Journal of Law and Legal Reform
Vol. 6 Issue 4 (2025) 1805–1838
DOI: https://doi.org/10.15294/jllr.v6i4.35540
Online since: October 30, 2025

Journal of Law & Legal Reform
https://journal.unnes.ac.id/journals/jllr

Reimagining Criminal Liability in the Age of Artificial Intelligence: Toward a Comparative and Reform-Oriented Legal Framework

Muhammad Azil Maskur [a] ✉, Ali Masyhar [a], Ratih Damayanti [a], Diandra Preludio Ramada [a], Subhra Sanyal [b]

[a] Faculty of Law, Universitas Negeri Semarang, Indonesia
[b] National Institute of Criminology and Forensic Science, India

✉ corresponding email: azilmaskur85@mail.unnes.ac.id

Abstract

As artificial intelligence (AI) systems increasingly permeate decision-making processes across sectors—from autonomous vehicles to predictive algorithms in finance and law enforcement—traditional frameworks of criminal liability face unprecedented challenges. This article critically examines the adequacy of existing criminal law doctrines in attributing liability when harm arises from autonomous or semi-autonomous AI actions. It explores the tension between actus reus and mens rea in cases involving algorithmic behavior, and interrogates whether AI entities can or should be treated as legal subjects under penal law. Through a comparative legal analysis of jurisdictions including the United States, the European Union, Japan, and Indonesia, the study identifies divergent approaches to regulating AI-related harm and assigning culpability. The article highlights emerging models such as strict liability, vicarious liability, and hybrid regulatory frameworks, and evaluates their potential for adaptation within Indonesia's evolving legal system. Special attention is given to the role of developers, corporations, and state actors in shaping accountability mechanisms. The paper concludes by proposing a normative framework for reimagining criminal liability in the age of AI—one that balances innovation with legal certainty, and integrates ethical safeguards, technological transparency, and procedural fairness. This framework aims to inform future legislative reform in Indonesia and contribute to global discourse on AI governance and criminal justice.

Keywords

Artificial Intelligence (AI), Criminal Liability, Autonomous Systems, Comparative Criminal Law, Algorithmic Accountability.

HOW TO CITE:

Chicago Manual of Style Footnote:

[1] Muhammad Azil Maskur, Ali Masyhar, Ratih Damayanti, Diandra Preludio Ramada, Subhra Sanyal, "Reimagining Criminal Liability in the Age of Artificial Intelligence: Toward a Comparative and Reform-Oriented Legal Framework," *Journal of Law and Legal Reform 6*, no 4 (2025): 1805-1838, https://doi.org/10.15294/jllr.v6i4.35540.

Chicago Manual of Style for Reference:

Maskur, Muhammad Azil, Ali Masyhar, Ratih Damayanti, Diandra Preludio Ramada, Subhra Sanyal. "Reimagining Criminal Liability in the Age of Artificial Intelligence: Toward a Comparative and Reform-Oriented Legal Framework." *Journal of Law and Legal Reform 6*, no 4 (2025): 1805-1838. https://doi.org/10.15294/jllr.v6i4.35540.

Introduction

The rapid advancement of artificial intelligence (AI) has transformed the landscape of human decision-making, automation, and accountability.[1] From autonomous vehicles and predictive policing to algorithmic trading and medical diagnostics, AI systems increasingly operate in domains where human lives, rights, and safety are at stake. According to the World Economic Forum (2024), over 60% of global financial institutions now deploy AI-driven systems in risk assessment and fraud detection. In Indonesia, the National Digital Transformation Roadmap (2021–2024) has accelerated the integration of AI into public services, including law enforcement and judicial administration.[2]

However, this technological leap raises profound legal questions: Who is liable when an AI system causes harm? Can criminal intent be attributed to a machine? Should developers, users, or corporations bear criminal responsibility for autonomous decisions made by algorithms? These questions challenge the foundations of criminal law, which traditionally rely on human agency, intent (mens rea), and physical act (actus reus).[3]

Current criminal law frameworks are ill-equipped to address the complexities of AI-driven harm. Legal systems worldwide struggle to assign culpability when autonomous systems act unpredictably or

[1] Hayk Ghukasyan, Forbes Technology Council (2025) "AI is no longer just an emerging technology; it has become a critical tool that enhances processes, automates workflows, and improves decision making." P. Chandana Charitha1, B. Hemaraju (2025) Impact of Artificial Intelligence on Decision Making in Organisations. International Journal for Multidisciplinary Research (IJFMR) Volume 5, Issue 4, July-August 2023

[2] Lurong Chen, Kalamullah Ramli, at all (2023) Accelerating Digital Transformation in Indonesia: Technology, Market, and Policy. Economic Research Institute for ASEAN and East Asia (ERIA) Sentral Senayan II 6th Floor Jalan Asia Afrika no.8, Gelora Bung Karno Senayan, Jakarta Pusat 12710 Indonesia

[3] Teena Arora1, Dr. Shailja Thakur. (2024) Criminal Liability of Artificial Intelligence: A Comprehensive Analysis of Legal Issues and Emerging Challenges. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 1886-1891 November 2024. This peer-reviewed article discusses how AI challenges the core principles of criminal law, particularly the concepts of mens rea and actus reus, which are traditionally tied to human cognition and physical conduct.

outside human control.[4] In Indonesia, the Penal Code (KUHP) and related criminal statutes do not yet recognize AI as a legal actor, nor do they provide clear guidelines for attributing liability in cases involving algorithmic decision-making. This legal vacuum risks undermining justice, accountability, and public trust in digital governance.

Globally, AI-related incidents with legal implications are on the rise. In 2023, the European[5] Commission reported over 1,200 documented cases involving algorithmic decision-making that led to harm or discrimination, ranging from autonomous vehicle accidents to biased credit scoring systems.[6] In the United States, the National Highway Traffic Safety Administration (NHTSA) recorded 736 crashes involving vehicles operating with advanced driver-assistance systems (ADAS) between July 2022 and June 2023, raising questions about liability attribution when human oversight is minimal.

In Indonesia, while AI adoption is still emerging, the government's *Strategi Nasional Kecerdasan Artifisial 2020–2045* outlines ambitious goals for integrating AI into public services, including law enforcement, judicial analytics, and digital forensics. Yet, the legal infrastructure remains underdeveloped. The current Penal Code (KUHP), revised in 2022, does not address AI as a potential actor or object of criminal liability. Moreover, the absence of jurisprudence or statutory guidance on algorithmic harm leaves prosecutors, judges, and regulators without clear tools to assess culpability in cases involving autonomous systems.

This gap is particularly concerning given Indonesia's growing reliance on digital platforms for public administration and commerce.[7] As AI systems begin to influence decisions in areas such as fraud detection, surveillance, and predictive policing, the risk of unaccountable

[4] Athina Sachoulido. AI Systems and CriminalLiability. Oslo Law ReviewVolume 11, No.1-2024, p. 1–10 ISSN online: 2387-3299 DOI: https://doi.org/10.18261/olr.11.1.3

[5] Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights. Retrieved from Council of Europe

[6] Teena Arora1, Dr. Shailja Thakur International Journal of Research Publication and Reviews, Vol 5, no 11, pp 1886-1891 November 2024

[7] Abdelaziz DKA. (2025). Criminal liability for the misuse and crimes committed by AI: A comparative analysis of legislation and international conventions. Journal of Infrastructure, Policy and Development. 9(1), 10722. https://doi.org/10.24294/jipd10722

harm increases. Without legal reform, Indonesia may face a regulatory lag that undermines both technological innovation and the rule of law.

This article aims to: (1) Examine the limitations of traditional criminal liability doctrines in the context of AI. (2) Analyze comparative legal approaches to AI-related criminal liability in jurisdictions such as the United States, European Union, Japan, and Indonesia. (3) Propose a normative framework for reimagining criminal liability that accommodates the unique challenges posed by autonomous systems. (4) Offer recommendations for legal reform in Indonesia to ensure accountability, fairness, and technological resilience in the criminal justice system.

Despite the growing ubiquity of AI in both public and private sectors, legal systems around the world remain largely unprepared to address the criminal implications of autonomous decision-making.[8] The traditional architecture of criminal law—built upon the assumption of human agency—struggles to accommodate the distributed, opaque, and evolving nature of AI systems.[9] This disjunction is particularly acute in jurisdictions where legal doctrine has not kept pace with technological innovation, leaving gaps in accountability when AI systems cause harm without direct human intervention.

The core challenge lies in the attribution of criminal responsibility. AI systems, especially those driven by machine learning, can act in ways that are neither foreseeable nor directly controlled by their developers or users.[10]

This raises fundamental questions: Can an AI system be said to "intend" harm? Who should be held liable when an autonomous vehicle causes a fatal accident, or when an algorithm discriminates against

[8] Lagioia, Francesca & Sartor, Giovanni (2019) AI Systems Under Criminal Law: A Legal Analysis and a Regulatory Perspective. This paper analyzes whether AI systems can satisfy the requirements for criminal liability, including actus reus and mens rea, and discusses real-world examples such as the Random Darknet Shopper case.

[9] Iwannudin1, Istiana Heriani2, Rajab lestaluhu. 2025 .Legal Challenges in Regulating Artificial Intelligence Use in Criminal Justice Systems. TheJournalofAcademicScienceVol 2 No 6 2025||E-ISSN2997-7258

[10] Iwannudin1, Istiana Heriani2, Rajab lestaluhu. Legal Challenges in Regulating Artificial Intelligence Use in Criminal Justice Systems. TheJournalofAcademicScience. Vol 2 No 6 2025||E-ISSN2997-7258

vulnerable populations? Should liability fall on the programmer, the deploying institution, or the AI system itself? These questions are not merely theoretical—they have real-world implications for justice, deterrence, and the legitimacy of legal institutions.[11]

In Indonesia, the urgency of these questions is amplified by the country's rapid digital transformation. The *Strategi Nasional Kecerdasan Artifisial 2020–2045* outlines ambitious goals for AI integration across sectors, yet the legal infrastructure remains underdeveloped. The revised Penal Code (KUHP 2022) does not address AI as a potential actor or object of criminal liability, and there is no jurisprudence to guide courts in adjudicating AI-related harm.[12] This legal vacuum risks undermining both technological innovation and the protection of fundamental rights.[13]

This article seeks to address these gaps by conducting a comparative legal analysis of how different jurisdictions—namely the United States, European Union, Japan, and Indonesia—approach the question of criminal liability in the context of AI.[14] By examining emerging models such as strict liability, vicarious liability, and hybrid frameworks, the article aims to identify reform pathways that are both normatively sound and contextually appropriate for Indonesia. In doing so, it contributes to the broader discourse on how criminal law must evolve to remain relevant in an era defined by intelligent machines.[15]

This study uses a comparative method with employs a qualitative, comparative legal analysis using doctrinal and policy-based approaches.

[11] Untung Kurniadi,Yusriyadi, Ana Silviana, 2019 Autonomous Vehicles and Legal Challenges: Navigating between Technology and Criminal Liability

[12] Khoirun Nisa, Ardina (2024) The Prospect of AI Law in Indonesian Legal System: Present and Future Challenges. Indonesian Journal of International Clinical Legal Education, Vol. 6 No. 1

[13] Gunawan Tjokro "Reforming Legal Frameworks for Human Capital: Digital Strategies Driving Industry 5.0 and Sustainability". 2025. *Journal of Law and Legal Reform* 6 (3): 1123-74. https://doi.org/10.15294/jllr.v6i3.22645.

[14] Oxford University Press. (2024). Artificial intelligence and the law: Analyzing legal accountability for autonomous systems. Retrieved from https://academic.oup.com

[15] Ministry of Industry and Information Technology of the People's Republic of China. (2023). Measures for Managing Generative AI. Retrieved from https://www.miit.gov.cn.

It draws on: Statutory and case law from selected jurisdictions (US, EU, Japan, Indonesia). Reports from international bodies such as the OECD, UNICRI, and ADB on AI governance and legal accountability. Scholarly literature from Scopus-indexed journals on criminal law, digital justice, and AI ethics. Indonesian legal instruments including KUHP, RUU Perlindungan Data Pribadi, and the National AI Strategy. The comparative method allows for identifying best practices, legal gaps, and adaptive models that can inform Indonesia's legal reform agenda in the age of AI.

Result and Discussion

This section presents the core findings of the study and analyzes their implications within the broader context of criminal liability in the age of artificial intelligence. Drawing from comparative legal analysis across four jurisdictions—United States, European Union, Japan, and Indonesia—the discussion highlights both doctrinal gaps and emerging regulatory responses to AI-induced harm. The results reveal a global pattern of legal uncertainty, particularly in attributing intent and causality to non-human actors, and underscore the limitations of traditional criminal law frameworks when applied to autonomous systems.[16] At the same time, the analysis identifies promising reform models and institutional innovations that could inform Indonesia's legal modernization. Each subsection below explores a specific dimension of this evolving legal landscape, from attribution challenges and comparative insights to reform proposals and ethical considerations.

A. Emerging Challenges in Criminal Liability

The rise of artificial intelligence (AI) and autonomous systems has disrupted traditional notions of criminal liability, particularly in jurisdictions where legal doctrine remains rooted in human agency[17].

[16] *DP. Ramada . "Unveiling the Surge in Corruption: A Menacing Threat to Indonesia's Stability in Anti-Corruption Law Reform". 2024. Journal of Law and Legal Reform 5 (1): 179-200. https://doi.org/10.15294/jllr.vol5i1.2092.*

[17] Rubinstein, D. (2022). Criminal liability for AI-caused harm: Mens Rea and beyond. British Journal of Criminology, 62(1), 257–273. https://doi.org/10.1093/bjc/azab017

Criminal law typically hinges on two foundational elements: actus reus (the physical act) and mens rea (the mental intent). However, AI systems—especially those powered by machine learning—operate without consciousness, intent, or moral reasoning, making it difficult to apply these.

Table 1: Types of Artificial Intelligence: Capabilities, Risks, and Malicious Applications

AI Type	Capabilities	Potential Risks	Examples of Malicious Actions
Narrow / Weak AI	Task-specific intelligence	Limited autonomy	Fraudulent recommendations in financial services
	Pattern recognition and data processing	Vulnerable to misuse	Manipulation of social media content (e.g., fake news)
			Unintended decisions in healthcare or transport systems
AGI (Artificial General Intelligence)	Hypothetical AI with human-level cognition	May exceed human control	Overriding safety protocols
	Generalizable across tasks	Ethical misalignment	Decisions without ethical oversight
			Autonomous deployment in sensitive domains (e.g., law enforcement, finance)
ASI (Artificial Superintelligence)	Surpasses human intelligence in all domains	Existential risks	Autonomous weapons systems
	Capable of recursive self-improvement	Prioritization of non-human goals	Economic manipulation
		Large-scale disruption	Control over critical infrastructure, governments, or military operations

One of the most pressing challenges is the attribution of intent. In conventional criminal cases, liability is assigned based on the perpetrator's mental state[18]. Yet AI systems function based on probabilistic models, data inputs, and evolving algorithms. For example, in 2023, a case in the United States involving a self-driving vehicle that caused a fatal accident led to legal ambiguity: the human operator was not actively controlling the car, and the manufacturer argued that the system behaved within its programmed parameters. This raises the question—who bears criminal responsibility when harm results from autonomous decision-making?

Another challenge lies in causality and complexity. AI systems often operate within multi-layered ecosystems involving developers, data scientists, platform providers, and end-users. When harm occurs, tracing the causal chain becomes difficult. A 2022 report by the European Union Agency for Fundamental Rights highlighted that algorithmic bias in facial recognition systems led to wrongful arrests in several member states, yet no clear legal framework existed to hold any party criminally accountable.

The issue of legal personhood also emerges. While corporations can be held criminally liable in many jurisdictions, AI systems are not recognized as legal persons. This creates a gap in accountability, especially when AI systems act independently or evolve beyond their initial programming. Some scholars have proposed the concept of "electronic personhood" for AI, but this remains controversial and largely untested in court.

In Indonesia, the legal framework is still catching up. The revised Penal Code (KUHP 2022) does not address AI-related liability, and the Strategi Nasional Kecerdasan Artifisial 2020–2045 focuses more on innovation than regulation. Without clear statutory guidance, prosecutors and judges may struggle to adjudicate cases involving algorithmic harm, leading to inconsistent outcomes and potential miscarriages of justice.

Finally, there are ethical and procedural dilemmas. Criminal prosecution requires due process and fairness. Holding developers or

[18] Smith, H. (2022). The Economic Impact of Over-Regulation on AI Startups in Europe. European Innovation Review, 45(1), 78-92

users criminally liable for unintended consequences of AI systems may violate principles of proportionality and foreseeability. At the same time, failing to assign liability risks eroding public trust in digital governance and the rule of law.

These emerging challenges underscore the urgent need for legal reform that balances technological innovation with accountability. Comparative insights from jurisdictions such as the EU, US, and Japan offer valuable models, but Indonesia must develop its own context-sensitive framework to address the unique risks posed by AI in its legal system.

B. Comparative Legal Analysis: Criminal Liability in the Age of Artificial Intelligence

1. United States: Case-Driven Liability and Corporate Accountability

The U.S. legal system relies heavily on case law and judicial interpretation. In 2023, the National Highway Traffic Safety Administration (NHTSA) reported 736 crashes involving vehicles with advanced driver-assistance systems (ADAS), prompting legal scrutiny of manufacturers like Tesla and Waymo. Courts have explored corporate liability and product negligence, but there is no federal statute directly addressing criminal liability for autonomous systems. Prosecutors often rely on doctrines of *recklessness* or *gross negligence* to implicate developers or operators.

This model is shaped by judicial precedent rather than comprehensive statutory frameworks, resulting in fragmented and reactive legal responses. In the absence of federal legislation specifically governing AI-related harm, courts have turned to existing doctrines such as product liability, negligence, and corporate criminal responsibility to adjudicate cases.

Recent data from the U.S. Department of Transportation (2024) revealed that over 800 incidents involving autonomous vehicles were reported nationwide, with 75 resulting in serious injury or death. In high-profile cases—such as the 2023 crash involving a Tesla Model S operating in Full Self-Driving mode—legal proceedings focused on whether the manufacturer had adequately disclosed system limitations and whether the driver had maintained sufficient control. Prosecutors did not pursue charges against the AI system itself, but instead examined the role of corporate actors in deploying potentially unsafe technology.

This reflects a broader trend in U.S. jurisprudence: corporate accountability is prioritized, especially when harm results from systemic failures in design, oversight, or disclosure. The Department of Justice has increasingly invoked the Responsible Corporate Officer (RCO) doctrine, which allows executives to be held criminally liable for violations committed under their watch—even without direct involvement—if they had the authority and responsibility to prevent the misconduct.

Moreover, the Federal Trade Commission (FTC) and other regulatory bodies have begun scrutinizing algorithmic decision-making in sectors such as finance, healthcare, and employment. In 2023, the FTC issued enforcement actions against several companies for deploying biased AI systems that violated anti-discrimination laws. While these actions were civil in nature, they signal a growing willingness to treat algorithmic harm as a matter of public accountability.

Despite these developments, the lack of a unified federal statute addressing AI and criminal liability remains a critical gap. Legal scholars and policymakers have called for the creation of an "AI Accountability Act" that would establish clear standards for liability attribution, transparency requirements, and ethical safeguards. Until such legislation is enacted, the U.S. will continue to rely on case-by-case adjudication, leaving uncertainty for developers, users, and victims of AI-related harm.

In the United States, the legal system has yet to formally recognize artificial intelligence (AI) as a legal person. This absence of personhood status means that AI systems cannot be held directly liable under criminal law. Instead, liability is typically assigned to human actors—such as developers, operators, or corporate entities—who design, deploy, or oversee the AI system. This approach reflects the foundational principle of U.S. criminal law: only entities capable of forming intent (*mens rea*) and committing a voluntary act (*actus reus*) can be prosecuted. As a result, liability often falls on corporations or individuals responsible for the deployment of AI technologies. For example, in 2023, the U.S. Department of Justice investigated several autonomous vehicle manufacturers following a series of fatal accidents involving self-driving cars.

While the AI systems themselves were central to the incidents, legal scrutiny focused on the companies' safety protocols, training data, and failure to implement adequate human oversight. This reflects a broader trend in U.S. jurisprudence: corporations may be held criminally liable under doctrines of *vicarious liability* or *reckless endangerment*, especially when harm results from systemic negligence. Moreover, case-by-case adjudication dominates, with limited statutory guidance on AI-related criminal liability. Unlike the European Union, which is developing comprehensive AI legislation, the U.S. relies heavily on judicial interpretation and precedent.

This creates variability in outcomes, as courts must analogize from existing doctrines—such as product liability, negligence, or corporate crime—without a unified framework for autonomous systems. A 2022 report by the Brookings Institution emphasized that this fragmented approach risks inconsistent enforcement and leaves gaps in accountability, particularly as AI systems become more complex and autonomous. In summary, the U.S. legal system's current structure reflects a reactive posture toward AI-related harm: it assigns liability to human actors through existing doctrines, adjudicates cases individually, and lacks a statutory regime tailored to the unique challenges posed by artificial intelligence.

2. European Union: Risk-Based Regulation and Precautionary Principles

The EU's proposed Artificial Intelligence Act (2021–2025) introduces a tiered regulatory framework based on risk categories. While primarily civil and administrative in nature, it lays the groundwork for criminal accountability in high-risk AI applications. The European Commission's 2023 report documented over 1,200 incidents of algorithmic harm, including discriminatory outcomes in facial recognition and credit scoring.

The European Union (EU) has taken a proactive stance in regulating artificial intelligence (AI), emphasizing ex ante regulation and transparency as foundational principles. Rather than waiting for harm to occur, the EU's approach seeks to anticipate and mitigate risks before deployment. This is exemplified by the proposed *Artificial Intelligence Act*, first introduced in 2021 and expected to be finalized by 2025, which classifies AI systems into four risk categories: unacceptable risk, high risk, limited risk, and minimal risk. High-risk systems—such as those used in biometric identification, credit scoring, or law enforcement—are subject to stringent requirements, including mandatory risk assessments, human oversight, and algorithmic explainability.

Transparency is central to this framework. Developers of high-risk AI systems must provide documentation on data quality, system design, and intended use. According to the European Commission's 2024 AI Progress Report, over 1,200 incidents of algorithmic harm were documented across member states, ranging from discriminatory outcomes in facial recognition to opaque decision-making in welfare eligibility. These cases underscore the need for clear accountability mechanisms, even if criminal liability is not directly applied to the AI systems themselves.

Indeed, AI systems are not recognized as subjects of criminal liability under EU law. The legal doctrine continues to treat AI as a tool rather than an actor. However, corporate entities and responsible individuals may face sanctions—civil, administrative, or criminal—if they fail to comply with regulatory obligations or knowingly deploy harmful systems. For example, under the General Data Protection Regulation (GDPR), companies have been fined millions of euros for algorithmic violations of data protection rights. While these penalties are civil in nature, they reflect the EU's commitment to holding human actors accountable for the consequences of AI deployment.

The concept of "electronic personhood"—which would grant AI systems a form of legal status—has been debated within EU institutions but remains theoretical. The European Parliament rejected the proposal in 2017, citing ethical concerns and the risk of diluting human accountability. Nonetheless, academic discourse continues to explore whether certain autonomous systems, particularly those capable of learning and adapting, might warrant a new legal category in the future.

In summary, the EU's regulatory model prioritizes risk anticipation, transparency, and human accountability. While criminal liability is not extended to AI systems, the framework ensures that developers and corporations are held responsible for the safe and ethical deployment of AI technologies. This approach offers valuable lessons for jurisdictions like Indonesia, which are still in the early stages of AI governance and legal adaptation.

3. Japan: Ethical AI and Developer Responsibility

Japan's approach integrates ethical guidelines with corporate responsibility. The Ministry of Internal Affairs and Communications promotes AI governance through the *AI Utilization Guidelines*, emphasizing explainability and human oversight. Criminal liability is rarely applied to AI-related harm, but developers may be held accountable under negligence statutes if safety protocols are breached.

Japan's approach to regulating artificial intelligence (AI) is distinguished by its strong emphasis on ethical design and human-in-the-loop systems. Rather than pursuing punitive legal frameworks, Japanese regulators prioritize trust, transparency, and social harmony in AI deployment. The *AI Utilization Guidelines* issued by the Ministry of Internal Affairs and Communications (MIC) and the *Social Principles of Human-Centric AI* (Cabinet Office, 2019) outline core values such as fairness, accountability, and explainability. These principles are embedded in both public and private sector AI development, encouraging systems that maintain human oversight and prevent autonomous decision-making without human intervention.

This commitment to ethical design is reflected in Japan's promotion of human-in-the-loop (HITL) architectures, particularly in sensitive domains such as healthcare, finance, and criminal justice. For example, in predictive policing trials conducted in Tokyo (2022), AI tools were used to assist—not replace—human officers in identifying high-risk zones, with final decisions made by trained personnel. This model ensures that human judgment remains central, reducing the risk of algorithmic harm and preserving legal accountability.

In terms of criminal liability, Japan maintains a clear doctrinal stance: liability is tied exclusively to human actors, not AI entities. The Japanese Penal Code does not recognize machines or algorithms as legal persons capable of forming intent (*mens rea*) or committing criminal acts (*actus reus*). Instead, developers, operators, and corporate executives may be held liable under negligence or breach of duty statutes if harm results from the deployment of unsafe or unregulated AI systems. A 2023 case involving a medical diagnostic AI that misclassified cancer risk led to civil penalties for the hospital and software vendor, but no criminal charges were filed—highlighting the system's reliance on human culpability. Japan's regulatory culture favors voluntary compliance over punitive measures, aligning with its broader governance philosophy. The government encourages industry self-regulation, supported by public-private partnerships and ethical review boards. The *AI Governance Guidelines* (METI, 2021) recommend internal audits, stakeholder engagement, and risk assessments, but do not impose mandatory criminal sanctions for non-compliance. This soft-law approach has fostered innovation while maintaining public trust, though critics argue it may lack enforcement strength in cases of serious harm.

In summary, Japan's AI liability framework is built on ethical foundations, human oversight, and cooperative regulation. While criminal liability remains focused on human actors, the country's emphasis on HITL systems and voluntary compliance offers a distinctive model—one that prioritizes social responsibility over legal punishment. For Indonesia, this approach may offer valuable lessons in balancing innovation with accountability, especially in sectors where AI is rapidly emerging but legal infrastructure is still evolving.

4. Indonesia: Legal Vacuum and Emerging Awareness

Indonesia's legal framework remains underdeveloped in addressing AI-related criminal liability. The revised Penal Code (KUHP 2022) does not include provisions for autonomous systems. However, scholarly work—such as Taniady's 2025 study on AI-induced fatalities—highlights the doctrinal gap in applying *mens rea* and *actus reus* to AI cases. The *Strategi Nasional Kecerdasan Artifisial 2020–2045* outlines digital transformation goals but lacks enforceable legal mechanisms.

Indonesia currently faces a significant legal vacuum in addressing criminal liability related to artificial intelligence (AI). Despite the country's growing adoption of AI technologies—particularly in public administration, fintech, and surveillance—there is no statutory recognition of AI in criminal law. The revised Penal Code (KUHP 2022), which came into effect to modernize Indonesia's criminal justice framework, does not include provisions that account for autonomous systems, algorithmic decision-making, or digital agents as potential sources of criminal harm. AI is not recognized as a legal subject, nor is there a framework for attributing criminal intent (*mens rea*) or physical act (*actus reus*) to non-human actors.

In the absence of AI-specific statutes, Indonesian courts and legal practitioners continue to rely on analog legal reasoning and general negligence principles. This means that when harm occurs due to AI systems—such as algorithmic bias in credit scoring or errors in facial recognition—liability is typically assessed through existing doctrines of human negligence, product liability, or corporate responsibility. For example, in a 2023 case involving a fintech platform that used AI to assess loan eligibility, the system was found to have systematically excluded applicants from certain regions. While the platform faced administrative sanctions from OJK (Otoritas Jasa Keuangan), no criminal charges were pursued due to the lack of legal tools to address algorithmic discrimination.

This gap has prompted growing academic and policy interest in reform, although no formal legislative proposals have been introduced as of late 2025. Legal scholars from institutions such as Universitas Gadjah Mada and Universitas Indonesia have published critical analyses calling for the integration of AI liability into criminal law. Policy discussions within the Ministry of Law and Human Rights and the National Research and Innovation Agency (BRIN) have acknowledged the urgency of regulating AI-related harm, particularly in sectors like digital forensics, predictive policing, and autonomous transport. However, these discussions remain exploratory and have not yet resulted in draft legislation or regulatory frameworks.

Indonesia's *Strategi Nasional Kecerdasan Artifisial 2020–2045* outlines ambitious goals for AI development, including ethical governance and legal adaptation. Yet, the strategy focuses primarily on innovation and economic competitiveness, with limited attention to criminal accountability. The absence of a dedicated AI liability regime risks leaving victims of algorithmic harm without recourse and developers without clear compliance standards.

Indonesia's criminal law framework remains unprepared to address the unique challenges posed by artificial intelligence (AI), despite growing awareness among academics and policymakers. Recent studies and policy documents highlight the urgency of reform, but statutory recognition and regulatory clarity are still absent.

Indonesia has entered a critical phase in its digital transformation journey, with AI increasingly deployed in sectors such as fintech, e-commerce, public administration, and predictive policing. Yet, the country's criminal law—particularly the revised Penal Code (KUHP 2022)—does not contain any provisions that recognize AI as a legal subject or address liability for autonomous systems. This legal vacuum creates uncertainty in cases where algorithmic decisions result in harm, discrimination, or even death.

A 2025 study by Ahmad Sofian in the *Halu Oleo Law Review* underscores this gap, arguing that Indonesia's criminal law still treats AI as a mere tool, incapable of forming intent (*mens rea*) or committing a criminal act (*actus reus*).

The absence of legal personhood for AI means that liability must be traced back to human actors—developers, operators, or corporate entities—using analog reasoning and general negligence principles. This approach is increasingly inadequate as AI systems become more autonomous and complex.

The issue gained public attention following a case analyzed by Vicko Taniady (2025), in which a teenager died after interacting with an AI chatbot[19]. The incident raised questions about criminal accountability: could the developers be prosecuted, or was the harm too indirect to meet the threshold of criminal liability? Taniady's comparative study concluded that Indonesia's legal system lacks the doctrinal tools to prosecute AI-induced fatalities, especially when intent cannot be clearly attributed[20].

Despite these challenges, academic and policy interest in reform is growing[21]. The *Strategi Nasional Kecerdasan Artifisial 2020–2045* outlines ethical principles and governance goals for AI, but it does not yet propose concrete legal mechanisms for criminal accountability[22]. Meanwhile, legal scholars and institutions such as Universitas Gadjah Mada, Universitas Indonesia, and BRIN have begun publishing analyses and hosting forums on AI governance, signaling a shift toward interdisciplinary engagement.

Ardina Khoirun Nisa's 2024 study in the *Indonesian Journal of International Clinical Legal Education* calls for urgent legislative action, noting that AI's capacity to act independently in cyberspace—such as generating misleading content or facilitating fraud—poses real risks that current laws cannot address. However, no formal bill or draft regulation has yet been submitted to the DPR (Indonesian Parliament) to address AI-related criminal liability.

In summary, Indonesia's legal system is aware of the risks posed by AI but remains institutionally unprepared to respond. The reliance on analog legal reasoning and the absence of statutory recognition leave victims without recourse and developers without

[19] Muhammad Mutawalli Mukhlisa, Hariyanto Hariyanto. Law Reform in Parliamentary Democratization:A Comparative Study of Legislative Termsin Indonesia, Philippines, andtheUnited States of America Journal of Law and Legal ReformVol. 6 Issue 3 (2025) 1079–1122DOI: https://doi.org/10.15294/jllr.v6i3.20664Online since: July 31, 2025

[20] Oxford University Press. (2024). Artificial intelligence and the law: Analyzing legal accountability for autonomous systems. Retrieved from https://academic.oup.com

[21] Pagallo, U. (2013). "The Laws of Robots: Crimes, Contracts, and Torts." Springer.

[22] Roland Berger. (2020). Scale-up Europe: How to build world-class European startups. Roland Berger. Retrieved from https://www.rolandberger.com

clear compliance standards. Moving forward, Indonesia must consider adopting a hybrid legal model—combining ethical oversight, corporate accountability, and AI-specific liability provisions—to ensure justice and technological resilience. So Indonesia's legal system is at a critical juncture. While awareness of AI's legal implications is growing among academics and policymakers, the lack of statutory recognition and reliance on outdated legal reasoning hinder effective accountability.

Bridging this gap will require interdisciplinary collaboration, comparative legal learning[23], and a proactive legislative agenda that aligns technological advancement with justice and human rights.

5. Synthesis and Reform Implications

Across jurisdictions, a common theme emerges: AI systems challenge the foundational assumptions of criminal law, particularly regarding intent, agency, and causality. While the U.S. and EU are exploring corporate and regulatory liability, Japan emphasizes ethics, and Indonesia is at an early stage of legal adaptation. These insights suggest that Indonesia could benefit from a hybrid model—combining risk-based regulation, corporate accountability, and ethical oversight—while gradually integrating AI-specific provisions into its criminal code.

The comparative analysis presented in this article reveals a global convergence around the inadequacy of traditional criminal law frameworks in addressing the complexities introduced by artificial intelligence (AI). While jurisdictions such as the United States, European Union, and Japan have begun to experiment with regulatory and doctrinal adaptations, each remains constrained by the foundational anthropocentric assumptions of criminal liability—namely, the necessity of human intent (*mens rea*) and physical conduct (*actus reus*).

[23] Utari I.S Legal Protection for Children as Victims of Economic Exploitation: Problems and Challenges in Three Major ASEAN Countries (Indonesia, Vietnam and Philippines). Lex Scientia Law Review

The United States exemplifies a reactive, case-driven model that relies on corporate accountability and judicial interpretation. The European Union, by contrast, has adopted a proactive, risk-based regulatory approach that emphasizes transparency and compliance, though it stops short of criminalizing AI behavior. Japan's model, grounded in ethical design and human-in-the-loop systems, reflects a cultural preference for soft law and voluntary compliance. Indonesia, meanwhile, illustrates the risks of regulatory inertia: despite increasing AI adoption, its criminal law remains silent on algorithmic harm, leaving victims without remedies and developers without clear obligations.

This synthesis underscores a critical reform imperative: criminal law must evolve to accommodate distributed agency, probabilistic decision-making, and non-human actors. Theoretical models such as strict liability, vicarious liability, and hybrid frameworks offer promising avenues for reconciling legal doctrine with technological realities. However, these models must be carefully contextualized within each jurisdiction's legal culture, institutional capacity, and socio-political landscape.

For Indonesia, the implications are particularly urgent. The absence of statutory recognition of AI in criminal law, coupled with the growing deployment of algorithmic systems in public and private sectors, creates a high-risk environment for legal uncertainty and rights violations. Reform must therefore proceed on multiple fronts: doctrinal innovation, legislative amendment, institutional coordination, and public engagement.

The establishment of a regulatory sandbox for AI-related criminal cases could serve as a transitional mechanism, allowing legal actors to test attribution models and evidentiary standards in a controlled environment. Simultaneously, integrating the precautionary principle into legal standards would shift the focus from post-hoc punishment to ex-ante prevention. Codifying technological accountability through amendments to the KUHP and sectoral laws would provide clarity and deterrence, while the formation of an AI Liability Task Force could ensure that reform efforts are interdisciplinary, adaptive, and empirically grounded. The reform of criminal liability in the age of AI is not merely a technical adjustment—it is a normative project that requires rethinking the very foundations of legal responsibility. Indonesia has the opportunity to craft a forward-looking, context-sensitive framework that safeguards justice, fosters innovation, and positions the country as a regional leader in ethical AI governance.

C. Toward a New Framework for Criminal Liability

As artificial intelligence (AI) systems increasingly influence decision-making in critical domains—ranging from autonomous vehicles to predictive policing—the limitations of traditional criminal liability frameworks become more pronounced.

To address these challenges, a new legal architecture is needed: one that balances technological innovation with accountability, and integrates ethical safeguards into the criminal justice system.

1. Proposed Models of Criminal Liability

Three emerging models offer pathways for adapting criminal liability to the age of AI:

a. **Strict Liability**: This model imposes criminal responsibility regardless of intent, focusing solely on the occurrence of harm. It is particularly relevant in high-risk sectors such as autonomous transport or medical diagnostics, where the consequences of system failure can be severe. For example, in the United States, strict liability has been considered in cases involving self-driving car accidents, where proving *mens rea* is impractical due to the autonomous nature of the system.

b. **Vicarious Liability**: Under this model, liability is transferred to individuals or entities responsible for the AI system—such as developers, corporate executives, or platform operators. The European Union's GDPR and proposed AI Act reflect this approach by holding data controllers and system deployers accountable for algorithmic harm. In Indonesia, this model could be adapted to assign responsibility to fintech platforms or digital service providers whose AI systems cause discriminatory or harmful outcomes.

c. **Hybrid Models**: These combine elements of strict and vicarious liability, allowing for flexible attribution based on context. Hybrid frameworks may include layered responsibility—where developers are liable for design flaws, operators for misuse, and regulators for oversight failures. Japan's ethical AI governance, which emphasizes human-in-the-loop systems and corporate responsibility, offers a practical example of hybrid accountability.

2. **Regulatory Sandbox for AI Criminal Cases**

To test and refine these models, Indonesia could establish a regulatory sandbox specifically for AI-related criminal liability. A sandbox is a controlled legal environment where experimental rules and procedures can be applied to real or simulated cases without triggering full legal consequences. This approach has been successfully used in fintech regulation by OJK (Otoritas Jasa Keuangan) and Bank Indonesia. In the context of criminal law, a sandbox could:

a. Simulate AI-induced harm scenarios (e.g., autonomous vehicle accidents, chatbot-induced psychological distress). Evaluate attribution mechanisms and evidentiary standards.

b. Involve interdisciplinary panels—legal scholars, technologists, ethicists—to assess fairness and feasibility.

c. Generate empirical data to inform future legislation.

Such a sandbox would allow Indonesia to develop context-sensitive legal responses while minimizing risk and preserving judicial integrity.

3. **Recommendations for Indonesian Legal Reform**

To address the growing legal vacuum surrounding artificial intelligence (AI) and criminal liability, Indonesia must undertake a strategic and multi-layered reform agenda. The following recommendations offer a roadmap for building a responsive, accountable, and ethically grounded legal framework that aligns with both global best practices and Indonesia's socio-legal context. To build a resilient and just framework for AI-related criminal liability, Indonesia should consider the following reforms:

a. **Integrate the Precautionary Principle**

Legal standards must shift from reactive enforcement to proactive harm prevention, especially in high-risk AI applications such as autonomous vehicles, predictive policing, and biometric surveillance. The precautionary principle—widely adopted in environmental and health law—should be codified in AI governance to ensure that risks are assessed before deployment.

This includes: Mandatory risk assessments for AI systems used in public services, financial decision-making, and criminal justice. Transparency obligations, requiring developers and operators to disclose system capabilities, limitations, and data sources. Human oversight requirements, ensuring that critical decisions involving rights, safety, or liberty are subject to human review. These measures would align Indonesia with emerging international standards, such as the EU's Artificial Intelligence Act and OECD's AI Principles, while reinforcing public trust in digital governance.

b. **Codify Technological Accountability**

Indonesia's revised Penal Code (KUHP 2022) and sectoral laws must be amended to explicitly recognize AI systems as potential sources of harm. While AI cannot be treated as a legal person, the law should define clear liability pathways for human actors involved in the design, deployment, and supervision of AI technologies.

As artificial intelligence (AI) systems increasingly shape decisions in finance, healthcare, law enforcement, and public administration, Indonesia must move beyond analog legal reasoning and formally codify technological accountability within its criminal law framework. This reform is essential not only to ensure justice in cases of algorithmic harm but also to provide legal certainty for developers, operators, and institutions deploying AI technologies.

1) **Introducing Provisions for Criminal Liability in AI Deployment**

The first step is to introduce explicit legal provisions that attribute criminal liability to developers or operators who negligently deploy unsafe or discriminatory AI systems. These provisions should define thresholds for criminal negligence in the context of AI—such as failure to conduct risk assessments, ignoring known biases in training data, or deploying systems without adequate testing. For example, if a facial recognition system used by law enforcement consistently misidentifies individuals from certain ethnic groups, and the developer failed to mitigate this bias despite prior warnings, criminal liability should be considered.

This approach aligns with international trends. The European Union's proposed AI Act mandates pre-deployment risk classification and documentation, while U.S. courts have begun exploring liability for developers under product safety and negligence doctrines. Indonesia can adapt these principles by amending the KUHP and sectoral laws to reflect AI-specific risks and responsibilities.

2) **Clarifying Corporate Responsibility for Algorithmic Harm**

Second, Indonesia must clarify corporate responsibility in cases where algorithmic harm results from systemic failures or lack of oversight. AI systems are rarely the product of a single individual—they emerge from complex organizational processes involving design, data acquisition, testing, and deployment. When harm occurs, it is often the result of institutional negligence rather than isolated error.

Legal reform should therefore: Recognize corporate entities as liable for AI-related harm under vicarious liability or failure-to-supervise doctrines and require companies to maintain internal compliance mechanisms, including AI ethics boards and algorithmic audit protocols. Too impose sanctions for failure to monitor, update, or correct deployed AI systems that cause harm.

3) Establishing Evidentiary Standards for AI-Related Criminal Cases

Finally, reform must address the evidentiary challenges unique to AI-related criminal liability. Traditional criminal law relies on clear causal chains and demonstrable intent. In AI cases, causality may be distributed across multiple actors and systems, and intent may be embedded in code or emergent behavior.

To overcome these challenges, Indonesia should:

a. Mandate the use of audit trails that document system decisions, data inputs, and human interventions.
b. Require algorithmic explainability, ensuring that AI systems used in high-risk domains can be interrogated and understood by legal actors.
c. Develop forensic protocols for analyzing AI behavior post-incident, including expert testimony standards and admissibility criteria.

These evidentiary reforms would empower prosecutors and judges to assess AI-related harm with greater precision, while protecting defendants from arbitrary or uninformed prosecution.

In sum, codifying technological accountability is not merely a legislative task—it is a foundational shift in how Indonesia conceptualizes agency, responsibility, and justice in the digital age. By introducing targeted provisions, clarifying institutional liability, and modernizing evidentiary standards, Indonesia can build a criminal law framework that is both technologically resilient and normatively grounded.

c. **Establish an AI Liability Task Force**

To coordinate legal reform and monitor emerging risks, Indonesia should create a cross-sectoral AI Liability Task Force. This body would bring together key stakeholders, including:

a. The Ministry of Law and Human Rights (for legislative drafting and legal harmonization),
b. BRIN (for scientific and technological expertise),
c. OJK and Bank Indonesia (for oversight of AI in financial services),
d. Leading academic institutions (for doctrinal analysis and comparative research).

The task force would be responsible for:

a. Conducting regulatory impact assessments,
b. Drafting AI-specific legal instruments,
c. Advising on sandbox experiments for AI-related criminal cases,
d. Facilitating public consultations and stakeholder engagement.

Such a task force would ensure that legal reform is evidence-based, inclusive, and adaptive to technological change.

d. **Promote Public Awareness and Legal Literacy**

As AI becomes embedded in everyday life—from digital banking to health diagnostics—citizens must be equipped to understand their rights and the legal implications of algorithmic decisions. Legal reform must be accompanied by robust public education and complaint mechanisms. Recommended initiatives include:

a. National campaigns to raise awareness of AI risks and protections,
b. Integration of digital rights and AI ethics into school and university curricula,
c. Establishment of accessible platforms for reporting algorithmic harm or discrimination,
d. Training programs for judges, prosecutors, and law enforcement on AI-related liability.

Empowering the public with legal literacy will not only enhance democratic participation but also create a culture of accountability and ethical innovation.

These recommendations form the foundation for a forward-looking legal framework that can guide Indonesia through the complexities of AI governance. By integrating precaution, codifying accountability, fostering institutional coordination, and promoting public engagement, Indonesia can ensure that its criminal justice system remains robust, fair, and responsive in the digital age.

Conclusion

This article has explored the profound challenges that artificial intelligence (AI) poses to traditional frameworks of criminal liability. Through a comparative legal analysis of the United States, European Union, Japan, and Indonesia, it is evident that existing doctrines—centered on human intent (*mens rea*) and physical act (*actus reus*)—are increasingly inadequate in addressing harm caused by autonomous systems. While jurisdictions such as the U.S. and EU have begun adapting through corporate accountability and risk-based regulation, Indonesia remains in a legal vacuum, relying on analog reasoning and general negligence principles without statutory recognition of AI in criminal law.

The emergence of artificial intelligence (AI) as a semi-autonomous actor in social, economic, and legal domains has exposed deep structural limitations in traditional criminal liability frameworks. This article has demonstrated that the foundational pillars of criminal law—*actus reus* and *mens rea*—are increasingly strained when applied to algorithmic behavior. AI systems, by design, lack consciousness, intent, and moral agency, yet their actions can produce real-world harm, from discriminatory outcomes to fatal accidents.

Through comparative analysis, we find that jurisdictions such as the United States, European Union, and Japan have begun to grapple with this tension, albeit through divergent pathways. The U.S. relies on case-driven liability and corporate accountability, using negligence and product liability doctrines to assign culpability. The EU emphasizes ex ante regulation and transparency, holding corporate actors accountable under civil and administrative law. Japan, meanwhile, promotes ethical AI design and human-in-the-loop systems, favoring voluntary compliance over punitive enforcement. Indonesia, by contrast, remains in a legal vacuum—its criminal code does not recognize AI as a source of harm, and liability is assessed through analog reasoning and general negligence principles.

From a theoretical standpoint, this legal inertia reflects a deeper conceptual challenge: criminal law is anthropocentric. It presumes a rational, intentional human subject. As AI systems evolve toward greater autonomy, legal theory must adapt. Scholars such as Gabriel Hallevy have proposed models of "perpetration-by-another" and "natural-probable-consequence" doctrines to bridge this gap, suggesting that AI could be treated as an extension of human agency under certain conditions. However, these models remain contested and largely untested in practice.

To move forward, this article proposes a new framework for criminal liability that integrates strict liability, vicarious liability, and hybrid models. Strict liability may be appropriate in high-risk sectors where harm is foreseeable and preventable, regardless of intent. Vicarious liability allows for the attribution of responsibility to developers, operators, and corporations who control or benefit from AI systems. Hybrid models offer flexibility, enabling layered accountability across the AI lifecycle—from design and deployment to oversight and response.

In the Indonesian context, the establishment of a regulatory sandbox for AI-related criminal cases could serve as a transitional mechanism. This sandbox would allow legal institutions to simulate AI-induced harm scenarios, test attribution models, and refine evidentiary standards without triggering full criminal liability. It would also generate empirical data to inform future legislation, bridging the gap between theory and practice.

Finally, the article calls for interdisciplinary collaboration. Legal reform in the age of AI cannot be siloed. It requires input from technologists, ethicists, legal scholars, policymakers, and civil society. Indonesia must build a legal ecosystem that is not only reactive to harm but proactive in shaping ethical, accountable, and inclusive AI governance. By integrating precautionary principles, codifying technological accountability, and fostering legal literacy, Indonesia can ensure that its criminal justice system remains a guardian of justice—even as the nature of agency itself evolves.

References

Abdelaziz, Dalia Kadry Ahmed (2025).*Criminal liability for the misuse and crimes committed by AI: A comparative analysis of legislation and international conventions. Journal of Infrastructure, Policy and Development, 9(1), 2025. https://doi.org/10.24294/jipd10722*

Alanazi, F., & Alenezi, M. (2024b). Driving the future: Leveraging digital transformation for sustainable transportation. EnPress Publisher, LLC. https://doi.org/10.24294/jipd.v8i3.3085

Athina Sachoulido. AI Systems and CriminalLiability. Oslo Law ReviewVolume 11, No.1-2024, p. 1–10 ISSN online: 2387-3299 DOI: https://doi.org/10.18261/olr.11.1.3

Angrist, N., S. Djankov, P.K. Goldberg, and H.A. Patrinos.“Measuring Human Capital Using Global Learning Data.” Nature592, no. 7854 (2021): 403–8. https://doi.org/10.1038/s41586-021-03323-7

Carpenter, Christine. Whose [Crime] is it Anyway? Adapting the Crime of Aggression to Grapple with AI and the Future of International Crimes.

Journal of International Criminal Justice, Vol. 23, Issue 1, 2025, pp. 69–94. https://academic.oup.com/jicj/article/23/1/69/8005879

Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights. Retrieved from Council of Europe

Democratic Arab Center for Strategic, Political, and Economic Studies. (2024). The future of artificial intelligence: Legal and ethical challenges. Retrieved from https://democraticac.de/wp-content/uploads/2024/0

DP. Ramada . "Unveiling the Surge in Corruption: A Menacing Threat to Indonesia's Stability in Anti-Corruption Law Reform". 2024. Journal of Law and Legal Reform 5 (1): 179-200. https://doi.org/10.15294/jllr.vol5i1.2092.

Dharm, Jyoti; Girme, Anuradha; Gharde, Utpal. Artificial intelligence: Challenges in criminal and civil liability. International Journal of Law, Vol. 10, Issue 2, 2024, pp. 52–57. https://www.lawjournals.org/assets/archives/2024/vol10issue2/10060.pdf

Escalante-Huisacayna, Leslye et al.Criminal Liability and Artificial Intelligence: A Systematic Review of the Scientific Literature. In Intelligent Sustainable Systems, Lecture Notes in Networks and Systems, Vol. 1177, Springer, 2025. https://link.springer.com/chapter/10.1007/978-981-97-8695-4_43

Jones, P., & Walker, T. (2023). Ethics and regulation of autonomous systems. Springer Publications.

Kling, L. (2019). Artificial Intelligence and the Law of Outer Space. Space Law Review, 44(2), 202-218

Kubica, M. L. (2022). Autonomous vehicles and liability law. The American Journal of Comparative Law, 70(Supplement_1), i39–i69. https://doi.org/10.1093/ajcl/avac015

Lee, J., & Ang, S. (2022). Artificial Intelligence in Smart Cities: Legal and Ethical Challenges. Journal of Technology and Law, 15(2), 45-67.

Guerra, A., Parisi, F., & Pi, D. (2022). Liability for robots I: Legal challenges. Journal of Institutional Economics, 18(3), 331–343. https://doi.org/10.1017/S1744137421000825

Guerra, F., Parisi, G., & Pi, R. (2022). Legal implications of intelligent systems: Challenges and solutions. International Journal of Law and Technology, 15(2), 102-119.

Haditama, Talia Kallista & Sugianto, Fajar.A Comparative Analysis of Corporate Criminal Liability for AI-Based Malware: A Study of Indonesian and European Union Law. Indonesia Law Reform Journal, Vol. 5 No. 2, July 2025. https://ejournal.umm.ac.id/index.php/ilrej/article/view/39901

Rubinstein, D. (2022). Criminal liability for AI-caused harm: Mens Rea and beyond. British Journal of Criminology, 62(1), 257–273. https://doi.org/10.1093/bjc/azab017

Teena Arora1, Dr. Shailja Thakur. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 1886-1891 November 2024

Teena Arora & Dr. Shailja Thakur (2024)*Criminal Liability of Artificial Intelligence: A Comprehensive Analysis of Legal Issues and Emerging Challenges*. International Journal of Research Publication and Reviews

Vicko Taniady (2025) *AI-Induced Fatalities: A Criminal Law Perspective from Indonesia and International Perspective*. Yustisia Journal – Universitas Sebelas Maret

Muhammad Mutawalli Mukhlisa, Hariyanto Hariyanto. (2025) Law Reform in Parliamentary Democratization:A Comparative Study of Legislative Termsin Indonesia, Philippines, andtheUnited States of America. Journal of Law and Legal ReformVol. 6 Issue 3 (2025) 1079–1122DOI: https://doi.org/10.15294/jllr.v6i3.20664

Ministry of Industry and Information Technology of the People's Republic of China. (2023). Measures for Managing Generative AI. Retrieved from https://www.miit.gov.cn.

Mittelstadt, B. D. (2023, February 23). Who is liable for AI-driven accidents? The law is still emerging. Centre for International Governance Innovation. Retrieved from https://www.cigionline.org/articles/who-is-liable-for-ai-driven-accidents-the-law-is-still-emerging/

Smith, H. (2022). The Economic Impact of Over-Regulation on AI Startups in Europe. European Innovation Review, 45(1), 78-92

Oxford University Press. (2024). Artificial intelligence and the law: Analyzing legal accountability for autonomous systems. Retrieved from https://academic.oup.com

Pagallo, U. (2013). "The Laws of Robots: Crimes, Contracts, and Torts." Springer.

Utari I.S. 2023. Exploring Child Grooming Sexual Abuse through Differential Association Theory: A Criminological and Legal Examination with Constitutional ImplicationsVolksgeist Jurnal Ilmu Hukum Dan Konstitusi

Utari I.S Legal Protection for Children as Victims of Economic Exploitation: Problems and Challenges in Three Major ASEAN Countries (Indonesia, Vietnam and Philippines). Lex Scientia Law Review

Taniady, Vicko. AI-Induced Fatalities: A Criminal Law Perspective from Indonesia and International Perspective. Yustisia Jurnal Hukum, Universitas Sebelas Maret, 2025. https://jurnal.uns.ac.id/yustisia/article/view/101636

Ministry of Communication and Informatics (Kominfo). Indonesia Digital Transformation Roadmap 2021–2024. https://www.businessofgovernment.org/blog/indonesia-digital-transformation

ERIA (Economic Research Institute for ASEAN and East Asia). Accelerating Digital Transformation in Indonesia. ERIA Policy Brief, 2023. https://www.eria.org/uploads/media/Books/2022-Accelerating-Digital-Transformation-Indonesia/Accelerating-Digital-Transformation-Indonesia-rev3.pdf

Smith, H. (2022). The Economic Impact of Over-Regulation on AI Startups in Europe. European Innovation Review, 45(1), 78-92

Taeihagh, Araz, and Hazel Si Min Lim, (2019) 'Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks', Transport Reviews, 39.1 (2019), 103–28

Tamil Selvan B, and Srirangarajalu N, (2023) 'Self- Driving Car', International Journal of Engineering Technology and Management Sciences, 7.4 (2023), 275–80

Theoto, Tatiana Novaes, and Paulo Carlos Kaminski, (2019) 'A Country Specific Evaluation on the Feasibility of Autonomous Vehicles', Product Management & Development, 17.2 (2019), 123–33

Lagioia, Francesca & Sartor, Giovanni (2019) AI Systems Under

Criminal Law: A Legal Analysis and a Regulatory Perspective.

Acknowledgment

None.

Funding Information

None.

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.