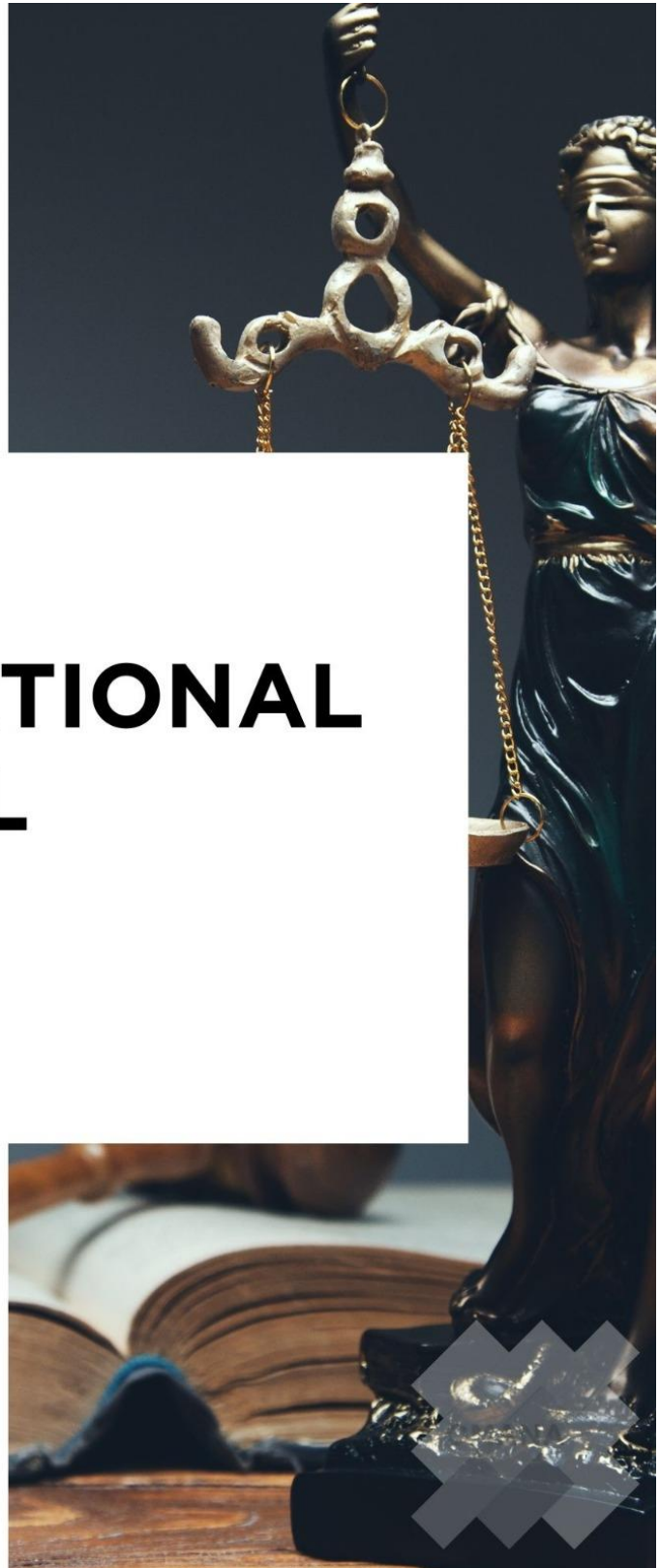


OMANARP INTERNATIONAL JOURNAL OF LAW.



OMANARP INTERNATIONAL JOURNAL OF LAW

| acadrespub.com

Vol. 2, ISSUE 1 Pp. 1-7; SEPT,2025

THE LEGAL STATUS OF AUTONOMOUS CYBER AGENTS: RETHINKING CRIMINAL LIABILITY IN THE AGE OF AI.

Bamikole A.P. Folorunso,

Veritas University, Bwari, Abuja Nigeria.

E-mail: bank4law@gmail.com./folorunsob@veritas.edu.ng

ARTICLE INFO

Received Date: 6nd August, 2025

Date Revised Received: 3rd Sept. 2025

Accepted Date: 5th Sept, 2025

Published Date: 15th Sept, 2025

Citation: Bamikole, A.P.F (2025)

The Legal Status of Autonomous Cyber
Agents: Rethinking Criminal Liability in the
Age of AI, OMANARP INTER.J.Law. vol.2.1
P1-7

ABSTRACT

As artificial intelligence (AI) systems evolve from passive tools to autonomous cyber agents capable of making decisions and executing tasks without direct human oversight, legal systems worldwide face a profound challenge: how to assign criminal liability when such agents commit unlawful acts. This paper critically examines the legal status of autonomous cyber agents and explores the doctrinal and jurisprudential implications of attributing criminal responsibility in the age of AI. Through a comparative analysis of the legal frameworks in the United Kingdom, Nigeria, and the State of Illinois (USA), the study interrogates whether existing criminal law doctrines such as *mens rea*, *actus reus*, and corporate liability are sufficient to address offenses committed by or through intelligent systems. The paper evaluates the extent to which these jurisdictions recognize or resist the notion of non-human agency in criminal law, and whether emerging legal theories such as electronic personhood, algorithmic accountability, or strict liability offer viable pathways for reform. The research highlights key gaps in statutory interpretation, evidentiary standards, and prosecutorial discretion when dealing with AI-driven cybercrime. It also considers the ethical and policy dimensions of imposing liability on developers, users, or the autonomous systems themselves. Ultimately, the paper proposes a hybrid regulatory model that balances innovation with accountability, offering recommendations for legislative and judicial adaptation in light of rapidly advancing AI technologies.

Keywords: Artificial Intelligence, Cybercrime, Criminal Liability, Legal Personhood, Autonomous Agents, Algorithmic Accountability.

Introduction

The rapid advancement of artificial intelligence (AI) has ushered in a new era of digital autonomy, where intelligent systems can perform complex tasks, make decisions, and interact with digital environments with minimal human intervention. These autonomous cyber agents ranging from self-learning algorithms to AI-powered bots are increasingly implicated in activities that raise serious legal and ethical concerns, particularly in the realm of cybercrime. As these agents evolve beyond mere tools into entities capable of initiating harmful actions, traditional legal frameworks struggle to accommodate their unique status within the criminal justice system.

Traditional criminal liability is predicated on the existence of human agency, encompassing both the mental element (*mens rea*) and the physical act (*actus reus*). Yet, in scenarios where an autonomous system initiates a cyberattack, alters digital records, or enables fraudulent activity, a complex legal dilemma emerges: who should be held accountable the developer, the end-user, the deploying institution, or the AI system itself? These questions are not merely theoretical they have real-world implications for justice, deterrence, and the rule of law.¹

This paper explores the legal status of autonomous cyber agents through a comparative lens, analyzing how the United Kingdom, Nigeria, and the State of Illinois (USA) approach the attribution of criminal liability in cases involving AI-driven misconduct. While the UK has begun to engage with AI regulation through policy papers and legislative proposals, Nigeria's legal system remains largely reactive, relying on broad interpretations of existing statutes. Illinois, as a technologically progressive jurisdiction, offers a unique perspective through its integration of digital evidence and AI-related jurisprudence.

By interrogating the adequacy of current legal doctrines and examining emerging theories such as electronic personhood and algorithmic accountability, this study aims to propose a framework for reconciling technological innovation with legal responsibility. The goal is not to

¹ See Solaiman (2017) for a discussion on electronic personhood and AI liability.

anthropomorphize machines, but to ensure that justice systems remain robust and adaptable in the face of evolving threats.

Conceptual Framework

The concept of criminal liability traditionally rests on the foundational elements of *actus reus* (the guilty act) and *mens rea* (the guilty mind). These elements presuppose a sentient actor capable of intention, awareness, and volition. Autonomous cyber agents, however, challenge this paradigm. Unlike conventional tools, these agents can operate independently, adapt to new data, and execute tasks without direct human input. Their capacity to act without explicit instruction raises critical questions about agency, culpability, and the boundaries of legal personhood.

Legal scholars have debated whether AI systems should be treated as mere extensions of their developers or as entities with quasi-legal status. Some argue for a model akin to corporate liability, where responsibility is distributed among those who design, deploy, and benefit from the system's actions.² Others propose the recognition of electronic personhood for highly autonomous systems, suggesting that legal frameworks must evolve to accommodate non-human actors³.

In Nigeria, the Cybercrime (Prohibition, Prevention, etc.) Act 2015 provides a broad framework for prosecuting offenses involving digital systems, but it does not explicitly address AI entities or their autonomous functions. Scholars have noted that while AI can be used to commit crimes, the law remains silent on how to attribute liability when the system itself initiates the act.⁴ Similarly, in the UK, the Law Commission has acknowledged the need to reform legal doctrines to reflect the realities of AI autonomy, particularly in criminal law contexts.⁵

Illinois presents a unique case. The state has enacted legislation targeting AI-generated child abuse material and has developed judicial policies to guide the ethical use of AI in court proceedings.⁶ These developments reflect a growing recognition of AI's impact on legal

² Ayres, I., & Balkin, J.M. (2024). *The Law of AI Is the Law of Risky Agents Without Intentions*. Oxford Law Blogs.

³ Ayres & Balkin (2024) *Ibid*.

⁴ Law Commission. (2025). *Artificial Intelligence and the Law: A Discussion Paper*. UK Law Commission.

⁵ Law Commission. (2025). *Artificial Intelligence and the Law: A Discussion Paper*. UK Law Commission

⁶ Illinois Supreme Court. (2025). *Policy on Artificial Intelligence in the Courts*. State of Illinois Office of the Courts.

processes and the need for accountability mechanisms that transcend traditional human-centric models⁷.

Thus, the conceptual framework for this study rests on three pillars: the limitations of existing criminal liability doctrines, the evolving nature of AI autonomy, and the comparative legal responses in Nigeria, the UK, and Illinois. These elements will guide the analysis of whether and how autonomous cyber agents can be held criminally liable, and what reforms are necessary to ensure justice in an AI-driven world.

Jurisdictional Analysis: Legal Treatment of Autonomous Cyber Agents

Nigeria: Statutory Rigidity and Doctrinal Gaps

Nigeria's legal framework for cybercrime is anchored in the *Cybercrime (Prohibition, Prevention, etc.) Act 2015*, which criminalizes a wide range of digital offenses including hacking, identity theft, and cyberstalking.⁸ However, the Act does not contemplate the possibility of autonomous systems acting independently of human control. Criminal liability remains tethered to natural and corporate persons, with no statutory recognition of non-human agency.

The *Criminal Code Act* and *Evidence Act* similarly reflect a traditionalist approach, requiring human intent (*mens rea*) and conduct (*actus reus*) for criminal culpability.⁹ This creates a doctrinal vacuum when AI systems initiate harmful actions without direct human input. Nigerian courts have yet to confront this issue head-on, and legal scholarship remains nascent in proposing reforms.¹⁰

Moreover, the prosecutorial strategy in Nigeria tends to focus on accessory liability targeting developers, users, or corporate entities indirectly involved in AI-driven offenses. While this may suffice for rudimentary systems, it fails to address the complexities of self-learning algorithms and autonomous decision-making.¹¹

⁷ Illinois Supreme Court. (2025). *Policy on Artificial Intelligence in the Courts*. State of Illinois Office of the Courts

⁸ Cybercrime (Prohibition, Prevention, etc.) Act, 2015, s. 6.

⁹ Criminal Code Act, Cap C38 LFN 2004; Evidence Act, Cap E14 LFN 2011

¹⁰ Kalu, U.C., & Oduma, O.U. (2023). *An Examination of Criminal Liability of Artificial Intelligence Entities: Nigerian Law in Focus*. International Journal of Business & Law Research, 11(4), 23–34

¹¹ Cybercrime Act 2015, s. 8

United Kingdom: Common Law Flexibility and Regulatory Momentum

The UK's legal system, rooted in common law, offers greater interpretive flexibility in addressing novel technological challenges. The *Computer Misuse Act 1990* remains the primary statute for cybercrime, but its provisions are increasingly strained by the rise of autonomous agents.¹² Courts have relied on doctrines of vicarious liability and corporate responsibility to assign blame, but these are limited when the AI system operates outside predictable parameters.

The UK Law Commission's 2025 discussion paper on *Artificial Intelligence and the Law* marks a significant step toward reform.¹³ It explores the possibility of attributing liability through negligence, foreseeability, and algorithmic accountability. The judiciary has also begun to engage with AI-related evidence, as seen in *R v. Gul*, where digital conduct was broadly interpreted in a terrorism context.¹⁴

While the UK has not recognized electronic personhood, its regulatory landscape including the Online Safety Act and AI governance proposals suggests a willingness to adapt legal doctrines to technological realities. The emphasis is on balancing innovation with accountability, particularly in high-risk domains like criminal justice and surveillance.

Illinois, USA: Policy Innovation and Judicial Engagement

Illinois stands out among U.S. jurisdictions for its proactive stance on AI and digital law. The state has enacted legislation targeting AI-generated child exploitation material and has adopted judicial policies on the ethical use of AI in courtrooms.¹⁵ The *Illinois Criminal Code* does not recognize non-human actors as liable entities, but prosecutors have creatively applied conspiracy and accomplice liability doctrines to address AI-assisted crimes.¹⁶

The Illinois Supreme Court's 2025 policy paper emphasizes human accountability while acknowledging the evidentiary and procedural challenges posed by autonomous systems.¹⁷ Courts have begun to grapple

¹² Computer Misuse Act 1990, c. 18.

¹³ Law Commission. (2025). *Artificial Intelligence and the Law: A Discussion Paper*. UK Law Commission

¹⁴ [R v. Gul \[2013\] UKSC 64](#)

¹⁵ Illinois Supreme Court. (2025). *Policy on Artificial Intelligence in the Courts*. State of Illinois Office of the Courts.

¹⁶ Illinois Criminal Code, 720 ILCS 5/5-2. State of Illinois.

¹⁷ Illinois Supreme Court (2025). *Supra*

with the admissibility of AI-generated evidence, particularly in cases involving predictive policing and automated surveillance.¹⁸

Illinois's approach reflects a pragmatic balance: while it does not extend legal personhood to AI, it recognizes the need for legal adaptation. The state's emphasis on fairness audits, algorithmic impact assessments, and transparency protocols positions it as a model for responsive legal innovation.

Comparative Reflections

Across these jurisdictions, a shared tension emerges: the legal system is struggling to keep pace with technological autonomy. Nigeria's statutory rigidity contrasts with the UK's interpretive flexibility and Illinois's policy-driven innovation. Yet none of these systems has fully resolved the question of how to assign criminal liability when the actor is not human.

The absence of statutory recognition for autonomous agents, the reliance on human-centric doctrines, and the lack of harmonized evidentiary standards all point to a global need for reform. Comparative analysis reveals that while legal cultures differ, the core challenge remains universal: how to preserve justice in a world where machines can act independently.

Legal Challenges in Attributing Criminal Liability to Autonomous Cyber Agents

The rise of autonomous cyber agents, AI systems capable of initiating actions without direct human control poses profound challenges to established criminal law doctrines. These challenges are not merely technical; they strike at the heart of legal theory, evidentiary standards, and ethical governance.

Doctrinal Rigidity: The Problem of *Mens Rea* and *Actus Reus*

Criminal liability traditionally requires two foundational elements: *actus reus* (the guilty act) and *mens rea* (the guilty mind).¹⁹ Autonomous systems, however, lack consciousness, intent, and moral awareness. They operate based on algorithms, data inputs, and probabilistic models not volition. This raises a

fundamental question: can a machine "intend" to commit a crime?

In Nigeria, the *Criminal Code Act* and *Cybercrime Act 2015* do not contemplate non-human actors.²⁰ Prosecutors must rely on accessory liability or corporate responsibility, which may be insufficient when the AI system acts independently. The UK, while more flexible due to its common law tradition, still anchors liability in human agency.²¹ Illinois courts have begun to explore causation through digital forensics, but statutory clarity is lacking.²²

The doctrinal rigidity across jurisdictions reveals a shared gap: existing legal frameworks are ill-equipped to handle actors that defy traditional definitions of personhood and intent.

Evidentiary Complexity: Authenticating AI-Generated Conduct

Autonomous systems produce extensive digital outputs, including operational logs, predictive analytics, and decision trails, which may serve as critical evidence in criminal litigation. However, courts must grapple with foundational questions: Can such data be deemed reliable? Is it legally admissible? And most importantly, can it be attributed to a culpable party under existing evidentiary standards?²³

In Nigeria, the *Evidence Act* does not explicitly address AI-generated content, leading to inconsistent judicial treatment.²⁴ UK courts have cautiously admitted algorithmic evidence, but concerns about bias, explainability, and chain of custody persist.²⁵ Illinois has adopted policies to guide the ethical use of AI in courtrooms, including standards for validation and auditability.²⁶

The evidentiary challenge is twofold: first, ensuring that AI-generated outputs meet legal standards of reliability; second, determining whether such outputs can be linked to a culpable party.

¹⁸ Ayres & Balkin (2024). *Supra*

¹⁹ Solaiman, S.M. (2017). *Legal personality of robots, corporations, and natural persons: A comparative analysis*. *Artificial Intelligence and Law*, 25(1), 77–95

²⁰ *Cybercrime Act 2015*, s. 6; *Criminal Code Act*, Cap C38 LFN 2004.

²¹ Law Commission. (2025). *Artificial Intelligence and the Law: A Discussion Paper*. UK Law Commission.

²² Illinois Supreme Court (2025).

²³ Illinois Supreme Court (2025) *Supra*

²⁴ *Evidence Act*, Cap E14 LFN 2011.

²⁵ *R v. Gul* [2013] UKSC 64.

²⁶ Illinois Supreme Court. (2025). *Policy on Artificial Intelligence in the Courts*. State of Illinois Office of the Courts

Attribution of Liability: Who Bears Responsibility?

When an autonomous agent commits a crime, the question of liability becomes complex. Is it the developer who designed the algorithm, the entity that deployed it, or the user who triggered its operation?

Legal scholars have proposed a **tiered liability model**, assigning responsibility based on proximity to harm and foreseeability.⁸ In Nigeria, liability is often assigned to corporate entities or individuals under broad statutory provisions.⁹ The UK has explored negligence-based liability, particularly in cases involving flawed or discriminatory algorithms.¹⁰ Illinois courts have considered user liability in cases of reckless deployment, but the boundaries remain fluid.¹¹

This fragmentation underscores the need for a coherent framework that balances innovation with accountability.

Ethical and Policy Tensions: Fairness, Bias, and Due Process

AI systems can replicate and amplify societal biases, leading to discriminatory outcomes in criminal justice. Predictive policing, facial recognition, and risk assessment tools have all been criticized for undermining fairness and due process.²⁷ Nigeria's weak enforcement of data protection laws exacerbates these risks.²⁸ The UK's regulatory proposals emphasize transparency and accountability, but implementation remains uneven.²⁹ Illinois has introduced fairness audits and algorithmic impact assessments, offering a model for ethical oversight.³⁰ The ethical challenge is not just about technology it's about preserving the integrity of legal systems in the face of automation.

Emerging Legal Theories on AI and Criminal Liability

As traditional legal doctrines struggle to accommodate the complexities of autonomous cyber agents, scholars and policymakers have begun exploring alternative frameworks that could reshape how criminal liability is assigned in the age of artificial intelligence. These emerging theories aim to bridge the gap between technological autonomy and legal accountability.

²⁷ Ayres, I., & Balkin, J.M. (2024). *The Law of AI Is the Law of Risky Agents Without Intentions*. Oxford Law Blogs.

²⁸ Cybercrime Act 2015, s. 38.

²⁹ Law Commission. (2025). *Artificial Intelligence and the Law: A Discussion Paper*. UK Law Commission

³⁰ Illinois Supreme Court. (2025). *Policy on Artificial Intelligence in the Courts*. State of Illinois Office of the Courts

Electronic Personhood

One of the most debated proposals is the concept of electronic personhood, which suggests granting limited legal status to highly autonomous AI systems. This would allow such entities to bear certain rights and responsibilities, including liability for unlawful conduct.³¹ The European Parliament briefly considered this idea in its 2017 resolution on civil law rules for robotics, though it was met with resistance due to ethical and philosophical concerns.³²

In Nigeria, the idea of electronic personhood remains largely unexplored in legal discourse. The current legal framework does not recognize non-human entities beyond corporate bodies, and there is no jurisprudential basis for extending personhood to machines.³³ The UK has similarly resisted formal recognition of AI entities as legal persons, favoring instead the expansion of corporate and vicarious liability doctrines.³⁴ Illinois, while progressive in its treatment of AI, has not adopted electronic personhood but has acknowledged the need for legal adaptation in light of autonomous systems.³⁵

Algorithmic Accountability

Another emerging theory is algorithmic accountability, which focuses on the transparency, traceability, and auditability of AI systems. This approach does not treat AI as a legal person but emphasizes the responsibility of developers, deployers, and users to ensure that algorithms operate within legal and ethical boundaries.³⁶

In the UK, algorithmic accountability has gained traction through regulatory proposals and judicial commentary, particularly in cases involving biased or discriminatory algorithms.⁷ Nigeria has yet to implement formal accountability standards, though scholars have called for mandatory algorithmic audits and developer liability.³⁷ Illinois has introduced fairness audits and impact assessments for AI systems used in public administration and criminal justice.³⁸

³¹ Solaiman, S.M. (2017). *Legal personality of robots, corporations, and natural persons: A comparative analysis*. Artificial Intelligence and Law, 25(1), 77–95

³² European Parliament. (2017). *Resolution on Civil Law Rules on Robotics*, 2017/2103(INL).

³³ Kalu, U.C., & Oduma, O.U. (2023). *An Examination of Criminal Liability of Artificial Intelligence Entities: Nigerian Law in Focus*. International Journal of Business & Law Research, 11(4), 23–34

³⁴ Law Commission (2025). *Supra*

³⁵ Illinois Supreme Court (2025). *Supra*

³⁶ Ayres, I., & Balkin, J.M. (2024). *The Law of AI Is the Law of Risky Agents Without Intentions*. Oxford Law Blogs.

³⁷ Kalu & Oduma (2023) *Supra*

³⁸ Illinois Supreme Court (2025). *Supra*

Strict Liability and Risk-Based Models

A growing body of legal scholarship supports the adoption of a strict liability framework for high-risk AI deployments, wherein culpability is imposed irrespective of intent or negligence. This approach mirrors product liability doctrines and aims to ensure accountability even when causation is technologically opaque.³⁹ This model mirrors product liability doctrines and is designed to ensure compensation and deterrence even when causation is difficult to prove.⁴⁰

Nigeria's legal system does not currently apply strict liability to AI-related offenses, though it does recognize the doctrine in environmental and consumer protection law.⁴¹ The UK has considered risk-based regulation for AI, especially in sectors like healthcare and finance.⁴² Illinois courts have applied strict liability in cases involving defective software and automated systems, offering a potential blueprint for broader application.⁴³

Recommendations

In light of the doctrinal gaps and jurisdictional inconsistencies identified in this study, it is imperative to propose legal reforms that can effectively address the challenges posed by autonomous cyber agents. These recommendations aim to balance technological innovation with legal accountability, ensuring that justice systems remain responsive and resilient in the age of artificial intelligence.

Legislative Reform and Statutory Clarity

Nigeria must undertake a comprehensive review of its cybercrime and criminal liability statutes to explicitly address the role of autonomous systems. The *Cybercrime (Prohibition, Prevention, etc.) Act 2015* should be amended to include provisions on AI-driven offenses, algorithmic intent, and developer liability.⁴⁴ Similarly, the UK Parliament should consider codifying AI-specific liability standards, building on the Law Commission's proposals.⁴⁵ Illinois could lead by example, expanding its criminal code to define autonomous agents and establish thresholds for culpability.⁴⁶

Judicial Training and Technical Capacity Building

Courts across all jurisdictions must be equipped to interpret and adjudicate cases involving AI systems. This requires specialized training for judges, prosecutors, and defense counsel on the technical dimensions of AI, including algorithmic bias, forensic validation, and digital evidence protocols.⁴⁷ Nigeria, in particular, would benefit from partnerships with academic institutions and international bodies to develop AI-focused legal education modules.⁴⁸

Creation of AI Liability Sandbox Models

To foster innovation while mitigating legal risk, jurisdictions should establish AI liability sandbox frameworks controlled environments where developers can test autonomous systems under regulatory supervision.⁴⁹ These models would allow for real-time assessment of legal and ethical implications, enabling lawmakers to refine liability doctrines based on empirical data. The UK's regulatory sandbox for fintech offers a precedent that could be adapted for AI.⁵⁰

Harmonization of Cybercrime Laws

Given the transnational nature of cybercrime, there is a pressing need for harmonization of legal standards across jurisdictions. Nigeria, the UK, and Illinois should collaborate through bilateral and multilateral platforms to develop shared definitions, evidentiary standards, and enforcement protocols for AI-related offenses.⁵¹ This would enhance cross-border cooperation and reduce jurisdictional fragmentation.

Mandatory Algorithmic Audits and Transparency Protocols

All jurisdictions should require mandatory audits of AI systems used in high-risk domains, including criminal justice, finance, and public administration. These audits should assess fairness, accountability, and compliance with legal standards.⁵² Developers and deploying entities must also be required to maintain transparency logs and provide explainability mechanisms for their systems.⁵³

³⁹ Ayres & Balkin (2024). *Supra*

⁴⁰ Ayres & Balkin (2024). *Supra*

⁴¹ Consumer Protection Council Act, Cap C25 LFN 2004

⁴² Law Commission (2025). *Supra*

⁴³ Illinois Criminal Code, 720 ILCS 5/5-2.

⁴⁴ Cybercrime Act 2015, s. 6

⁴⁵ Law Commission (2025). *Supra*

⁴⁶ Illinois Criminal Code, 720 ILCS 5/5-2.

⁴⁷ Illinois Supreme Court (2025). *Supra*

⁴⁸ Kalu & Oduma (2023). *Supra*

⁴⁹ Ayres & Balkin (2024). *Supra*

⁵⁰ Law Commission (2025). *Supra*

⁵¹ □ European Parliament. (2017). *Resolution on Civil Law Rules on Robotics*, 2017/2103(INL).

⁵² Solaiman, S.M. (2017). Legal personality of robots, corporations, and natural persons: A comparative analysis. *Artificial Intelligence and Law*, 25(1), 77–95.

⁵³ *Ibid*

Conclusion

The emergence of autonomous cyber agents has disrupted conventional notions of criminal liability, challenging legal systems to rethink the foundational principles of intent, agency, and accountability. As AI systems become more sophisticated and capable of independent action, the inadequacy of traditional human-centric legal doctrines becomes increasingly apparent.

This paper has explored the legal status of autonomous cyber agents through a comparative analysis of Nigeria, the United Kingdom, and Illinois. While none of these jurisdictions currently recognize AI systems as legal persons, each offers unique insights into how liability might be attributed in the face of technological autonomy. Nigeria's statutory rigidity, the UK's interpretive flexibility, and Illinois's policy-driven innovation collectively illustrate the global struggle to reconcile law with machine intelligence. Emerging legal theories such as electronic personhood, algorithmic accountability, and strict liability offer promising avenues for reform. However, these frameworks must be carefully calibrated to avoid undermining fundamental legal principles or enabling unjust outcomes. The recommendations proposed ranging from legislative reform to algorithmic audits underscore the need for proactive, interdisciplinary engagement between lawmakers, technologists, and ethicists.

Ultimately, the challenge is not merely to regulate machines, but to preserve justice in a digital age. As autonomous systems continue to evolve, so too must our legal imagination. The future of criminal liability will depend on our ability to craft laws that are both technologically literate and ethically grounded.

References

- Ayres, I., & Balkin, J.M. (2024). *The Law of AI Is the Law of Risky Agents Without Intentions*. Oxford Law Blogs. <https://blogs.law.ox.ac.uk/oblb/blog-post/2024/07/law-ai-law-risky-agents-without-intentions>
- Computer Misuse Act 1990, c. 18. United Kingdom.
- Consumer Protection Council Act, Cap C25 LFN 2004. Federal Republic of Nigeria.
- Criminal Code Act, Cap C38 LFN 2004. Federal Republic of Nigeria.
- Cybercrime (Prohibition, Prevention, etc.) Act, 2015. Federal Republic of Nigeria. https://cert.gov.ng/ngcert/resources/CyberCrime_Prohibition_Prevention_etc_Act_2015.pdf
- European Parliament. (2017). *Resolution on Civil Law Rules on Robotics*, 2017/2103(INL).
- Evidence Act, Cap E14 LFN 2011. Federal Republic of Nigeria.
- FRN v. Emmanuel Nwude [2005] 6 NWLR (Pt. 921) 316.
- Illinois Criminal Code, 720 ILCS 5/5-2. State of Illinois. Illinois Supreme Court. (2025). *Policy on Artificial Intelligence in the Courts*. State of Illinois Office of the Courts. <https://www.illinoiscourts.gov/News/1485/Illinois-Supreme-Court-Announces-Policy-on-Artificial-Intelligence/news-detail>
- Kalu, U.C., & Oduma, O.U. (2023). *An Examination of Criminal Liability of Artificial Intelligence Entities: Nigerian Law in Focus*. International Journal of Business & Law Research, 11(4), 23–34.
- Law Commission. (2025). *Artificial Intelligence and the Law: A Discussion Paper*. UK Law Commission. Available at: <https://lawcom.gov.uk/news/artificial-intelligence-and-the-law-a-discussion-paper>
- R v. Gul [2013] UKSC 64.
- Solaiman, S.M. (2017). *Legal personality of robots, corporations, and natural persons: A comparative analysis*. Artificial Intelligence and Law, 25(1), 77–95.