeze, ‘Appraisal of the Legal and Ethical Implications of Artificial Intelligence Adoption in Corporate Decision-Making in Nigeria’ [2024] (11)(4) *NAU Journal of Commercial and Property Law*.

³³ R Calo, ‘Robotics and the Lessons of Cyberlaw’ [2015] (103)(3) *California Law Review*, 513–563.

³⁴ (2005)8 NWLR (PT.927) 429 SC

³⁵ (1989)2 NWLR (PT.105) 558

³⁶ (2018) LPELR-45708(SC)

and software development entities, individuals and datasets.³⁷ Determining accountability in AI systems is challenging, as responsibility extends to developers, organizations deploying AI, policymakers and users interacting with A-generated outputs. There is also the issue of giving the right input upon which an AI is expected to provide solution. Therefore, identifying the chain of responsibility and creating frameworks that outline responsibilities and consequences for AI decisions is essential.³⁸

ii. Contract Formation and Smart Contracts

The emergence of smart contracts self-executing agreements written in code has introduced new challenges in contract law. Unlike traditional contracts, smart contracts automatically perform actions when specified conditions are met, with little or no room for human interpretation.

However, legal disputes may arise when a smart contract fails due to a programming error, unexpected outcome, misleading or wrong input or ambiguity in the original terms. Courts are faced with determining whether these coded contracts are legally enforceable and how to interpret the "intent" behind code-driven actions.³⁹ If the courts use the fault principle to determine the issue then liability would be avoided by showing the absence of fault. Who then bears the the burden? It is also impossible to fix intention in cases requiring intention to fix liability. It therefore goes without saying that despite the gains, the rigidity of smart contracts also limits the flexibility often necessary in complex commercial relationships.

Another problem that would be faced by the court is to determine the validity of an unsigned contract entered into by AI. As a general rule an unsigned document is a useless piece of paper and has no evidential value. See the case of *Amaizu V Nzeribe*⁴⁰ where it was held that an unsigned document is a worthless piece of paper and the case of *Uzokwelu V PDP & Ors*⁴¹ where the Court of Appeal held that “An unsigned document is a worthless paper”. However, see the case of *Awolaja V Setrade G.B.V*⁴² .which identified a major exception thus the court held that an unsigned contract may still be binding if parties acted on it and do not dispute it’s existence. However, the issue will be if an AI is capable of forming an intention to create a legal relation and can be held liable for acts done by it. Furthermore, can AI be referred to as a party for the purposes of satisfying the above exception. It is only a clear legislation that can clear this ambiguity and or confer AI a legal personality for the purposes of making it or it’s owner really liable.

iii. Data Protection and Privacy Regulations

The adoption of AI in raises significant data protection and privacy concerns, as AI systems often rely on vast amounts of personal data that must be collected, stored and processed in compliance with the country’s Data Protection Regulation.⁴³ AI systems rely heavily on data particularly personal and financial data to operate effectively. In commercial settings, this reliance raises significant concerns under data protection laws.⁴⁴ Companies that use such AI systems in commercial transactions risk breaching privacy laws and incurring regulatory penalties. Up till

³⁷ A B Brendel and others, ‘Ethical Management of Artificial Intelligence’ [2021] (13)(4) *Sustainability*, 1

³⁸ Aduma and Ikpeze (n 31)S

³⁹ K Werbach and Cornell (n 26)

⁴⁰ (1989) 4NWL (PT.118)755

⁴¹ (2018)LPELR-43737(CA)

⁴² (2002) 4NWL (PT 758)520 at 532

⁴³ A Cavoukian, & J Jonas, ‘Privacy by Design in the Age of Big Data’ <<https://jeffjonas.typepad.com/Privacy-by-Designin-the-Era-of-Big-Data.pdf>> accessed 11 May 2025.

⁴⁴ B Goodman and S Flaxman, ‘European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation’ [2017] (38)(3) *AI Magazine*, 50–57.

the publication of this work there is no system that has been designed to prevent AI from using confidential data obtained in the course of performing its function in other words this has been demonstrated in the likeness or similarity noticed in works that were heavily dependent on AI. Thus, copyright infringement and breach of confidentiality agreements are the bane of AI usage in commercial transactions.

Tensions have already arisen where countries like China impose data localization (requiring data to be stored locally) which can hamper the cross-border data flows AI needs. Meanwhile, at the WTO level, concerns have been raised that such restrictions, though often motivated by privacy or security, could become barriers to trade. Balancing the free flow of data for AI innovation with the protection of personal information is a key issue that international frameworks have yet to resolve.⁴⁵

iv. Bias and Discrimination

AI systems can unintentionally perpetuate existing biases in data, leading to discriminatory outcomes in areas like pricing, credit scoring, and hiring. For example, an AI model used for loan approvals might systematically disadvantage certain demographic groups due to biases in historical data. If the data is incomplete, inaccurate or biased, it can lead to erroneous outcomes, perpetuating and amplifying existing inequalities.⁴⁶

Such outcomes may violate anti-discrimination laws and consumer protection statutes, yet proving that an AI system is responsible for discrimination is legally and technically challenging. Regulators and courts must develop standards for detecting and evaluating algorithmic bias, and businesses must implement safeguards to ensure fairness in automated decision-making.⁴⁷

Thus, it has been warned that over dependence on AI should be curtailed.

v. Jurisdictional Ambiguities and Cross-Border Transactions

AI technologies enable transactions that transcend national borders, complicating the determination of applicable legal jurisdiction. A transaction conducted between two AI systems may involve parties in different countries, with varying contract laws, consumer protection rules, and liability standards. This fragmentation creates uncertainty about which court has authority, what laws govern the transaction, and how judgments can be enforced. Moreover, the lack of harmonized international AI regulations makes it difficult for global companies to ensure compliance across jurisdictions.⁴⁸

When an AI system operates across multiple jurisdictions and causes an error or loss, it is unclear who bears responsibility. Existing international commercial law and contract doctrines were not designed with non-human decision agents in mind, leading to gaps in how to treat AI actions or agreements. Scholars have noted that the rise of AI poses “formidable challenges” to the global trade governance system, yet so far scant attention has been paid to these challenges from the standpoint of international trade law.⁴⁹ There is a risk that outdated rules could leave parties without clear remedies or obligations when AI tools malfunction or make biased decisions in cross-border contexts. For instance, if an algorithmic trading agent enters into an international contract or sets prices collusively without human input, can traditional contract and antitrust laws

⁴⁵ M A Turdialiev, ‘Current Trends in the Application of AI in Cross-Border Commercial Transactions’ [2025] (4)(2) *Journal of Intellectual Property and Human Rights*, 588.

⁴⁶ C O’Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown, 2016)

⁴⁷ S Barocas and A D Selbst, ‘Big Data’s Disparate Impact’ [2016] (104)(3) *California Law Review*, 671–732.

⁴⁸ B Wagner, ‘Ethics as an Escape from Regulation: From Ethics-washing to Ethics-shopping?’ in E Bayamlioglu (eds.), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press, 2018) 84-88.

⁴⁹ Turdialiev (n 38)

adequately address the situation? Current laws may struggle to capture such scenarios, potentially allowing AI-driven outcomes to escape full legal scrutiny.⁵⁰ This situation may create both national and international economic emergencies.

vi. Competitive and Ethical Concerns

AI algorithms can inadvertently facilitate anti-competitive practices – a prominent example being algorithmic collusion. Firms using similar pricing algorithms might end up synchronizing prices without any formal agreement, effectively forming a cartel via code. Competition authorities warn that widespread use of self-learning pricing AI could make it easier to sustain collusion “without any formal agreement or human interaction”. Traditional antitrust law, which requires evidence of an agreement or intent, may not easily reach tacit algorithmic coordination, allowing some AI-driven price-fixing to go unpunished.⁵¹ This is especially so as intention is an element of many criminal offences. On the ethical front, AI systems used in credit scoring, customer targeting, or hiring for international business can unintentionally perpetuate bias or discrimination.⁵²

If an AI model systematically favors or excludes certain groups (e.g. based on gender, ethnicity, nationality or race) in making commercial decisions, it raises human rights and fairness issues. Ensuring algorithmic transparency and non-discrimination in such scenarios is difficult – many AI models are “black boxes” whose decision rationale is not readily explainable. This opacity undermines trust and can complicate legal accountability; as commentators note, without understanding an AI’s decision criteria, affected parties cannot effectively challenge outcomes, impeding their right to due process. These ethical concerns have direct legal implications, from potential liability for discriminatory outcomes to calls for laws mandating AI transparency and explainability in high-stakes commercial uses.⁵³

5. COMPARATIVE ANALYSIS OF THE REGULATION OF ARTIFICIAL INTELLIGENCE IN COMMERCIAL TRANSACTIONS IN NIGERIA AND THE UNITED STATES

5.1 Nigeria

Artificial Intelligence (AI) is transforming industries and societies worldwide, offering innovative solutions while raising significant legal, ethical, and regulatory concerns. In commercial transactions, AI tools are increasingly used for contract formation, customer engagement (e.g., chat-bots), predictive analytics, autonomous systems and market trends in order to identify potentially fraudulent activities and risks.⁵⁴ As nations strive to regulate AI’s development and deployment, Nigeria faces the dual challenge of fostering technological innovation and ensuring adequate regulatory safeguards.⁵⁵

⁵⁰ *Ibid.*

⁵¹ A Ezrachi and M E Stucke, Artificial Intelligence & Collusion: When Computers Inhibit Competition <<https://www.illinoislawreview.org/wp-content/uploads/2017/10/Ezrachi-Stucke.pdf#:~:text=Despite%20similar%20effects%20as%20in,the%20category%20of%20technological%20implementation>> accessed 11 May 2025.

⁵² Turdialiev (n 38)

⁵³ Turdialiev (n 38)

⁵⁴ F Mertens, The Use of Artificial Intelligence in Corporate Decision-making at Board Level: A Preliminary Legal Analysis (Financial Law Institute Working Paper Series, 2023) 1– 30.

⁵⁵ M Aisha, ‘Regulating AI in Nigeria: A Comparative Analysis with Global Frameworks’, <<https://www.linkedin.com/pulse/regulating-ai-nigeria-comparative-analysis-global-aisha-morohunfolasfoff>> accessed 12 May 2025.

Currently, Nigeria does not have a dedicated legal framework for regulating AI. However, several existing laws touch on elements related to AI in commercial transactions. The Nigerian Data Protection Act (NDPA), 2023 regulates the collection and processing of personal data, which is fundamental to AI systems. It introduces principles such as purpose limitation, data minimization, and user consent.⁵⁶ Also, the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 addresses unlawful access and cyber-enabled fraud but lacks provisions targeting AI-generated threats such as algorithmic manipulation or deep fakes.

The Nigerian Companies and Allied Matters Act 2020 (CAMA 2020) while not AI-specific, governs company obligations in contracts and disclosures, which could be indirectly impacted by AI-generated decisions. However, CAMA, which is the primary statute governing companies in Nigeria is still silent on the use of AI in corporate governance. The implication of this is that companies are not legally mandated to develop strategies that would promote AI utilization in corporate operations and board management.⁵⁷

While these efforts mark progress, they fail to provide a comprehensive legal and ethical framework for AI regulation. Hence, the regulation of AI in commercial transactions in Nigeria remains nascent, with limited statutory and institutional frameworks in place to address AI-specific risks such as algorithmic bias, liability, data misuse, and transparency. There lies the dilemma of using a system that our laws did not make provision for.

5.2 United States

The U.S. regulates AI in commerce through a sectoral model, where various agencies oversee specific domains. The Federal Trade Commission (FTC), under the Biden administration, had signaled an aggressive approach to use its existing authority to regulate AI.⁵⁸ The FTC issued a warning to market participants that it may violate the FTC Act to use AI tools that have discriminatory impacts, make claims about AI that are not substantiated, or to deploy AI before taking steps to assess and mitigate risks.⁵⁹ The FTC has already taken enforcement action against various companies that have deceived or otherwise harmed consumers through AI.⁶⁰

The Securities and Exchange Commission (SEC) oversees AI use in algorithmic trading and robo-advising to prevent market manipulation.⁶¹ National AI Initiative Act of 2020, which focused on expanding AI research and development and created the National Artificial Intelligence Initiative Office that is responsible for “overseeing and implementing the US national AI strategy”.⁶² Additionally, the Consumer Financial Protection Bureau (CFPB) has produced guidance, reports, and proposed rules related to the use of AI in certain contexts, mostly related to consumer credit.

⁵⁶ Nigerian Data Protection Act (NDPA), 2023; Aisha (n 48)

⁵⁷ M P Richard, ‘Legal Perspective on the Use of Artificial Intelligence in Corporate Governance in Nigeria: Potentials and Challenges’ [2024] (34)(48) *Journal of Legal Studies*.

⁵⁸ EEOC-CRT-FTC-CFPB, ‘Joint Statement on Enforcement Efforts against Discrimination and Bias in Automated Systems’ <https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf> accessed 12 May 2025.

⁵⁹ Federal Trade Commission, ‘Keep Your AI Claims in Check’, <<https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check>> accessed 12 May 2025.

⁶⁰ Federal Trade Commission, ‘FTC Announces Crackdown on Deceptive AI Claims and Schemes’ <<https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>> accessed 12 May 2025.

⁶¹ A & O Shearman, ‘Zooming in on AI - #5: AI under financial regulations in the U.S., EU and U.K. – a comparative assessment of the current state of play: part 1’, <<https://www.aoshearman.com/en/insights/ao-shearman-on-tech/zooming-in-5-ai-under-financial-regulations-in-the-us-eu-and-uk-a-comparative-assessment-part-1>> accessed 12 May 2025.

⁶² National AI Initiative Act of 2020, <<https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210>> accessed 12 May 2025.

For example, it has issued guidance noting that creditors that use AI or complex algorithms in aspects of the credit decisions must still provide a notice to consumers that discloses the specific reasons for taking adverse action, and that creditors must be able to explain the specific reasons for their credit decisions, including when using AI. The CFPB has also published a report highlighting the potential issues and consumer harm arising from the use of AI chatbots.⁶³

Despite its tradition of minimal regulation, the U.S. has made notable strides in addressing the ethical and societal implications of AI. Recent developments indicate a growing focus on responsible AI use, while balancing the need to foster innovation. Key regulatory initiatives include the Artificial Intelligence Risk Management Framework (AI RMF 1.0) which was released by the National Institute of Standards and Technology (NIST AI RMF 1.0) in January 2023, this framework provides guidelines for managing AI-related risks. It emphasizes transparency, accountability, and risk management to ensure that AI technologies are developed and deployed responsibly.⁶⁴

Another one is the Blueprint for an AI Bill of Rights which outlines five principles to protect individual rights and ensure ethical AI use. That is, preventing harm from AI systems; safeguarding personal data and ensuring transparency; avoiding biases and ensuring fairness; providing clear explanations for AI decisions; and holding developers and users accountable.⁶⁵

Comparison

In Nigeria, AI regulation remains nascent, with no dedicated legal framework specifically targeting AI. Existing laws, such as the Nigerian Data Protection Act (NDPA) 2023, address data privacy but do not comprehensively regulate AI risks like algorithmic bias or liability in AI deployment.⁶⁶ The CAMA 2020 governs corporate obligations but is silent on AI in corporate governance, indicating a substantial regulatory gap.⁶⁷ In contrast, the United States employs a sectoral regulatory model. Agencies like the Federal Trade Commission (FTC) actively interpret and enforce existing laws to oversee AI, especially concerning consumer protection, discrimination, and truthful claims about AI capabilities. The FTC has issued warnings and taken enforcement actions against deceptive AI practices, reflecting a proactive but piecemeal regulatory approach.⁶⁸

Both countries grapple with issues of accountability, liability, and transparency in AI use.⁶⁹ Nigeria faces challenges due to the lack of specific laws on algorithmic bias, AI liability, and transparency, despite existing laws touching indirectly on data privacy and cybercrimes. The document notes that Nigerian law recognizes only natural and juristic persons, complicating accountability for AI harms.

The U.S. addresses liability through an evolving understanding that AI systems, lacking legal person-hood, place responsibility on developers, deployers, or users. The FTC's approach

⁶³ A & O Shearman (n 54)

⁶⁴ F R N Alfiani and F Santiago, A Comparative Analysis of Artificial Intelligence Regulatory Law in Asia, Europe, and America (SHS Web of Conferences, 2024) 204 <https://www.shs-conferences.org/articles/shsconf/pdf/2024/24/shsconf_diges-grace2024_07006.pdf> accessed 12 May 2025.

⁶⁵ *Ibid.*

⁶⁶ Nigerian Data Protection Act (NDPA), 2023; Aisha (n 48)

⁶⁷ Richard (n 50)

⁶⁸ Federal Trade Commission (n 53)

⁶⁹ Alfiani and Santiago (n 57)

emphasizes assessing and mitigating discriminatory impacts and false claims, but comprehensive legislation on AI liability remains under development.

6. CONCLUSION

The pervasiveness of artificial intelligence (AI) is transforming the commercial transactions landscape. Providers across industries are looking to utilize third-party AI tools, or utilize customer data to train AI models, in connection with providing services or implementing use cases proposed by their customers to create efficient and cost savings services. The intellectual property (IP) stakes are heightened, and parties on either side of a transaction will need to carefully leverage agreements to maintain IP rights in their own data, secure IP rights in resulting products, and protect themselves against claims of infringement.

The adoption of AI in commercial transactions and corporate decision-making is inevitable, offering benefits such as improved decision-making, operational efficiency, and risk management. However, it raises significant legal and ethical concerns that must be addressed. To address these concerns, robust legal and regulatory frameworks are essential to guide its implementation and maximize its potential, focusing on accountability, human-centered values, data privacy, confidentiality, transparency, and other critical considerations. Establishing a robust data governance framework is crucial to ensure data quality, accuracy and integrity, addressing bias and fairness in data collection.

The integration of AI into commercial transactions thus offers tremendous potential, but it also poses profound legal challenges. These challenges include issues of liability, contract enforceability, data privacy, discrimination, and determining criminal liability and jurisdiction to entertain matters arising from AI transactions. Existing legal frameworks are often inadequate to address the unique characteristics of AI systems, necessitating innovative regulatory responses. As AI continues to evolve, so too must the legal structures that govern its use in commerce ensuring not just efficiency and innovation, but also accountability and justice.

7. RECOMMENDATIONS

Despite the humongous benefits of AI, it has presented several challenges to the commercial world, thus the following recommendations aim to guide policymakers, legal professionals, and businesses in shaping a coherent and effective regulatory framework to maximize its benefits without causing harm:

- i. The Nigerian government should consider drafting AI-specific laws and code of conduct for use that define liability, standards of care, and operational boundaries for AI systems. These laws must clearly assign responsibility for harms caused by autonomous systems and ensure that legal accountability cannot be evaded due to the complexity of AI decision-making.
- ii. Mandatory disclosure requirements should be implemented for high-risk AI systems used in commercial transactions. Developers and operators must be able to explain, at least in principle, how key decisions are made. This would help meet legal obligations under data protection laws and increase trust among consumers and counter-parties.
- iii. Given the global nature of commercial transactions and AI systems, harmonization of legal standards across jurisdictions is critical. International bodies such as the World Trade Organization, United Nations or regional organizations such as AU and ECOWAS could coordinate efforts to develop treaties or model laws on AI governance, addressing cross-border enforcement, data flows, and dispute resolution.
- iv. Independent auditing of AI systems should be required, especially those used in sectors involving consumer finance, e-commerce, or legal agreements. Certification programs can

- ensure that AI systems meet minimum standards for fairness, security, and compliance with contract and privacy laws.
- v. Businesses must adopt responsible data governance practices, ensuring that AI systems do not rely on biased or incomplete datasets. Regulatory guidelines should promote ethical AI use, requiring impact assessments and bias testing prior to commercial deployment.
 - vi. The criminal liability of AI users should also be defined to avoid escape of criminal liability by pleading non est factum.