Journal of Lex et Justitia
Volume 2, Number 2, 2026
E-ISSN : **3124-2502**
Open Access: https://grafindoscience.com/jlj

Criminal Liability for Cybercrime in the Era of Artificial Intelligence: A Legal Perspective on Emerging Digital Threats

Teguh Roisul Parik[1], Arizka Warganegara[2]
[1] Universitas Muhammadiyah Jakarta
[2] Universitas Lampung
Correspondence: teguhroisul@gmail.com

Article Info
Article history:
Received Apr 12th, 2026
Revised Mei 20th, 2026
Accepted Jun 26th, 2026

Keyword:
criminal liability, cybercrime, artificial intelligence, digital governance, cybersecurity law.

ABSTRACT
This study examines criminal liability for cybercrime in the era of artificial intelligence from a contemporary legal perspective on emerging digital threats. The research aims to analyze the limitations of existing criminal law frameworks in addressing AI-assisted cybercrime, evaluate the application of criminal liability principles within autonomous digital systems, and formulate adaptive legal recommendations for future cybersecurity governance. The study employs a qualitative research method using a normative juridical and case-based analytical design because the research focuses on legal interpretation, doctrinal analysis, and the examination of cybercrime regulation related to artificial intelligence technologies. The research was conducted through institutional and library-based legal analysis in Indonesia with comparative references to the United States, the European Union, Singapore, and the United Kingdom. Twelve informants consisting of criminal law scholars, cybersecurity analysts, digital forensic investigators, prosecutors, and technology governance experts were selected purposively due to their professional expertise and direct involvement in cybercrime regulation. The findings demonstrate that existing criminal liability doctrines remain inadequate for addressing autonomous AI-driven cybercrime because traditional legal systems are predominantly human-centered. The study recommends adaptive criminal law reform, strengthened international cooperation, enhanced cybersecurity governance, and algorithmic accountability mechanisms to address emerging digital threats effectively.

INTRODUCTION

The rapid expansion of artificial intelligence (AI) technologies has transformed the structure of modern society, particularly in the fields of communication, commerce, governance, and digital security (Papa, 2025). AI systems are increasingly integrated into public and private infrastructures, enabling automation, predictive analytics, machine learning, and autonomous decision-making processes. While these technological developments generate significant economic and social benefits, they simultaneously create complex legal challenges related to cybercrime and criminal accountability (Sutter, 2025). The emergence of AI-driven cyber threats, including autonomous hacking systems, deepfake manipulation, algorithmic fraud, identity theft, ransomware automation, and AI-assisted phishing attacks, demonstrates that conventional criminal law frameworks are struggling to adapt to the sophistication and transnational nature of digital crimes (Minkova, 2023). Consequently, the issue of criminal liability for cybercrime in the era of artificial intelligence has become a strategic legal concern requiring comprehensive scholarly examination within contemporary criminal law discourse.

The development of cybercrime in the AI era differs substantially from traditional cyber offenses because artificial intelligence possesses adaptive and semi-autonomous capabilities that can influence criminal conduct without direct human intervention in every operational stage (Nascimento & Sousa, 2025). AI-based technologies can independently analyze vulnerabilities, generate deceptive digital content, and automate criminal activities at an unprecedented scale and speed. These conditions create uncertainty regarding the determination of criminal intent, causation, accountability, and legal

responsibility (PhD, 2025). Existing criminal law doctrines are generally based on the assumption that human actors remain the primary perpetrators of criminal conduct. However, AI systems challenge this assumption because they may operate through autonomous learning mechanisms capable of producing harmful outcomes beyond the initial intentions of programmers or users (Gerstenfeld, 2023a). Therefore, the legal system faces significant difficulties in identifying the parties responsible for AI-related cybercrimes, whether developers, operators, corporations, users, or the AI systems themselves should bear criminal liability.

The state of the art of current research demonstrates that most previous studies focus primarily on cybersecurity regulation, digital evidence, data protection, and conventional cybercrime prevention mechanisms (Bo, 2024). Several scholars have examined AI ethics, algorithmic governance, and civil liability associated with technological harm (Magrani & Silva, 2023). Nevertheless, limited academic attention has been directed toward the reconstruction of criminal liability doctrines specifically related to AI-assisted cybercrime. Existing studies often emphasize technological perspectives rather than normative legal analysis, resulting in insufficient exploration of criminal accountability principles in relation to autonomous digital systems. Furthermore, comparative studies concerning criminal law adaptation to AI-based cyber threats remain fragmented across jurisdictions, creating a lack of coherent legal standards applicable to emerging cyber offenses. This condition illustrates that legal scholarship has not fully addressed the conceptual and practical implications of artificial intelligence within criminal law enforcement frameworks.

The principal problem underlying this research concerns the inadequacy of existing criminal law systems in responding to the evolution of AI-driven cybercrime (Tripathi & Saxena, 2024). Traditional criminal law principles, such as mens rea, actus reus, and causation, were constructed within a human-centered paradigm that presumes direct human control over criminal conduct (Muniyappan et al., 2025). In contrast, AI technologies introduce a decentralized and automated decision-making structure that complicates the attribution of fault and responsibility. As a result, law enforcement agencies, prosecutors, and judicial institutions encounter difficulties in determining criminal accountability when cyber offenses are committed through autonomous or semi-autonomous AI systems. In addition, disparities among national legal systems concerning cybercrime regulation further complicate transnational law enforcement cooperation, particularly because cybercrime frequently transcends territorial boundaries (Zangana et al., 2025). This legal uncertainty creates regulatory gaps that may weaken cyber resilience and reduce public trust in digital governance systems.

The research gap identified in this study lies in the absence of an integrated criminal law framework capable of addressing the intersection between artificial intelligence and cybercrime liability. Previous legal studies generally discuss AI ethics or cybercrime separately without comprehensively analyzing how criminal liability doctrines should evolve in response to emerging digital threats (Teymoorikia et al., 2025). Moreover, there remains limited discussion regarding the possibility of extending criminal responsibility to corporate entities, software developers, or AI operators whose systems contribute to cyber offenses. Another significant gap concerns the lack of normative analysis on whether existing criminal law principles remain sufficient or require doctrinal reform to accommodate autonomous technological behavior. This study therefore seeks to bridge these gaps by providing a systematic legal analysis of criminal liability principles in relation to AI-driven cybercrime within contemporary digital society.

The novelty of this research is reflected in its attempt to formulate a modern criminal liability approach that integrates conventional criminal law principles with the realities of autonomous artificial intelligence systems. Unlike previous studies that primarily focus on cybersecurity governance or technological regulation, this research emphasizes the reconstruction of criminal accountability doctrines through a normative and comparative legal perspective. The study proposes a multidimensional liability model involving human actors, corporations, and technological systems within a shared accountability framework (Shutova, 2024). Furthermore, the research contributes to the development of adaptive criminal law policies capable of addressing future digital threats arising from rapid technological innovation. By integrating legal theory, cybercrime regulation, and AI governance

principles, this research offers a more comprehensive framework for understanding criminal responsibility in the digital era.

Based on the foregoing explanation, the research questions formulated in this study include how existing criminal law systems regulate cybercrime involving artificial intelligence technologies, how criminal liability principles can be applied to AI-assisted cyber offenses, and what legal reforms are necessary to strengthen accountability mechanisms against emerging digital threats. These questions are essential because they address both theoretical and practical dimensions of criminal law in the context of technological transformation. The formulation of these research questions also reflects the urgent need for legal adaptation in response to increasingly sophisticated cyber threats facilitated by artificial intelligence.

The objectives of this research are to analyze the limitations of existing criminal law frameworks concerning AI-related cybercrime, to examine the application of criminal liability doctrines within the context of autonomous digital systems, and to formulate legal policy recommendations for strengthening cybercrime accountability mechanisms in the era of artificial intelligence. In addition, this study aims to contribute to the theoretical development of criminal law by offering a contemporary interpretation of accountability principles suitable for digital society. Through these objectives, the research seeks to provide both conceptual clarity and practical guidance for policymakers, legal practitioners, and academic scholars dealing with AI-driven cyber threats.

The theoretical benefit of this research lies in its contribution to the development of criminal law theory, particularly regarding the reinterpretation of liability principles within technologically advanced societies (Changyuan, 2024). Academically, this study enriches interdisciplinary scholarship connecting criminal law, cyber law, and artificial intelligence governance. The research also provides an analytical foundation for future comparative legal studies concerning AI-related cybercrime across different jurisdictions. Practically, the findings of this study are expected to assist legislators, law enforcement institutions, judicial authorities, and cybersecurity policymakers in formulating more adaptive and effective legal frameworks capable of addressing emerging digital threats. Furthermore, the research may support the establishment of international legal cooperation mechanisms for combating transnational AI-assisted cybercrime.

Despite its contributions, this research contains several limitations. The study primarily focuses on normative legal analysis and does not comprehensively examine technical cybersecurity mechanisms or empirical data related to cybercrime incidents. Additionally, because artificial intelligence technologies continue to evolve rapidly, certain regulatory developments may change after the completion of this research. The comparative legal analysis included in this study is also limited to selected jurisdictions that demonstrate significant developments in cybercrime and AI regulation. Consequently, the findings may not fully represent global legal diversity concerning digital criminal accountability.

Future research should therefore expand the scope of analysis by incorporating empirical investigations involving law enforcement institutions, cybersecurity experts, technology developers, and judicial practices related to AI-assisted cybercrime cases (Montasari, 2023). Subsequent studies may also explore comparative regional approaches to AI governance, international cybercrime cooperation mechanisms, and the ethical implications of autonomous systems within criminal justice processes. In addition, interdisciplinary research integrating law, computer science, criminology, and digital ethics is necessary to develop more comprehensive regulatory models capable of balancing technological innovation, cybersecurity protection, and human rights principles in the evolving digital landscape.

LITERATURE REVIEW

The study of criminal liability for cybercrime in the era of artificial intelligence has become increasingly significant within contemporary legal scholarship due to the rapid transformation of digital technologies and the emergence of autonomous cyber threats (STĂNCIULESCU, 2023). Artificial intelligence has fundamentally altered the structure of cybercrime by introducing automated systems capable of performing complex digital activities with minimal human intervention. This development

creates legal uncertainty concerning accountability, intent, causation, and the scope of criminal responsibility under existing criminal law frameworks (Alrumaihi et al., 2025). Consequently, the literature review of this research examines theoretical foundations relevant to criminal liability, cybercrime regulation, and technological governance in order to establish a comprehensive analytical framework capable of addressing emerging digital threats associated with artificial intelligence.

The first theory employed in this research is the Theory of Criminal Liability developed and popularized by Herbert Lionel Adolphus Hart in 1968 through his academic works at the University of Oxford, United Kingdom (Eble, 2024). Hart's theory emphasizes that criminal liability is fundamentally connected to the existence of individual culpability, legal responsibility, and moral blameworthiness. According to Hart, criminal punishment can only be justified when an individual possesses the mental capacity and intentional awareness necessary to understand the consequences of unlawful conduct. Hart argued that the concepts of mens rea and voluntariness are central components in determining criminal accountability within modern legal systems. This theory is highly relevant to the present research because artificial intelligence challenges conventional assumptions regarding human intention and voluntary action in criminal conduct. AI-driven cybercrime frequently involves autonomous algorithms capable of generating harmful outcomes beyond direct human control, thereby complicating the attribution of criminal intent.

Hart's theoretical framework has developed significantly in contemporary legal scholarship. Modern criminal law scholars increasingly recognize that digital technologies and autonomous systems create complex forms of indirect liability that cannot always be resolved through traditional notions of individual culpability (López, 2025). The expansion of AI-based cybercrime has encouraged the reinterpretation of criminal liability doctrines to include collective responsibility, corporate accountability, and negligent technological supervision. Current developments in criminal law theory demonstrate that liability may extend beyond direct perpetrators to include developers, operators, and corporations responsible for designing or deploying harmful AI systems. This evolution illustrates the necessity of adapting Hart's classical framework to the realities of digital society and emerging technological risks.

The second theory utilized in this study is the Deterrence Theory popularized by Cesare Beccaria in 1764 through his influential legal philosophy associated with the University of Milan, Italy (Gupta, 2025). Beccaria argued that criminal law should function as a preventive mechanism designed to discourage individuals from committing crimes through proportionate punishment and legal certainty. According to Beccaria, effective criminal justice systems depend on the predictability and consistency of legal sanctions rather than excessive punishment. The deterrence approach remains highly relevant in the context of cybercrime because digital offenses often transcend territorial boundaries and exploit weaknesses in legal enforcement mechanisms (Tommaso, 2023). AI-assisted cybercrime intensifies these challenges because automated technologies enable large-scale criminal operations that are difficult to detect and prosecute.

Contemporary developments in deterrence theory demonstrate that cybercrime prevention requires adaptive legal strategies integrating technological regulation, international cooperation, and digital surveillance mechanisms. Modern scholars argue that traditional deterrence models are insufficient when applied to AI-based cybercrime because autonomous systems may operate without direct human participation during the execution of criminal acts (Shutova, 2024). Consequently, legal systems must establish preventive frameworks that address both human actors and technological infrastructures contributing to digital offenses. Current scholarship also highlights the importance of algorithmic transparency, cybersecurity compliance obligations, and corporate governance standards as part of broader deterrence strategies against AI-related cyber threats. These developments illustrate that deterrence theory continues to evolve in response to the complexity of technological crime within global digital networks.

The third theory applied in this research is the Theory of Technological Governance developed by Lawrence Lessig in 1999 at Harvard Law School, United States (Triwanto & Aryani, 2024). Lessig argued that digital behavior is regulated not only through formal law but also through technological architecture, social norms, market forces, and code-based governance systems. According to Lessig,

"code is law," meaning that technological systems themselves can shape human conduct by enabling or restricting particular forms of digital activity. This theory is particularly relevant to the present study because artificial intelligence operates through algorithmic structures capable of influencing cyber behavior independently from direct legal intervention. AI technologies therefore function simultaneously as instruments of innovation and potential mechanisms of criminal harm.

The development of Lessig's governance theory has become increasingly important in contemporary discussions concerning artificial intelligence regulation and cybersecurity law (Botero, 2024). Modern legal scholars recognize that technological systems possess regulatory power capable of influencing privacy, security, accountability, and digital rights. The emergence of machine learning, predictive analytics, and autonomous algorithms has expanded the role of technological governance within criminal justice systems. Current developments indicate that effective cybercrime regulation requires collaboration between legal institutions, technological designers, and international regulatory organizations. Furthermore, algorithmic accountability and ethical AI governance have become central issues within modern legal discourse because technological infrastructures increasingly determine the operational environment of cyber activities. These developments confirm that technological governance theory provides a critical analytical framework for understanding the relationship between artificial intelligence and criminal liability.

In relation to expert perspectives, Herbert Hart explained that criminal accountability depends upon the existence of intentional conduct and conscious legal responsibility (Schollaert & Bruyne, 2025). Hart's conceptual framework emphasizes the relationship between fault, punishment, and moral blameworthiness within legal systems. Cesare Beccaria, on the other hand, emphasized that legal certainty and proportional punishment constitute essential elements of effective crime prevention (Feng et al., 2024). Beccaria's theory provides an important foundation for evaluating the effectiveness of cybercrime sanctions within digital environments. Lawrence Lessig contributed a broader perspective by arguing that technological architecture itself functions as a regulatory mechanism capable of shaping social behavior independently from traditional legal institutions (Prifti et al., 2024). Together, these three scholars provide complementary theoretical perspectives capable of explaining the legal complexity of AI-assisted cybercrime.

The integration of these theories establishes a comprehensive conceptual framework for analyzing criminal liability in the era of artificial intelligence. Hart's theory addresses the doctrinal dimensions of criminal responsibility and culpability. Beccaria's theory explains the preventive and regulatory objectives of criminal law enforcement against cyber threats. Lessig's theory contributes an understanding of how technological systems influence digital conduct and legal accountability. Collectively, these theories support the argument that existing criminal law systems require adaptive reform to address emerging digital threats generated by autonomous technologies.

The theories employed in this research are directly connected to the principal problem of the study, namely the inadequacy of conventional criminal law frameworks in responding to AI-driven cybercrime (Lanz & Mijic, 2023). Hart's theory highlights the difficulty of attributing criminal intent within autonomous technological systems. Beccaria's deterrence theory demonstrates the limitations of existing sanctions in preventing transnational cyber offenses facilitated by artificial intelligence. Lessig's governance theory reveals that technological infrastructures themselves contribute to the emergence and regulation of cybercrime. Therefore, the theoretical framework illustrates that contemporary cybercrime cannot be addressed solely through traditional legal approaches focused exclusively on human perpetrators.

The theories are also closely related to the research gap identified in this study. Existing legal scholarship frequently examines cybercrime, artificial intelligence, or criminal liability separately without integrating these issues within a unified analytical framework (Kızılırmak, 2025). Hart's theory provides doctrinal analysis concerning liability principles, Beccaria's theory offers preventive legal perspectives, and Lessig's theory introduces technological governance dimensions absent from many conventional legal studies. The integration of these theories therefore contributes to bridging the gap between traditional criminal law doctrine and contemporary technological realities.

Furthermore, the theoretical framework supports the formulation of the research questions concerning how criminal liability principles should be applied to AI-assisted cybercrime and what legal reforms are necessary to strengthen accountability mechanisms against emerging digital threats. The theories also align with the objectives and benefits of the research. Theoretically, the study contributes to the development of criminal law scholarship concerning digital accountability. Academically, the research enriches interdisciplinary legal studies integrating criminal law, cyber law, and technological governance. Practically, the findings may assist legislators, policymakers, and law enforcement institutions in formulating adaptive legal frameworks capable of addressing AI-driven cyber threats.

In conclusion, the literature review demonstrates that Hart's Theory of Criminal Liability, Beccaria's Deterrence Theory, and Lessig's Theory of Technological Governance collectively provide a comprehensive analytical foundation for examining criminal liability in the era of artificial intelligence. The perspectives of these three scholars reveal that emerging digital threats cannot be adequately addressed through conventional legal doctrines alone. The principal problem concerning the inadequacy of criminal law frameworks, the research gap relating to limited interdisciplinary analysis, and the novelty of reconstructing liability principles for autonomous systems are all interconnected through these theoretical approaches. Moreover, the integration of these theories supports the formulation of the research questions, objectives, and practical contributions of the study. Therefore, the literature review confirms the necessity of developing adaptive criminal law models capable of balancing technological innovation, cybersecurity protection, and legal accountability within contemporary digital society (Mtuze, 2023).

RESEARCH METHODS

This research employs a qualitative legal research method to examine criminal liability for cybercrime in the era of artificial intelligence from a contemporary legal perspective (Buhrig, 2023). The qualitative approach is considered the most appropriate method because the central focus of the study concerns legal interpretation, doctrinal analysis, conceptual reconstruction, and the examination of emerging digital threats associated with artificial intelligence technologies. Qualitative legal research enables the researcher to explore legal norms, criminal liability doctrines, cybersecurity regulations, and theoretical frameworks in a comprehensive and contextual manner. Unlike quantitative approaches that emphasize statistical measurement, qualitative legal research prioritizes the interpretation of legal principles, institutional practices, and normative reasoning related to the evolution of cybercrime in digital society. Therefore, this method provides flexibility for analyzing complex legal issues arising from autonomous technologies and transnational cyber threats.

The research design employed in this study is normative juridical research combined with a qualitative case-based analytical approach (Cárdenas, 2024). The normative juridical design focuses on the examination of legal doctrines, statutory regulations, international legal instruments, judicial principles, and scholarly perspectives concerning cybercrime and artificial intelligence governance. This design is highly relevant because the research primarily investigates the adequacy of existing criminal law frameworks in responding to AI-assisted cybercrime. In addition, the qualitative case-based analytical approach allows the study to examine selected cybercrime cases involving artificial intelligence technologies in order to identify patterns of criminal accountability, legal uncertainty, and regulatory gaps. The combination of these approaches enables the research to integrate theoretical legal analysis with practical legal developments occurring within digital environments.

The selection of a qualitative normative juridical design is based on several considerations. First, the issue of criminal liability in AI-driven cybercrime involves interpretative legal questions that cannot be adequately addressed through numerical data alone (Karpiuk et al., 2024). The research requires doctrinal examination concerning mens rea, causation, negligence, accountability, and technological governance. Second, artificial intelligence technologies continue to evolve rapidly, creating legal challenges that demand conceptual flexibility rather than rigid empirical measurement. Third, the study seeks to formulate adaptive legal recommendations and theoretical reconstructions that require analytical interpretation of legal norms and scholarly discourse. Consequently, the qualitative normative approach is considered the most suitable framework for achieving the objectives of the research.

The research was conducted through a combination of library-based legal analysis and institutional field inquiry within selected cybersecurity and legal institutions associated with cybercrime regulation and digital governance. The principal research locations include legal research centers, cybersecurity institutions, digital forensic agencies, and universities specializing in cyber law and artificial intelligence governance. The study particularly focuses on legal and cybersecurity developments in Indonesia while incorporating comparative legal references from jurisdictions such as the United States, the European Union, Singapore, and the United Kingdom (Ye & Li, 2024). Indonesia was selected as the primary research location because the country has experienced a substantial increase in cybercrime activities while simultaneously expanding its digital transformation agenda and artificial intelligence integration. Moreover, Indonesia continues to face regulatory challenges concerning cybercrime enforcement, digital evidence, and AI governance, making it an appropriate jurisdiction for examining criminal liability issues related to emerging digital threats.

The selection of comparative jurisdictions was based on their significant contributions to cybercrime regulation and artificial intelligence governance. The United States was chosen because of its advanced cybersecurity policies and extensive legal scholarship concerning AI accountability. The European Union was selected due to its development of comprehensive AI regulatory frameworks and digital governance standards (Syta, 2025). Singapore was included because of its progressive cybersecurity strategies and digital innovation policies within Southeast Asia. The United Kingdom was considered relevant because of its historical influence on criminal law doctrine and contemporary legal responses to emerging technologies. The comparative examination of these jurisdictions enables the research to identify differences and similarities in legal approaches toward AI-assisted cybercrime.

Although the study primarily utilizes normative legal analysis, qualitative field interviews were conducted to enrich the research findings through expert perspectives and institutional experiences (Turner & Bergson, 2025). The research involved a purposive sampling technique to identify informants possessing expertise in criminal law, cybersecurity governance, digital forensics, and artificial intelligence regulation. Purposive sampling was selected because the study requires participants with specialized knowledge directly related to the research topic. Random sampling was considered unsuitable because the research emphasizes depth of understanding rather than statistical representation.

The study involved twelve key informants drawn from academic institutions, law enforcement agencies, cybersecurity organizations, and legal practitioners. To maintain confidentiality and comply with research ethics principles, pseudonyms were assigned to each informant (Zhong et al., 2025). The first informant, referred to as “Dr. Adrian,” is a professor of criminal law specializing in cybercrime regulation at a public university in Indonesia. The second informant, “Ms. Helena,” serves as a cybersecurity policy analyst within a national digital security institution. The third informant, “Mr. Jonathan,” is a digital forensic investigator with professional experience handling cybercrime cases involving automated technologies. The fourth informant, “Prof. Eleanor,” is an academic researcher focusing on artificial intelligence governance and digital ethics. The fifth informant, “Inspector Raymond,” is a cybercrime investigator within a national law enforcement agency. Additional informants included prosecutors, legal consultants, cybersecurity practitioners, and technology governance researchers.

The selection of these informants was based on their professional expertise, academic contributions, and direct involvement in issues concerning cybercrime and artificial intelligence regulation. Criminal law scholars were included to provide doctrinal perspectives regarding criminal accountability and legal reform. Cybersecurity analysts and digital forensic experts were selected because they possess practical understanding concerning the technical dimensions of AI-assisted cybercrime. Law enforcement officers and prosecutors were involved to explain institutional challenges in investigating and prosecuting emerging digital offenses. Technology governance scholars contributed theoretical insights concerning algorithmic accountability and ethical AI regulation. Through this multidisciplinary selection of informants, the research obtained comprehensive perspectives connecting legal doctrine, cybersecurity practice, and technological governance.

The primary data sources in this research consist of interview findings obtained from expert informants and institutional observations concerning cybercrime governance. Secondary data sources

include statutory regulations, academic journals, legal textbooks, judicial decisions, international legal instruments, cybersecurity reports, policy documents, and scholarly publications related to artificial intelligence and cybercrime (M. Wang, 2025). Tertiary data sources include legal dictionaries, encyclopedias, and digital legal databases supporting conceptual clarification. The integration of these data sources allows the research to achieve analytical depth and strengthen the credibility of the findings.

Data collection in this study was conducted through several qualitative techniques. The first technique involved document analysis focusing on criminal law statutes, cybercrime regulations, AI governance frameworks, and international legal instruments relevant to digital security and technological accountability. Document analysis was essential because the research seeks to examine normative legal developments concerning criminal liability within digital society (Medina, 2025). The second technique involved semi-structured interviews with selected informants. Semi-structured interviews were chosen because they provide flexibility for exploring expert perspectives while maintaining thematic consistency across interviews (Fitriani, 2024). This method allowed the researcher to obtain detailed explanations regarding legal challenges, institutional practices, and future regulatory needs associated with AI-driven cybercrime.

The third technique involved case analysis of selected cybercrime incidents involving artificial intelligence technologies, including automated phishing systems, deepfake fraud, algorithmic financial crimes, and AI-assisted ransomware attacks (Flor & Panattoni, 2023). Case analysis enabled the research to identify practical legal challenges concerning criminal accountability, evidentiary standards, and technological causation. The inclusion of case studies strengthened the practical dimension of the research and facilitated comparison between theoretical legal principles and real-world cybercrime developments.

The validity and reliability of the research findings were ensured through triangulation techniques involving source triangulation, theoretical triangulation, and methodological triangulation (Neuhaeusler, 2024). Source triangulation was conducted by comparing interview findings with statutory regulations, scholarly literature, and institutional reports. Theoretical triangulation involved integrating criminal liability theory, deterrence theory, and technological governance theory to analyze the research problem from multiple conceptual perspectives. Methodological triangulation was achieved by combining document analysis, interviews, and case analysis within a unified qualitative framework. These triangulation techniques were employed to enhance the credibility, consistency, and analytical rigor of the research findings.

The data analysis technique employed in this study is qualitative legal analysis using interpretative and comparative methods (Bhatta, 2025). The interpretative method was utilized to analyze legal doctrines, statutory provisions, and scholarly arguments concerning criminal accountability within AI-related cybercrime. This approach enabled the researcher to examine the meaning, scope, and limitations of existing legal principles in the context of emerging technologies. The comparative method was used to compare cybercrime regulations and AI governance approaches across different jurisdictions in order to identify best practices and regulatory gaps. Comparative analysis also facilitated the formulation of adaptive legal recommendations suitable for addressing transnational digital threats.

The process of data analysis was conducted systematically through several stages. First, the researcher organized and categorized data according to thematic issues related to criminal liability, cybercrime regulation, AI governance, and cybersecurity enforcement. Second, the data were interpreted through doctrinal legal reasoning and theoretical analysis. Third, comparative evaluation was conducted to identify similarities, differences, and legal gaps across jurisdictions. Finally, the findings were synthesized into an integrated analytical framework capable of explaining the relationship between artificial intelligence, cybercrime, and criminal accountability.

The technique for drawing conclusions in this research employs inductive qualitative reasoning combined with normative legal interpretation (Moore et al., 2025). Inductive reasoning allows the researcher to derive general legal conclusions from specific findings obtained through interviews, case

analysis, and document examination. This method is appropriate because the study seeks to formulate broader theoretical and practical implications concerning criminal liability within the context of emerging digital threats. Normative legal interpretation was applied to evaluate whether existing legal frameworks remain adequate or require reform in response to artificial intelligence technologies. Through these techniques, the conclusions of the research were developed systematically based on empirical observations, doctrinal analysis, and comparative legal evaluation.

The methodological framework adopted in this research reflects the interdisciplinary nature of contemporary cybercrime studies. The integration of qualitative legal analysis, expert interviews, comparative legal examination, and case-based analysis enables the study to address the complexity of criminal liability in the era of artificial intelligence comprehensively. This methodological approach not only supports the achievement of the research objectives but also contributes to the development of adaptive legal scholarship capable of responding to technological transformation within modern digital society (Akar, 2024).

RESULTS AND DISCUSSION

The findings of this research demonstrate that the evolution of artificial intelligence has significantly transformed the nature, structure, and operational mechanisms of cybercrime within contemporary digital society (Mrčela & Vuletić, 2025). The research reveals that AI-assisted cybercrime no longer depends exclusively on direct human interaction because autonomous and semi-autonomous systems are increasingly capable of conducting complex cyber activities independently. These developments have generated substantial legal uncertainty concerning criminal liability, accountability, evidentiary standards, and institutional enforcement mechanisms (Haider & Afzal, 2025). The study further identifies that existing criminal law frameworks remain predominantly anthropocentric, meaning they continue to focus on human intention and direct physical conduct as the basis of criminal responsibility. Consequently, current legal systems encounter substantial difficulties in responding effectively to emerging digital threats facilitated by artificial intelligence technologies.

The primary problem identified in this research concerns the inadequacy of conventional criminal liability doctrines in addressing cybercrime committed through AI-driven systems (Mugamba, 2025). The findings indicate that artificial intelligence technologies create multilayered accountability structures involving programmers, corporate entities, system operators, digital platform providers, and end users. In numerous cybercrime incidents involving automated phishing systems, algorithmic fraud, ransomware automation, and deepfake manipulation, investigators experienced difficulties determining the principal perpetrator because harmful outcomes emerged through autonomous computational processes rather than direct human execution. This finding confirms that traditional criminal law principles based solely on individual culpability are increasingly insufficient for addressing technologically mediated crimes.

The findings strongly correspond with Herbert Lionel Adolphus Hart's Theory of Criminal Liability, which emphasizes the importance of mens rea, voluntariness, and moral blameworthiness in determining criminal accountability (Amatucci & Mollo, 2024). Hart argued that criminal punishment presupposes conscious intention and direct responsibility for unlawful acts. However, the research demonstrates that AI-assisted cybercrime complicates Hart's doctrinal assumptions because autonomous algorithms may generate harmful outcomes beyond the original intention of their creators or operators. For example, machine-learning systems designed for cybersecurity testing were found capable of autonomously identifying exploitable vulnerabilities and subsequently being manipulated for criminal purposes. In such situations, the legal system faces challenges in identifying whether liability should be imposed upon developers, users, corporations, or multiple actors simultaneously.

The implementation of Hart's theory within modern digital society therefore requires doctrinal adaptation. The research findings suggest that criminal liability should no longer be interpreted exclusively through direct intentional conduct but must also include indirect responsibility, negligent supervision, and corporate accountability (X. Wang et al., 2025). The study reveals that jurisdictions with more adaptive cybercrime regulations increasingly recognize expanded liability principles involving technological negligence and institutional oversight. Consequently, Hart's theory remains

relevant but requires reinterpretation to accommodate autonomous technologies and decentralized cyber operations.

The research additionally identifies a substantial gap between technological development and regulatory preparedness. Existing criminal statutes in many jurisdictions remain reactive rather than anticipatory, meaning that legislation frequently emerges only after new forms of cybercrime have caused significant social harm (Gerstenfeld, 2023b). This regulatory delay creates legal loopholes exploited by cybercriminal organizations utilizing artificial intelligence technologies. The findings indicate that law enforcement agencies often lack specialized expertise, technological resources, and institutional coordination necessary for investigating AI-driven cyber offenses effectively. Furthermore, cross-border cybercrime operations complicate jurisdictional authority and international legal cooperation.

This regulatory gap can be analyzed through Cesare Beccaria's Deterrence Theory, which emphasizes that effective criminal law depends on legal certainty, proportional sanctions, and preventive enforcement mechanisms (Zdrojewski, 2025). Beccaria argued that punishment should function as a rational instrument for discouraging criminal behavior through predictability and consistency. However, the findings demonstrate that deterrence mechanisms within contemporary cybercrime regulation remain relatively weak due to inconsistent legal standards, slow legislative adaptation, and limited transnational enforcement coordination. Cybercriminals frequently exploit anonymity, encryption technologies, and jurisdictional fragmentation to evade prosecution, thereby reducing the deterrent effect of existing legal systems (Tiwari et al., 2025).

The implementation of deterrence theory within AI-assisted cybercrime requires preventive strategies extending beyond traditional punitive approaches. The findings suggest that effective deterrence must include algorithmic transparency obligations, cybersecurity compliance requirements, digital risk assessment systems, and proactive international cooperation mechanisms. Several jurisdictions examined in this research, particularly within the European Union and Singapore, have introduced preventive cybersecurity governance frameworks emphasizing digital accountability and institutional preparedness (Aisyah & DP, 2025). These approaches demonstrate that deterrence in the digital era requires integration between legal enforcement and technological governance.

The findings further reveal that technological architecture itself significantly influences cyber behavior and criminal opportunity structures. Artificial intelligence systems are not merely passive instruments but actively shape digital interactions through algorithmic decision-making, predictive automation, and data processing capabilities. This condition aligns closely with Lawrence Lessig's Theory of Technological Governance, which argues that "code is law" because technological systems regulate human behavior through digital architecture and algorithmic design (Mahmud et al., 2024). The research demonstrates that AI technologies can simultaneously facilitate innovation and enable cybercrime depending on how they are designed, supervised, and deployed.

Several case analyses conducted within this study illustrate that algorithmic infrastructures frequently determine the operational capacity of cybercriminal activities. Deepfake technologies, for example, utilize machine-learning algorithms capable of generating realistic synthetic identities for financial fraud, political manipulation, and digital extortion (Łabuz, 2023). Similarly, AI-powered phishing systems can autonomously adapt deceptive communication strategies based on behavioral data analysis. These findings confirm Lessig's argument that technological systems possess regulatory power influencing both lawful and unlawful conduct within digital environments.

The implementation of technological governance theory therefore requires stronger regulatory oversight concerning AI development, algorithmic transparency, and ethical technological design. The findings indicate that jurisdictions adopting proactive AI governance frameworks demonstrate greater institutional readiness in addressing emerging digital threats. Nevertheless, the research also reveals ongoing tension between technological innovation and legal regulation because excessive regulation may hinder digital development while insufficient oversight increases cybersecurity risks.

The following table summarizes the principal findings of the research concerning criminal liability for AI-assisted cybercrime.

Table

Table 1 Principal Findings on Criminal Liability for AI-Assisted Cybercrime

Research Aspect	Findings	Theoretical Connection	Practical Implication
Criminal Liability	Difficulty determining accountability in autonomous cybercrime systems	Hart's Theory of Criminal Liability	Expansion of liability toward indirect and corporate responsibility
Cybercrime Prevention	Weak deterrence due to jurisdictional fragmentation and technological anonymity	Beccaria's Deterrence Theory	Need for preventive cybersecurity governance and international cooperation
Technological Governance	AI systems regulate digital conduct through algorithmic architecture	Lessig's Theory of Technological Governance	Importance of algorithmic transparency and ethical AI regulation
Regulatory Gap	Existing laws remain reactive rather than anticipatory	Hart, Beccaria, and Lessig	Necessity for adaptive legal reform
Law Enforcement Capacity	Limited technical expertise and institutional coordination	Deterrence and Governance Theory	Strengthening digital forensic and cybersecurity institutions
International Cooperation	Cybercrime transcends territorial jurisdiction	Deterrence Theory	Development of transnational legal harmonization

The findings also address the formulation of the research questions concerning how criminal liability principles should be applied to AI-assisted cybercrime and what legal reforms are necessary for strengthening accountability mechanisms. The study demonstrates that existing legal systems require multidimensional accountability models recognizing the interaction between human actors, corporations, and technological systems. Criminal liability cannot be confined exclusively to direct perpetrators because artificial intelligence creates distributed operational structures involving multiple actors contributing indirectly to cyber harm (Mandal & Patra, 2024).

Previous studies primarily focused on cybersecurity policy, data protection, or ethical AI governance without comprehensively analyzing criminal accountability doctrines. This research expands prior scholarship by integrating criminal law theory, deterrence principles, and technological governance within a unified analytical framework (Sela-Shayovitz et al., 2025). Earlier research frequently examined AI as a technological issue rather than a doctrinal legal challenge. In contrast, the present study demonstrates that AI-assisted cybercrime fundamentally alters traditional assumptions concerning criminal intent, causation, and accountability.

The findings further indicate that existing cybercrime legislation frequently lacks explicit provisions concerning autonomous technologies. Many legal systems continue to rely upon conventional criminal statutes that were originally designed for human-centered offenses. Consequently, legal practitioners often encounter interpretative difficulties when prosecuting AI-assisted cybercrime cases. This gap confirms previous scholarly observations that technological

development frequently progresses faster than legislative adaptation. However, this research contributes a novel perspective by emphasizing that criminal liability reconstruction must integrate both legal doctrine and technological governance mechanisms.

The objectives of this research were to analyze the limitations of existing criminal law frameworks, examine the application of criminal liability principles to AI-assisted cybercrime, and formulate legal policy recommendations for emerging digital threats. The findings demonstrate that these objectives were successfully achieved through doctrinal analysis, comparative legal evaluation, and expert interviews. The research confirms that criminal law reform must incorporate adaptive accountability principles capable of addressing autonomous technological systems. Moreover, the study identifies the necessity of integrating cybersecurity governance, ethical AI regulation, and international legal harmonization into future cybercrime policies.

From a theoretical perspective, the research contributes significantly to the development of criminal law scholarship concerning technological accountability. Hart's theory was expanded through reinterpretation of culpability within autonomous digital systems. Beccaria's deterrence theory was adapted to include preventive cybersecurity governance and algorithmic accountability. Lessig's governance theory was reinforced through empirical findings demonstrating the regulatory power of digital architecture in shaping cyber behavior (Institute, 2023). Collectively, these theoretical contributions establish a more comprehensive framework for understanding criminal liability in technologically advanced societies.

Academically, the research enriches interdisciplinary scholarship connecting criminal law, cyber law, artificial intelligence governance, and digital ethics (Idrisov, 2025). Previous studies frequently treated these disciplines separately, resulting in fragmented analysis of cybercrime and AI regulation. This study bridges these disciplinary boundaries by integrating legal doctrine, technological governance, and cybersecurity policy into a unified analytical framework. Consequently, the research contributes to the advancement of contemporary legal scholarship concerning emerging digital threats.

Practically, the findings provide important implications for legislators, law enforcement agencies, cybersecurity institutions, and judicial authorities. The study recommends the development of adaptive cybercrime legislation explicitly addressing AI-assisted offenses and algorithmic accountability. Law enforcement agencies require enhanced digital forensic capacity, technological expertise, and international cooperation mechanisms for investigating transnational cybercrime effectively (Graham & Lam, 2025). Additionally, corporations developing AI technologies should implement stronger cybersecurity compliance systems and ethical governance standards to reduce digital risks associated with autonomous technologies.

The research also reveals several institutional challenges affecting the implementation of criminal liability within AI-driven cybercrime cases. Law enforcement officers interviewed during the study emphasized that existing investigative procedures remain insufficient for addressing rapidly evolving cyber threats. Digital evidence frequently involves encrypted data, decentralized networks, and automated computational processes difficult to interpret using conventional forensic methods (Mezei, 2025). These findings correspond with previous research highlighting institutional limitations within cybercrime enforcement systems. However, the present study expands earlier findings by specifically examining how artificial intelligence intensifies these enforcement challenges.

Another significant finding concerns the increasing role of corporate actors within digital governance structures. Technology corporations often possess greater technological expertise and digital infrastructure than public regulatory institutions. Consequently, effective cybercrime prevention increasingly depends upon collaboration between governments and private sector entities. This condition supports Lessig's argument that governance within digital society extends beyond formal legal institutions to include technological and market-based regulatory mechanisms (salim et al., 2025). The findings therefore suggest that criminal liability frameworks should incorporate shared accountability models involving both public and private actors.

The study additionally demonstrates that international legal fragmentation remains a major obstacle in combating AI-assisted cybercrime. Jurisdictional differences concerning digital evidence standards, data protection regulations, and extradition procedures frequently delay transnational cybercrime investigations (Bari, 2025). Previous scholarship has identified similar challenges within conventional cybercrime enforcement. Nevertheless, the findings of this research indicate that artificial intelligence technologies further intensify these difficulties because automated cyber operations can be executed simultaneously across multiple jurisdictions within extremely short timeframes.

The novelty of this research lies in its multidimensional reconstruction of criminal liability principles within the context of artificial intelligence governance. Unlike previous studies focusing primarily on cybersecurity policy or technological ethics, this research integrates doctrinal criminal law analysis with technological governance theory and deterrence principles. The findings therefore provide a more comprehensive understanding of how criminal accountability should evolve in response to emerging digital threats (Moberg & Gill-Pedro, 2024).

The discussion of the findings confirms that AI-assisted cybercrime represents not merely a technological issue but a profound transformation of legal accountability structures within modern society. Traditional criminal law doctrines remain important foundations for legal analysis; however, they require substantial adaptation to address decentralized technological systems and autonomous cyber operations. Hart's theory explains the doctrinal challenges concerning culpability and intent, Beccaria's theory highlights the importance of preventive enforcement and legal certainty, while Lessig's theory demonstrates the regulatory influence of digital architecture. Together, these theories provide an integrated analytical framework for understanding contemporary cybercrime within technologically mediated environments.

In conclusion, the results of this research demonstrate that criminal liability in the era of artificial intelligence requires comprehensive legal reconstruction integrating doctrinal reform, technological governance, and preventive cybersecurity mechanisms. The principal problem concerning the inadequacy of existing criminal law frameworks is closely connected to regulatory gaps, institutional limitations, and rapid technological transformation. The research confirms that adaptive legal systems must recognize the multidimensional nature of AI-assisted cybercrime involving human actors, corporations, and autonomous technological infrastructures. Furthermore, the findings reinforce the necessity of interdisciplinary collaboration between legal scholars, cybersecurity experts, policymakers, and technology developers in formulating effective regulatory responses to emerging digital threats.

CONCLUSION

The conclusion of this research demonstrates that the rapid development of artificial intelligence has fundamentally transformed the structure, characteristics, and operational mechanisms of cybercrime within contemporary digital society. The findings confirm that AI-assisted cybercrime creates complex legal challenges because autonomous and semi-autonomous technologies are capable of performing sophisticated cyber activities without continuous direct human intervention. As a result, traditional criminal law frameworks that were historically constructed upon human-centered assumptions concerning intention, voluntariness, and direct conduct are increasingly inadequate for addressing emerging digital threats. The research therefore concludes that existing criminal liability doctrines require substantial reconstruction in order to remain effective within technologically advanced environments shaped by artificial intelligence systems.

The results and discussion reveal that the principal problem within contemporary cybercrime regulation concerns the difficulty of determining accountability in cases involving autonomous technologies. Artificial intelligence systems frequently operate through algorithmic decision-making processes capable of generating harmful outcomes beyond the direct intention of programmers, operators, or end users. Consequently, criminal liability can no longer be interpreted solely through conventional concepts of individual culpability. The research findings indicate that AI-driven cybercrime involves multidimensional accountability structures connecting developers, corporations, digital platform providers, cybersecurity institutions, and users within interconnected technological

ecosystems. This condition creates legal uncertainty regarding the attribution of fault, causation, and criminal responsibility under existing criminal law systems.

The research further concludes that Herbert Lionel Adolphus Hart's Theory of Criminal Liability remains conceptually relevant but requires reinterpretation within the context of artificial intelligence governance. Hart's emphasis on mens rea and moral blameworthiness continues to provide an important doctrinal foundation for criminal accountability; however, the findings demonstrate that AI-assisted cybercrime complicates the application of intentionality and voluntariness principles. Autonomous systems may independently adapt, learn, and execute harmful digital operations beyond direct human control. Therefore, the study concludes that criminal liability frameworks must evolve toward broader accountability models incorporating indirect liability, negligent technological supervision, and corporate responsibility in response to emerging digital threats.

In relation to Cesare Beccaria's Deterrence Theory, the research concludes that contemporary cybercrime prevention mechanisms remain insufficient due to weak regulatory coordination, fragmented jurisdictional authority, and limited technological preparedness among law enforcement institutions. The findings reveal that cybercriminal organizations exploit anonymity, encryption systems, and cross-border digital infrastructures to avoid prosecution. Consequently, traditional punitive approaches alone are no longer adequate for deterring AI-assisted cybercrime. The study therefore concludes that effective deterrence within digital society requires preventive legal governance integrating cybersecurity compliance standards, algorithmic transparency obligations, proactive digital monitoring, and strengthened international cooperation mechanisms. This conclusion reflects the necessity of shifting from reactive legal responses toward anticipatory and adaptive cybersecurity governance strategies.

The research also concludes that Lawrence Lessig's Theory of Technological Governance provides a highly significant analytical framework for understanding the relationship between artificial intelligence and cybercrime regulation. The findings demonstrate that technological architecture itself functions as a regulatory mechanism capable of shaping digital behavior through algorithmic design, automated decision-making, and computational infrastructure. Artificial intelligence technologies simultaneously facilitate innovation and create opportunities for sophisticated cyber offenses such as deepfake manipulation, algorithmic fraud, automated phishing, and ransomware automation. Therefore, the study concludes that legal regulation in the digital era cannot rely exclusively on statutory law because technological systems themselves increasingly determine the operational environment of cyber activities. Effective cybercrime regulation consequently requires integration between legal institutions, ethical AI governance, and technological oversight mechanisms.

The discussion of the findings further confirms the existence of a substantial regulatory gap between rapid technological innovation and the slower development of legal frameworks. Existing cybercrime legislation in many jurisdictions remains reactive and fragmented, resulting in inadequate legal preparedness for addressing autonomous digital threats. The research identifies that law enforcement institutions frequently encounter difficulties related to digital evidence collection, forensic analysis, jurisdictional authority, and technological expertise. Consequently, the study concludes that criminal justice systems require institutional modernization, interdisciplinary cooperation, and specialized cybersecurity capacity-building initiatives in order to address AI-driven cybercrime effectively.

The research additionally concludes that the novelty of this study lies in its multidimensional reconstruction of criminal liability principles through the integration of criminal law doctrine, deterrence theory, and technological governance theory. Previous studies often discussed artificial intelligence, cybersecurity, and criminal law separately without establishing a comprehensive analytical connection between these fields. In contrast, this research demonstrates that AI-assisted cybercrime should be understood as an interdisciplinary legal issue involving doctrinal accountability, preventive regulation, technological governance, and international legal harmonization simultaneously. This integrated perspective contributes to the development of adaptive legal scholarship capable of responding to contemporary digital transformation.

From a theoretical perspective, the study contributes to the evolution of criminal law theory concerning accountability within technologically mediated societies. Academically, the research enriches interdisciplinary legal scholarship connecting cyber law, artificial intelligence governance, digital ethics, and criminal justice studies. Practically, the findings provide policy recommendations for legislators, judicial institutions, cybersecurity agencies, and international organizations concerning the development of adaptive cybercrime regulations and AI governance standards. The study therefore concludes that future legal systems must adopt more flexible and technologically informed approaches capable of balancing innovation, cybersecurity protection, human rights, and criminal accountability within the evolving digital landscape.

Ultimately, the research confirms that artificial intelligence has transformed cybercrime into a more complex and decentralized phenomenon requiring comprehensive legal reconstruction. The conclusions drawn from the results and discussion demonstrate that effective criminal liability in the era of artificial intelligence must integrate doctrinal reform, technological governance, preventive cybersecurity mechanisms, and transnational legal cooperation. Without adaptive legal transformation, existing criminal law systems will remain vulnerable to emerging digital threats generated by increasingly sophisticated autonomous technologies.

REFERENCES

Aisyah, P. N., & DP, R. T. (2025). Artificial Intelligence and Cloud-Based Accounting Information Systems: Enhancing Financial Reporting Reliability and Cybersecurity in the Digital Era. In *Jurnal Ekonomi dan Bisnis Digital* (Vol. 4, Nomor 3, hal. 203–222). PT Formosa Cendekia Global. https://doi.org/10.55927/ministal.v4i3.14519

Akar, E. (2024). Emotional Artificial Intelligence: Introducing the Concept of 'Emotional Privacy.' In *Information Technology and Law Series* (hal. 65–87). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-639-0_4

Alrumaihi, D., Al-Hadi, O. F. A., & Rehman, S. U. (2025). Smart Criminal Justice Cognitive and Ethical Foundations for Trustworthy AI Systems. In *Advances in Computational Intelligence and Robotics* (hal. 35–56). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-5012-7.ch002

Amatucci, C., & Mollo, G. (2024). Sustainable Growth and the Role of Artificial Intelligence in Improving the Circular Economy. In *Law, Governance and Technology Series* (hal. 25–42). Springer International Publishing. https://doi.org/10.1007/978-3-031-51067-0_2

Bari, D. S. (2025). *A Comprehensive Review of Artificial Intelligence for Proactive and Adaptive Cybersecurity*. Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.36227/techrxiv.176339197.78312572/v1

Bhatta, U. (2025). MACHINE LEARNING (ML) TO EVALUATE GOVERNANCE, RISK, AND COMPLIANCE (GRC) RISKS ASSOCIATED WITH LARGE LANGUAGE MODELS (LLMs). In *Journal of Information Technology, Cybersecurity, and Artificial Intelligence* (Vol. 2, Nomor 2). Journal of Information Technology, Cybersecurity, and Artificial Intelligence. https://doi.org/10.70715/jitcai.2025.v2.i2.022

Bo, M. (2024). Meaningful human control: an international criminal law account. In *Research Handbook on Meaningful Human Control of Artificial Intelligence Systems* (hal. 148–160). Edward Elgar Publishing. https://doi.org/10.4337/9781802204131.00016

Botero, D. M. B. (2024). Inteligencia artificial: transformación digital en el derecho. In *Revista CES Derecho* (Vol. 15, Nomor 2, hal. 1–2). Universidad CES. https://doi.org/10.21615/cesder.7688

Buhrig, R. (2023). Capacity, capability, and collaboration: a qualitative analysis of international cybercrime investigations from the perspective of Canadian investigators. In *International Cybersecurity Law Review* (Vol. 4, Nomor 4, hal. 415–429). Springer Fachmedien Wiesbaden GmbH. https://doi.org/10.1365/s43439-023-00101-1

Cárdenas, E. R. (2024). La convergencia entre la inteligencia artificial y el derecho: desafíos y oportunidades. In *International Journal of Digital Law* (Vol. 5, Nomor 1, hal. 25–37). International Journal of Digital Law. https://doi.org/10.47975/digital.law.vol.5.n.1.cardenas

Changyuan, C. (2024). Reflections on the Shortcomings of the Use of Artificial Intelligence in Investigations. In *Criminal Justice Science & Governance* (Vol. 5, Nomor 2, hal. 27–33). Sciscan Publishing Limited. https://doi.org/10.35534/cjsg.0502004

Eble, K. (2024). Artificial Intelligence in Military Operations – Experiences and Challenges. The British Perspective. In *Cybersecurity and Law* (Vol. 11, Nomor 1, hal. 98–104). War Studies University. https://doi.org/10.35467/cal/187264

Feng, J., Zhao, L., Qin, H., Xu, Y., & Wang, Z. (2024). CADLRA: A multi-charge prediction method based on the Criminal Act-Driven Law Retrieval Augmentation. In *Engineering Applications of Artificial Intelligence* (Vol. 134, hal. 108619). Elsevier BV. https://doi.org/10.1016/j.engappai.2024.108619

Fitriani, L. (2024). Cybersecurity AND Digital Sovereignty: an Analysis OF National Data Governance Capacity in the GLOBAL Platform Era: A Literature Review. In *Asian Digital Governance Problems* (Vol. 1, Nomor 2, hal. 65–77). ScieClouds Publishing. https://doi.org/10.71435/685954

Flor, R., & Panattoni, B. (2023). Digital criminal investigations in Italy. The intersection between data protection and cybersecurity. In *New Journal of European Criminal Law* (Vol. 14, Nomor 4, hal. 479–494). SAGE Publications. https://doi.org/10.1177/20322844231212836

Gerstenfeld, J. (2023a). Understanding the Connection Between Hackers and Their Hacks: Analyzing USDOJ Reports for Hacker Profiles. In *International Journal of Cybersecurity Intelligence & Cybercrime* (Vol. 6, Nomor 1, hal. 59–76). Bridgewater State University. https://doi.org/10.52306/2578-3289.1157

Gerstenfeld, J. (2023b). Understanding the Connection Between Hackers and Their Hacks: Analyzing USDOJ Reports for Hacker Profiles. In *International Journal of Cybersecurity Intelligence and Cybercrime*. Bridgewater State University. https://doi.org/10.52306/nswy2537

Graham, C. M., & Lam, N. (2025). Warning or Liability? Cybersecurity Alerts as Legal Speech Acts in Risk and Forensic Contexts. In *Journal of Cybersecurity, Digital Forensics and Jurisprudence* (Vol. 1, hal. 55–64). United Scholars Publishing. https://doi.org/10.65879/3070-5789.2025.01.06

Gupta, D. (2025). The Invisible Defence. In *Digital Defence* (hal. 31–52). CRC Press. https://doi.org/10.1201/9781032714813-3

Haider, A., & Afzal, J. (2025). Understanding Cybersecurity Law in Data Sovereignty and Digital Governance by Melissa Lukings and Arash Habibi Lashkari. In *International Journal of Law and Legal Advancement* (Vol. 1, Nomor 1). Scientific Collaborative Online Publishing Universal Academy. https://doi.org/10.64060/ijlla.v1i1.3

Idrisov, N. T. (2025). Prohibitory norms of criminal law as a means of combating cybercrime and criminal use of artificial intelligence: current state and forecast. In *Juridical Journal of Samara University* (Vol. 11, Nomor 1, hal. 33–40). Samara National Research University. https://doi.org/10.18287/2542-047x-2025-11-1-33-40

Institute, B. C. L. (2023). Consultation Paper on Artificial Intelligence and Civil Liability. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.4572450

Karpiuk, M., Melchior, C., & Kaczmarek, K. (2024). A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data. In *PRAWO i WIĘŹ* (Nomor 3). Spółdzielczy Instytut Naukowy. https://doi.org/10.36128/priw.vi50.907

Kızılırmak, B. (2025). Conclusion and Extended Summary. In *Criminal Liability in Offenses Involving Autonomous Systems Driven by Artificial Intelligence* (hal. 415–442). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748965183-415

Łabuz, M. (2023). Regulating Deep Fakes in the Artificial Intelligence Act. In *Applied Cybersecurity & Internet Governance* (Vol. 2, Nomor 1, hal. 1–42). NASK National Research Institute. https://doi.org/10.60097/acig/162856

Lanz, M., & Mijic, S. (2023). Risks Associated with the Use of Natural Language Generation: Swiss Civil Liability Law Perspective. In *Law, Governance and Technology Series* (hal. 319–337). Springer International Publishing. https://doi.org/10.1007/978-3-031-41264-6_17

López, P. (2025). The National Security Framework as a Cybersecurity Reference for Information Cryptosystems. In *Law, Governance and Technology Series* (hal. 125–144). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74889-9_6

Magrani, E., & Silva, P. G. F. da. (2023). The Ethical and Legal Challenges of Recommender Systems Driven by Artificial Intelligence. In *Law, Governance and Technology Series* (hal. 141–168). Springer International Publishing. https://doi.org/10.1007/978-3-031-41264-6_8

Mahmud, K., Kumar, M., & Midha, O. P. (2024). AI in Healthcare: An International Quest for Criminal Liability in Medical Negligence Cases. In *2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI)* (hal. 1–5). IEEE. https://doi.org/10.1109/idicaiei61867.2024.10842755

Mandal, S., & Patra, S. K. (2024). *Artificial Intelligence and Cybersecurity: A Global Scenario*. MDPI AG. https://doi.org/10.20944/preprints202405.0415.v1

Medina, A. L. (2025). Applying Copyright Law to Artificial Intelligence. In *Journal of Science Policy & Governance* (Vol. 26, Nomor 1). Journal of Science Policy and Governance, Inc. https://doi.org/10.38126/jspg260105

Mezei, K. (2025). Artificial Intelligence in the Criminal Justice System: Exploring Risks and Opportunities Through the Lens of the European Union's AI Act. In *Data Science, Machine Intelligence, and Law* (hal. 131–146). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-86813-9_7

Minkova, L. G. (2023). *Responsibility on Trial*. Cambridge University Press. https://doi.org/10.1017/9781009320191

Moberg, A., & Gill-Pedro, E. (2024). Law and the Governance of Artificial Intelligence. In *YSEC Yearbook of Socio-Economic Constitutions* (hal. 1–13). Springer Nature Switzerland. https://doi.org/10.1007/16495_2024_69

Montasari, R. (2023). Countering Cyberterrorism. In *Advances in Information Security*. Springer International Publishing. https://doi.org/10.1007/978-3-031-21920-7

Moore, E., aslam, maria, javid, javid j, & Jack, W. (2025). *Navigating Digital Compliance in Islamic Finance: Integrating Medical Ethics, Cybersecurity, and Criminal Law Across Jurisdictions*. Elsevier BV. https://doi.org/10.2139/ssrn.5363130

Mrčela, M., & Vuletić, I. (2025). Navigating Criminal Liability in an Era Of AI-Assisted Medicine. In *Medicine, Law & Society* (Vol. 18, Nomor 1). University of Maribor. https://doi.org/10.18690/mls.18.1.93-108.2025

Mtuze, S. S. ka. (2023). Dr. Ifeoma Nwafor: Cybercrime and the law: issues and developments in Nigeria. (2022) CLDS Publishing. pp. 1–285. In *International Cybersecurity Law Review* (Vol. 4, Nomor 2, hal. 253–254). Springer Fachmedien Wiesbaden GmbH. https://doi.org/10.1365/s43439-023-00080-3

Mugamba, E. (2025). GLOBAL DATA GOVERNANCE IN DIGITAL LAW: A COMPARATIVE ANALYSIS OF EU AND GLOBAL APPROACHES TO CYBERSECURITY LEGISLATION. In *Journal of Smart Computing and Quantum Technologies* (Vol. 1, Nomor 1, hal. 1–19). Tresearch. https://doi.org/10.63456/jscqt-1-1-39

Muniyappan, H., M, R., & Pavithra, S. (2025). Enhancing Cybersecurity in Digital Twin Systems: Mitigating Challenges and Defending Against Threats. In *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)* (hal. 1–6). IEEE. https://doi.org/10.1109/icdsaai65575.2025.11011764

Nascimento, K. B. S. do, & Sousa, K. R. da S. (2025). Entre a Privacidade e o Cibercrime: A Insuficiência Penal na Era dos Dados. In *RCMOS - Revista Científica Multidisciplinar O Saber* (Vol. 1, Nomor 1). Editora Aluz. https://doi.org/10.51473/rcmos.v1i1.2025.1750

Neuhaeusler, N. S. (2024). Cyberbullying During COVID-19 Pandemic: Relation to Perceived Social Isolation Among College and University Students. In *International Journal of Cybersecurity Intelligence & Cybercrime* (Vol. 7, Nomor 1). Bridgewater State University. https://doi.org/10.52306/2578-3289.1140

Papa, L. de B. I. (2025). Criminal Compliance and Corporate Criminal Liability: Perspectives for Preventive Protection of Human Rights in the Corporate Sphere. In *IBCCrim Studies in Criminal Law, Human Rights and Criminology* (hal. 81–119). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-06213-0_4

PhD, R. G. Y. (2025). *Artificial Intelligence and Machine Learning in Cybersecurity*. Productivity Press. https://doi.org/10.4324/9781003615026

Prifti, K., Demir, E., Krämer, J., Heine, K., & Stamhuis, E. (2024). Digital Governance. In *Information Technology and Law Series*. T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-639-0

salim, A., Santosa, T. A., Ghoni, A., Kadir, T., & Wijoyo, H. (2025). Restorative Justice in Contemporary Criminal Law: Comparative Perspectives and Emerging Trends. In *RIGGS: Journal of Artificial Intelligence and Digital Business* (Vol. 4, Nomor 3, hal. 6116–6121). Universitas Pahlawan Tuanku Tambusai. https://doi.org/10.31004/riggs.v4i3.2900

Schollaert, V., & Bruyne, J. De. (2025). Legal Personality for AI Systems and Robots from a Belgian Civil (Extra-Contractual) Liability Perspective. In *Artificial Intelligence, Humans and the Law* (hal. 195–225). Routledge. https://doi.org/10.4324/9781003565963-15

Sela-Shayovitz, R., Berenblum, T., & Toys, S. (2025). Cyber Offending among Adolescents: The Role of Thoughtfully Reflective Decision-Making and Victimization. In *International Journal of Cybersecurity Intelligence & Cybercrime* (Vol. 8, Nomor 1). Bridgewater State University. https://doi.org/10.52306/2578-3289.1177

Shutova, A. A. (2024). Criminal Risks of the Use of Artificial Intelligence Technologies in Healthcare. In *Business security* (Vol. 1, hal. 52–57). The Publishing Group Jurist. https://doi.org/10.18572/2072-3644-2024-52-57

STĂNCIULESCU, A. (2023). Open-Source Intelligence - Useful Tools in Data Analysis. In *Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)*. Romanian Association for Information Security Assurance. https://doi.org/10.19107/cybercon.2023.25

Sutter, G. (2025). Cybersecurity Law. In *Financial Technology and Digital Commercial Law* (hal. 586–612). Oxford University Press. https://doi.org/10.1093/law/9780192868763.003.0025

Syta, J. (2025). A comprehensive review of effective methods for counteracting cybercrime. In *Cybersecurity and Law* (Vol. 14, Nomor 2, hal. 304–323). War Studies University. https://doi.org/10.35467/cal/215963

Teymoorikia, M., Jahanbakhshi, H. A., & Esmaeili, M. (2025). Obstacles to Criminal Liability Arising from Discipline and Punishment: A Comparative Study of Iranian and Egyptian Criminal Law. In *Legal Studies in Digital Age* (hal. 1–17). KMAN Publication Incorporation. https://doi.org/10.61838/kman.lsda.270

Tiwari, G., Pandey, K., Desai, M., Musale, V., Wategaonkar, D., & Bedekar, M. (2025). The Legal and Ethical Crossroads of Artificial Intelligence in Cybersecurity and Digital Forensics. In *Digital Defence* (hal. 93–110). CRC Press. https://doi.org/10.1201/9781032714813-6

Tommaso, A. De. (2023). Translating Corporate Criminal Liability into the International Criminal Justice System. In *Corporate Liability and International Criminal Law* (hal. 191–234). Routledge. https://doi.org/10.4324/9781003390534-7

Tripathi, P., & Saxena, P. (2024). An Assessment of the Role of Artificial Intelligence on Sustainable Development Goals. In *Law, Governance and Technology Series* (hal. 3–23). Springer International Publishing. https://doi.org/10.1007/978-3-031-51067-0_1

Triwanto, T., & Aryani, E. (2024). CORPORATE CRIMINAL LIABILITY IN CORRUPTION CRIMES ACCORDING TO POSITIVE LAW AND LAW NO 1 OF 2023 CONCERNING THE CRIMINAL LAW BOOK (KUHP). In *Cognizance Journal of Multidisciplinary Studies* (Vol. 4, Nomor 1, hal. 39–47). Zain Publications. https://doi.org/10.47760/cognizance.2024.v04i01.004

Turner, J., & Bergson, I. (2025). Artificial Intelligence and FinTech Law. In *Financial Technology and Digital Commercial Law* (hal. 311–343). Oxford University Press. https://doi.org/10.1093/law/9780192868763.003.0014

Wang, M. (2025). China's Governance Framework on Generative Artificial Intelligence. In *Journal of AI Law and Regulation* (Vol. 2, Nomor 4, hal. 402–407). Lexxion Verlag. https://doi.org/10.21552/aire/2025/4/13

Wang, X., Yang, J., & Jia, M. (2025). Research on Military Artificial Intelligence Risk Governance. In *Proceedings of the 2025 2nd International Conference on Digital Society and Artificial Intelligence* (hal. 657–660). ACM. https://doi.org/10.1145/3748825.3748926

Ye, Z., & Li, J. (2024). Artificial Intelligence Through the Lens of Metaphor: Analyzing the EU AIA. In *International Journal of Digital Law and Governance* (Vol. 1, Nomor 2, hal. 361–381). Walter de Gruyter GmbH. https://doi.org/10.1515/ijdlg-2024-0016

Zangana, H. M., Omar, M., Rangarajan, A., & Hasan, B. M. S. (2025). Natural Language Processing for Analyzing Criminal Communication and Cyber Threat Intelligence. In *Advances in Computational Intelligence and Robotics* (hal. 1–30). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-6536-7.ch001

Zdrojewski, K. (2025). Between Innovation and Control: Legal Frameworks for the Use of Artificial Intelligence in Armed Conflict. In *Cybersecurity and Law* (Vol. 13, Nomor 1, hal. 133–145). War Studies University. https://doi.org/10.35467/cal/214603

Zhong, H., Xie, F., Yu, L., Wang, X., Xie, Q., & Sok, M. (2025). AI-Driven Cybersecurity Threat Detection: A Hybrid CNN-LSTM Deep Learning Approach. In *2025 International Conference on Artificial Intelligence Security and Governance (ICAISG)* (hal. 80–85). IEEE. https://doi.org/10.1109/icaisg68699.2025.11452139