International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838
Received: 22-11-2025, Accepted: 16-01-2026, Published: 31-01-2026
Volume 8, Issue 1, 2026, Page No. 81-86

Criminal liability of perpetrators of digital fraud using artificial intelligence-based deepfake technology

Thessa Yudha Dewanta Putra, Hatarto Pakpahan, Leni Dwi Nurmala
University of Merdeka Malang, Indonesia

Abstract
the development of artificial intelligence-based deepfake technology has given rise to a new form of digital fraud that is increasingly complex and difficult to detect. the ability of this technology to manipulate identity through synthetic images, voices, and videos that appear authentic poses serious challenges to the criminal justice system. this study aims to analyze the indonesian positive law framework for addressing deepfake-based digital fraud, assess the adequacy of existing concepts of criminal liability, and compare this regulation with those adopted in several other jurisdictions. this research employs a normative legal research method, drawing on statutory, conceptual, case, and comparative approaches. the findings indicate that, to date, indonesia has not enacted a specific, comprehensive regulatory framework governing digital fraud involving deepfake technology. law enforcement efforts continue to rely on general provisions under law number 1 of 1946 concerning the criminal code, law number 1 of 2023 concerning the criminal code, and law number 1 of 2024 concerning the second amendment to law number 11 of 2008 on electronic information and transactions, all of which were not designed to address the complexity of artificial intelligence–based digital identity manipulation. furthermore, the existing model of criminal liability remains predominantly oriented toward individual perpetrators as the sole subjects of criminal responsibility. accordingly, this study underscores the urgency of reforming criminal law policy in a more adaptive, preventive, and systemic manner in order to enhance legal certainty and the effectiveness of law enforcement in combating deepfake-based digital fraud.

Keywords: Criminal liability, digital fraud, deepfake, artificial intelligence, indonesian criminal law

Introduction

The development of artificial intelligence–based digital technology has brought significant changes to patterns of crime in cyberspace. One technology that poses serious challenges to the criminal law system is deepfake, namely a technique for manipulating images, voices, and videos generated through artificial intelligence algorithms, enabling the creation of digital representations that appear authentic, despite being entirely the product of artificial fabrication (Goodfellow *et al*., 2014) [16]. In practice, deepfake technology is not only used for creative purposes and the entertainment industry, but is also increasingly exploited for digital fraud that causes widespread harm to the public. (Ajder *et al*., 2019) [1].

Deepfake-based digital fraud exhibits characteristics fundamentally different from those of conventional fraud. This technology enables perpetrators to create compelling false identities, including those resembling public figures, state officials, or other individuals holding positions of authority. As a result, victims are more likely to trust the information or instructions conveyed through such manipulative content. Europol has even emphasized that deepfake technology has been employed in various cybercrime schemes, including social engineering and identity-based fraud (Europol Innovation Lab, 2022) [13]. This condition demonstrates that deepfake technology is not merely an auxiliary tool for crime but has evolved into a new modus operandi for fraud in the digital era.

Within the framework of Indonesian positive law, the regulation of deepfake-based digital fraud remains fragmented. The criminal provisions commonly invoked to prosecute perpetrators are derived from Law Number 1 of 1946 concerning the Criminal Code, Law Number 1 of 2023 concerning the Criminal Code, and Law Number 11 of 2008 on Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024. However, these regulations do not explicitly address deepfake technology or artificial intelligence-based synthetic content, either in terms of definitions, conduct classification, or the construction of criminal liability (Makarim, 2013) [23].

The absence of specific regulation creates practical difficulties for law enforcement, particularly in proving the elements of the unlawful act (actus reus) and the perpetrator's fault (mens rea). Deepfake-based fraud involves complex technological processes and often engages multiple actors, ranging from system designers and technology operators to end users and digital platform providers. Nevertheless, Indonesian criminal law continues to adhere predominantly to an individualistic model of criminal liability, oriented toward a single perpetrator, and therefore has yet to adequately capture the functional and structural relationships inherent in artificial intelligence-based crimes (Hamzah, 2008) [17].

Compared with legal developments in several other countries, a paradigm shift is evident in responses to the misuse of artificial intelligence. The European Union, for instance, through the Artificial Intelligence Act, has classified artificial intelligence systems by risk level, established transparency obligations, and set labeling requirements for synthetic content (European Union, 2024) [12]. Meanwhile, the People's Republic of China has imposed obligations on deep synthesis service providers to implement labeling measures and internal oversight to prevent the misuse of such technology (Cyberspace

Administration of China, 2023) [11]. These developments indicate that legal approaches to deepfake-related crime are no longer purely repressive but have increasingly adopted preventive and systemic dimensions.

Based on these conditions, it can be concluded that deepfake-based digital fraud constitutes a new criminal phenomenon that has not yet been fully accommodated within Indonesian positive law. This situation calls for an urgent in-depth examination of the existing legal framework and the construction of criminal liability applicable to the parties involved. Such an inquiry is essential not only to strengthen legal certainty but also to promote reform of national criminal law, making it more adaptive and responsive to developments in artificial intelligence and the growing complexity of digital crime (Arief, 2011) [4].

Research Methods

This study employs a normative legal research method to examine and analyze the legal framework and the concept of criminal liability in deepfake-based digital fraud. Normative legal research is selected because the study focuses on the analysis of positive legal norms, legal doctrines, and criminal law principles relevant to the development of artificial intelligence technology (Marzuki, 2017) [25]. The research approaches employed include the statutory, conceptual, case, and comparative approaches. (Ibrahim, 2006) [21]. The statutory approach is conducted by examining relevant legal provisions, particularly Law Number 1 of 2023 concerning the Criminal Code, Law Number 1 of 1946 concerning the Criminal Code, and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, in order to assess the adequacy of existing norms in regulating deepfake-based digital fraud. The conceptual approach is employed to analyze doctrines and theories of criminal law, especially the concepts of actus reus and mens rea, as well as theories of criminal liability in the context of technology-based crime (Sudarto, 1986) [31]. The case approach is applied through the analysis of court decisions on digital fraud and cybercrime to understand the concrete application of legal norms in judicial practice. Meanwhile, the comparative approach is utilized by comparing the legal regulation of deepfake technology and artificial intelligence in Indonesia with the regulatory frameworks of the European Union and the People's Republic of China, serving as a basis for evaluation and for formulating recommendations for the reform of national criminal law (Van Hoecke, 2011) [32] The legal materials used in this study consist of primary, secondary, and tertiary legal materials (Soekanto & Mamudji, 2006) [30]. All legal materials are analyzed qualitatively using prescriptive and argumentative legal reasoning methods to draw conclusions and formulate criminal law policy recommendations that are adaptive to developments in digital technology.

Results and Discussion

1. Legal Regulation of Deepfake-Based Digital Fraud under Indonesian Positive Law

The findings of this study indicate that, to date, Indonesian positive law has not established specific, explicit regulations governing deepfake technology or synthetic content generated by artificial intelligence. The handling of deepfake-based digital fraud continues to rely on general provisions contained in Law Number 1 of 1946 concerning the Criminal Code, Law Number 1 of 2023 concerning the Criminal Code, and Law Number 11 of 2008 on Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024. These provisions were formulated to address conventional forms of crime and, as such, are not yet fully capable of responding to the challenges posed by complex digital identity manipulation enabled by artificial intelligence technology (Sudarto, 1986) [31].

The absence of a normative definition of deepfake technology and synthetic content results in a lack of clear legal standards for determining the boundary between lawful digital content and criminal manipulative conduct. Consequently, law enforcement authorities are compelled to rely on analogical interpretations of conventional fraud provisions. This condition has the potential to generate legal uncertainty, divergent interpretations, and inconsistencies in the application of the law, particularly when addressing the evidentiary requirements for proving unlawful acts in the anonymous, cross-border nature of cyberspace (Arief, 2014) [5].

The results of this study underscore that Indonesia's criminal law framework remains largely reactive and has not yet adapted to the rapid development of digital technology. Without more specific regulatory reforms, criminal law risks lagging behind the evolving modus operandi of digital fraud facilitated by deepfake technology (Marzuki, 2016) [24].

2. Comparison of Legal Regulation on Deepfake-Based Digital Fraud between the European Union and China

From a comparative law perspective, the findings of this study indicate that Indonesia's regulatory response to deepfake-based digital fraud remains relatively underdeveloped when compared to several other jurisdictions. Several countries have already formulated legal policies that specifically regulate the use of artificial intelligence technology, including transparency obligations for synthetic content, oversight of technology providers, and mechanisms to prevent the misuse of high-risk technologies (Hildebrandt, 2015) [19].

These countries no longer regard deepfake-based digital fraud merely as a variation of conventional fraud, but rather as a new form of crime with distinct technological and social characteristics. Accordingly, regulatory measures are directed not only at direct perpetrators, but also at parties who exercise control over the development, operation, and distribution of artificial intelligence technology. (Yeung & Lodge, 2019) [34].

This comparison reveals a shift from predominantly repressive regulation toward a more preventive, systemic approach. In contrast, Indonesia continues to situate deepfake-based digital fraud within the general criminal law framework, without developing a specific legal policy that accounts for the complexity of artificial intelligence. This gap highlights the need to reformulate national legal policy to align it with global developments (Floridi *et al*., 2018) [15].

3. Criminal Liability for Deepfake-Based Digital Fraud under Indonesian Positive Law

The findings of this study indicate that criminal liability for deepfake-based digital fraud under Indonesian positive law remains oriented toward individual perpetrators as the sole

subjects of criminal responsibility. The criminal provisions contained in Law Number 1 of 1946 concerning the Criminal Code, Law Number 1 of 2023 concerning the Criminal Code, and Law Number 11 of 2008 on Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024, do not explicitly regulate the differentiation of criminal liability based on the functions and roles of the parties involved in the use of deepfake technology, such as system designers, technology operators, users, and digital platform providers (Saleh, 1983) [29].

This approach is consistent with the classical character of Indonesian criminal law, which grounds punishment on fault. Criminal liability can only be imposed on human actors who commit unlawful acts and possess personal culpability that can be individually attributed. Within this framework, deepfake technology is positioned merely as a tool or instrument, rather than as an element that normatively influences the structure of criminal liability (Hamzah, 2008) [17].

In law enforcement practice, this single-perpetrator orientation results in criminal liability being primarily directed at parties who directly use or disseminate deepfake content. Meanwhile, other actors who make structural contributions to the production, operation, and distribution of manipulative content often fall outside the scope of criminal responsibility. This condition demonstrates that Indonesian criminal law continues to adhere to an individualistic model of liability and has yet to address the complexity of digital crimes involving artificial intelligence adequately. (Brenner, 2010) [6, 7].

Furthermore, the existing regulatory framework does not yet impose specific preventive obligations on artificial intelligence technology providers, such as duties related to risk mitigation, internal supervision, or the labeling of synthetic content. As a result, criminal liability may only be imposed on technology providers where direct involvement or intent can be proven, thereby reinforcing the reactive character of the current criminal law system (Hartzog, 2018) [18].

Based on the overall findings and discussion, it can be concluded that Indonesian criminal law is not yet fully prepared to address deepfake-based digital fraud, which is complex, systemic, and involves multiple actors. Therefore, the reform of criminal law policy is an urgent necessity to ensure criminal liability is formulated in a more adaptive, proportional, and relevant manner, in line with developments in artificial intelligence technology, without disregarding the fundamental principle of fault in criminal law (Husak, 2010) [20].

4. Characteristics of Deepfake-Based Digital Fraud as a Modern Crime

Deepfake-based digital fraud exhibits characteristics fundamentally different from those of conventional fraud as understood in classical criminal law. In conventional fraud, the relationship between the perpetrator and the victim is generally direct, whether through face-to-face communication or personal interaction that allows for relatively easy identification of the perpetrator. By contrast, in deepfake-based fraud, perpetrators exploit artificial intelligence technology to create entirely manipulative digital identity representations, thereby rendering the relationship between perpetrator and victim indirect and mediated by technological systems (Brenner, 2010) [6, 7].

The primary characteristic of deepfake-based fraud lies in the manipulation of digital identity that is persuasive and difficult to distinguish from reality. This technology enables the creation of images, voices, or videos that closely resemble specific individuals, with a high degree of credibility, leading victims to assess the truthfulness of information not on rational grounds but on trust in the identity being presented. In this context, deepfake technology does not merely function as an auxiliary tool for crime, but has become an integral component of the fraudulent modus operandi itself (Citron, 2019) [10].

Furthermore, deepfake-based fraud is distinguished by the attenuation of a direct causal link between the actor's conduct and the resultant harm. The commission of such offenses frequently involves automated systems, machine learning algorithms, and cross-platform digital infrastructures. Consequently, liability cannot always be ascribed to a discrete individual act but instead emerges from a complex sequence of technological processes.

This characteristic poses a serious challenge to criminal law, which has traditionally been founded on the assumption of concrete human actions that are observable and directly ascertainable (Pasquale, 2015) [27]. Accordingly, deepfake-based digital fraud may be classified as a form of modern crime that challenges the paradigms of conventional criminal law. Such offenses rely not only on the malicious intent of the perpetrator but also exploit structural vulnerabilities in technological systems and the low level of digital literacy among the public, thereby necessitating a more adaptive and context-sensitive legal approach.

5. Evidentiary Challenges in Deepfake-Based Digital Fraud Cases

One of the most critical issues in handling deepfake-based digital fraud cases lies in the realm of evidence. In criminal law, establishing proof is the core of the enforcement process, as it determines whether an individual can be held criminally liable. However, the nature of deepfake technology poses specific challenges in proving the elements of unlawful conduct (*actus reus*) and criminal intent (*mens rea*) (Kerr, 2005) [22].

Proving the element of criminal intent (*mens rea*) becomes particularly problematic due to the separation of roles among the system designers, technology operators, and those who exploit the outputs. In many instances, the individuals who derive benefits from the fraud are not the same parties who technically create the deepfake content. This situation complicates the establishment of personal malicious intent, especially when perpetrators shield themselves behind digital anonymity and automated systems (Brenner & Clarke, 2005) [8].

Moreover, the authentication of digital content presents a distinct challenge. Deepfakes are engineered to closely mimic authentic material, thereby requiring specialized technical expertise and digital forensic methods to demonstrate manipulation. Law enforcement authorities often face resource and technical competence limitations when verifying synthetic content, which may ultimately weaken their evidentiary position in court proceedings (Farid, 2008) [14].

These evidentiary challenges demonstrate that deepfake fraud cannot be treated in the same manner as conventional fraud. Criminal law is therefore compelled to develop a more contextual approach to proof, including enhancing

expert involvement, establishing digital evidentiary standards, and ensuring an adequate understanding of the complexity of technological systems in determining criminal liability.

6. Limitations of the Single Actor Criminal Liability Model under the Electronic Information and Transactions Law

The criminal provisions under Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions fundamentally adhere to a single-actor criminal liability model, in which the legal subject held accountable is the direct perpetrator who commits the criminal act. This model is consistent with the classical principles of criminal law, which place personal culpability as the primary basis for punishment. (Hamzah, 2008) [17].

However, the application of the single-actor criminal liability model becomes problematic when confronted with deepfake crimes that involve a chain of actors and complex technological systems. In practice, deepfake fraud often involves multiple parties, including technology developers, system operators, content users, and digital platform providers. Nevertheless, Indonesian positive law has yet to establish a normative framework that differentiates criminal responsibility based on each party's function and degree of control (Arief, 2011) [4].

These limitations result in criminal liability being imposed on the party most easily identifiable, namely the end user of deepfake content. Meanwhile, other actors who play strategic roles in enabling the commission of the crime often remain beyond the reach of criminal law. This situation reflects the constraints of national criminal law in responding to technologically based, systemic, and distributed crimes.

Consequently, the single-actor criminal liability model as adopted under the Electronic Information and Transactions Law warrants reconsideration to ensure greater relevance to the nature of modern digital crimes, without disregarding the fundamental principle of culpability in criminal law.

7. Analysis of Case No. 124/Pid.B/2025/PN Gns Concerning Deepfake-Based Digital Fraud

The Gunung Sugih District Court Decision No. 124/Pid.B/2025/PN Gns represents a significant ruling in Indonesian criminal jurisprudence as it substantively addresses fraud offenses that exploit deepfake technology based on Artificial Intelligence. The decision demonstrates that, although Indonesian positive law has yet to regulate algorithmically generated visual and audio manipulations explicitly, the judiciary has nonetheless sought to bridge the normative gap by applying the Electronic Information and Transactions Law, as permitted within the framework of evolving criminal law interpretation (Arief, 2010) [3].

7.1. Reconstruction of Facts and Legal Position of the Case

In this case, the defendant, Almandela, was proven to have created and disseminated deepfake videos depicting the President, Vice President, and other state officials as if they were issuing official instructions to the public to transfer funds in order to receive certain assistance. The visual and audio manipulations closely resembled authentic statements by public officials and successfully fostered the victims' trust.

These legal facts were established through the testimony of the victims, the examination of electronic evidence, and the expert testimony of digital forensic specialists, who confirmed that the videos in question were the result of deepfake manipulation. Such a pattern of criminal conduct aligns with the characteristics of modern cybercrime, which exploits digital identity manipulation to create a simulated reality and mislead victims (Brenner, 2010) [6, 7]. Accordingly, the legal position in this case clearly falls within the category of fraud involving the manipulation of electronic information.

7.2. Application of Article 35 in Conjunction with Article 51(1) of Law Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions

The Panel of Judges based the defendant's criminal liability on Article 35 in conjunction with Article 51(1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions. Article 35 prohibits the manipulation or creation of electronic information in a manner that renders the data seemingly authentic, while Article 51(1) prescribes a maximum prison sentence of twelve years. In the context of deepfakes, the defendant's manipulation was not merely technical but also substantive, producing digital content capable of shaping a false perception among the public.

The Panel of Judges interpreted the phrase “seemingly authentic data” broadly to encompass AI-generated synthetic content. Such an interpretation remains within the permissible boundaries of criminal law, provided that it does not create a new offense and remains grounded in the rational meaning of the statutory norm (Moeljatno, 2015) [26]. This approach aligns with the view that criminal law must be capable of protecting society's legal interests against criminal schemes that evolve alongside technological advancements (Arief, 2008) [2].

7.3. Analysis of the Elements of Actus Reus and Mens Rea

From the perspective of criminal liability theory, this ruling demonstrates the clear fulfillment of both the actus reus and mens rea elements. The actus reus is reflected in the defendant's active conduct in creating and disseminating false digital content through social media and instant messaging applications. Such conduct constitutes the manipulation of electronic information that directly causes financial harm to victims, thereby satisfying the characteristics of a criminal act in cybercrime (Wall, 2007) [33].

The mens rea element is evident from the presence of direct intent (dolus directus), as reflected in the defendant’s choice to employ deepfake technology due to its ability to produce content that is convincing and difficult to distinguish from authentic material. The economic motive, coupled with a pattern of premeditated actions, indicates an intention to deceive, as required under the theory of culpability in criminal law (Saleh, 1983) [29]. No circumstances were found that would negate culpability, and therefore, full criminal liability can be attributed to the defendant.

7.4. Legal Evidence and the Role of Digital Forensic Experts

The decision also underscores the strategic role of scientific evidence in technology-based crime cases. Testimony from digital forensic experts was employed to identify data structures, metadata, and visual and audio distortions that authentic recordings could not have produced. In cybercrime cases, digital evidence plays a central role, enabling the court to understand the technical processes underlying the criminal conduct (Casey, 2011) [9]. The success of evidence in this case demonstrates that, despite the increasing sophistication of deepfake technology, synthetic content can be detected through scientific approaches. This reinforces the view that criminal law retains its reach in addressing crimes involving artificial intelligence.

7.5. Relation to Article 378 of Law No. 1 of 1946 on the Penal Code and Article 492 of Law No. 1 of 2023 on the Penal Code

Although the indictment did not invoke Article 378 of the Penal Code, the elements of conventional fraud were essentially satisfied, including deceit, the use of false identities, and actions that induced the victims to surrender their property. This demonstrates that deepfake-based fraud constitutes an evolution of the classic fraud modus operandi through digital technology. In relation to Article 492 of Law No. 1 of 2023 on the Penal Code, which comes into effect in 2026, the defendant's conduct also fulfills the elements of the offense of fraud. However, these provisions remain oriented toward conventional fraud patterns and do not yet explicitly address algorithmic manipulation driven by artificial intelligence. Therefore, supporting technical regulations are necessary to ensure that the fraud provisions in the Penal Code can be applied with greater precision to generative digital crimes.

7.6. Academic Relevance of the Ruling for Deepfake Regulation in Indonesia

From an academic perspective, this ruling demonstrates that Indonesian criminal law does not suffer from a legal vacuum. However, it is instead characterized by insufficient regulation, with norms that are not yet fully adaptive to the complexities of emerging technologies. The decision confirms that the Electronic Information and Transactions law can still serve as a basis for criminal liability; however, long-term legal certainty requires more explicit regulations regarding the use and misuse of deepfake technology. Accordingly, the analysis of this ruling functions not only as an illustration of judicial practice but also as an academic foundation for the development of criminal law policy and artificial intelligence regulation in Indonesia, aiming to make it more responsive to the dynamics of digital crime.

7.7. Implications of the Individual Criminal Liability System in Deepfake-Based Digital Fraud

Research findings indicate that the criminal liability system in Indonesian positive law remains oriented toward the individual perpetrator as the sole subject of criminal responsibility. This pattern is rooted in the classical character of Indonesian criminal law, which places the principle of culpability (geen straf zonder schuld) as the primary foundation for punishment. Consequently, liability can only be imposed on a human actor who directly commits the unlawful act and possesses personally attributable culpability (Hamzah, 2008) [17].

In this context, deepfake technology is positioned merely as a tool or means of committing the offense, rather than as a factor that normatively influences the structure of criminal liability. This individualistic approach carries profound implications when applied to deepfake-based digital fraud, which inherently involves complex, multilayered technological processes. Deepfake crimes do not depend solely on the actions of end users but also involve the roles of system designers, technology operators, and digital platform providers that supply infrastructure and artificial intelligence algorithms.

Nonetheless, the criminal provisions in the Penal Code, as well as in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, have yet to provide a clear normative basis for differentiating criminal liability according to the roles and levels of control exercised by the various actors (Arief, 2011) [4]. As a result, in law enforcement practice, criminal liability tends to focus on perpetrators who directly use or disseminate deepfake content for fraudulent purposes. Meanwhile, other actors who have structural contributions and exert significant influence over the commission of the crime often remain beyond the reach of criminal law.

This situation highlights the gap between the classical model of criminal liability and the realities of modern digital crime, which are systemic and technology-based (Brenner, 2010) [6, 7]. Furthermore, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions does not yet regulate specific preventive obligations for providers of artificial intelligence technology, such as risk mitigation, internal oversight, or labeling of synthetic content. The absence of such regulations means that criminal liability for technology providers can be imposed only if direct involvement or intent is proven, underscoring the reactive nature of the Indonesian criminal law system (Makarim, 2013) [23].

From the perspective of modern criminal law theory, this situation demonstrates the need to shift from purely individual liability to a more functional, contextual model of responsibility. Several scholars emphasize that criminal law must adapt to technological developments and increasingly complex crime structures without disregarding the fundamental principle of culpability (Rahardjo, 2009) [28]. Accordingly, reforming criminal law policy is essential to ensure the criminal liability system encompasses all actors who contribute significantly to deepfake-based digital fraud, while simultaneously preserving legal certainty and justice.

Conclusion

Based on the findings and discussion, it can be concluded that Indonesian positive law has not yet established a specific and comprehensive regulatory framework for deepfake-based digital fraud. The handling of this form of crime still relies on general provisions in Law Number 1 of 1946 on the Penal Code, Law Number 1 of 2023 on the Penal Code, and Law Number 11 of 2008 on Electronic Information and Transactions, as last amended by Law Number 1 of 2024. These provisions were not designed to address the complexities of digitally manipulated identities generated by artificial intelligence, and therefore have not

provided legal certainty or optimal law enforcement effectiveness against deepfake-based digital fraud. Comparative legal analysis shows that several other jurisdictions have developed more progressive and adaptive regulations to address the risks posed by AI misuse.

These countries not only criminalize deepfake-based digital fraud but also impose preventive obligations on technology providers and digital platforms, including transparency requirements, synthetic content labeling, internal oversight, and risk-mitigation measures. This approach reflects a paradigm shift from purely repressive law enforcement toward more preventive and systemic legal policy. By contrast, Indonesia still classifies deepfake-based digital fraud within the general criminal law framework, without specific regulations, leaving it behind in terms of legal certainty and technological crime prevention. Furthermore, criminal liability for deepfake-based digital fraud in Indonesian law remains oriented toward the individual perpetrator as the sole subject of responsibility. Deepfake technology is presented merely as a tool for committing the offense, rather than as a factor that shapes the structure of criminal liability.

Consequently, criminal law has not yet accommodated the allocation of responsibility based on the functions and roles of the parties involved in the use of artificial intelligence technology, such as system designers, technology operators, end users, and digital platform providers. This approach contrasts with trends in several other countries that are beginning to develop more functional, tiered models of liability based on the level of control and contribution of each actor. Accordingly, it can be affirmed that Indonesian criminal law still faces serious challenges in addressing the evolution of technology-based digital crimes such as deepfake fraud. Reform of criminal law policy has become an urgent necessity so that the national legal framework is not only reactive but also capable of adopting preventive and systemic approaches, as reflected in international practice. Such reform is needed to strengthen legal certainty, enhance law enforcement effectiveness, and provide optimal protection for society against threats posed by artificial intelligence–based digital fraud, without disregarding the fundamental principle of culpability in criminal law.

References

1. Ajder H, Patrini G, Cavalli F, Cullen L. The State of Deepfakes: Landscape, Threats, and Impact, 2019.
2. Arief BN. Masalah Penegakan Hukum dan Kebijakan Hukum Pidana. Kencana, 2008.
3. Arief BN. Bunga Rampai Kebijakan Hukum Pidana (3rd ed.). Kencana, 2010.
4. Arief BN. Masalah Penegakan Hukum dan Kebijakan Hukum Pidana. Kencana, 2011.
5. Arief BN. Bunga Rampai Kebijakan Hukum Pidana:(Perkembangan Penyusunan Konsep KUHP Baru), 2014. library.stik-ptik.ac.id. https://library.stik-ptik.ac.id/detail?id=49266&lokasi=lokal
6. Brenner SW. Cybercrime and the Law. Northeastern University Press, 2010.
7. Brenner SW. Cybercrime: Criminal Threats from Cyberspace. Praeger, 2010.
8. Brenner SW, Clarke LL. Distributed Security: Preventing Cybercrime. John Marshall Journal of Computer & Information Law,2005:23:659–710.
9. Casey E. Digital Evidence and Computer Crime (3rd ed.). Academic Press, 2011.
10. Citron DK. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review,2019:107(6):1753–1819.
11. Cyberspace Administration of China. Interim Measures for the Management of Generative Artificial Intelligence Services, 2023.
12. European Union. Artificial Intelligence Act, 2024.
13. Europol Innovation Lab. Facing Reality? Law Enforcement and the Challenge of Deepfakes, 2022.
14. Farid H. Digital Image Forensics. Scientific American,2008:298(6):66–71.
15. Floridi L, Cowls J, Beltrametti M, Chatila R. Artificial Intelligence and the Ethics of Responsibility. Philosophy & Technology, 2018, 31(1).
16. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, *et al*. Generative Adversarial Nets. Advances in Neural Information Processing Systems, 2014, 27.
17. Hamzah A. Asas-Asas Hukum Pidana. Rineka Cipta, 2008.
18. Hartzog W. Privacy's Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press, 2018.
19. Hildebrandt M. Smart Technologies and the End(s) of Law. Edward Elgar, 2015.
20. Husak D. Philosophy of Criminal Law. Oxford University Press, 2010.
21. Ibrahim J. Teori dan Metodologi Penelitian Hukum Normatif. Bayumedia, 2006.
22. Kerr OS. Digital Evidence and the New Criminal Procedure. Columbia Law Review,2005:105(1):279–318.
23. Makarim E. Hukum Telematika. RajaGrafindo Persada, 2013.
24. Marzuki PM. Pengantar Ilmu Hukum. Kencana, 2016.
25. Marzuki PM. Penelitian Hukum (Revisi). Kencana, 2017.
26. Moeljatno. Asas-Asas Hukum Pidana (9th ed.). Rineka Cipta, 2015.
27. Pasquale F. The Black Box Society: The Secret algorithms That Control Money and Information. Harvard University Press, 2015.
28. Rahardjo S. Hukum Progresif: Sebuah Sintesa Hukum Indonesia. Genta Publishing, 2009.
29. Saleh R. Perbuatan Pidana dan Pertanggungjawaban Pidana. Aksara Baru, 1983.
30. Soekanto S, Mamudji S. Penelitian Hukum Normatif: Suatu Tinjauan Singkat. RajaGrafindo Persada, 2006.
31. Sudarto. Hukum dan Hukum Pidana. Alums, 1986.
32. Van Hoecke M. (Ed.). Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline? Hart Publishing, 2011.
33. Wall DS. Cybercrime: The Transformation of Crime in the Information Age. Polity Press, 2007.
34. Yeung K, Lodge M. Algorithmic Regulation. Oxford University Press, 2019.