

Deepfake Technology and Criminal Liability: Challenges for Contemporary Criminal Law

Author

Imam Purnomo Aji^{1*},
Hillan Syamsudhuha
Ahmad el Hariz²,
Musyafa Syamil Arroyan³

¹ Sekolah Tinggi Agama
Islam An-Nur

Banyumas, Indonesia

² Universitas Amikom
Purwokerto, Indonesia

³ University of
Edinburgh, United
Kingdom

Corresponding Author:

*Imam Purnomo Aji,

Email:

imamaji@annurbanyumas
.ac.id

Data:

Received: Feb 12, 2026;

Accepted: Jun 12, 2026;

Published: Jun 26, 2026.

Keywords:

*Deepfake Technology;
Criminal Liability;
Artificial Intelligence;
Cybercrime.*

Abstract: The rapid advancement of deepfake technology, driven by artificial intelligence and deep learning algorithms, has created unprecedented challenges for contemporary criminal law. Deepfakes enable the realistic manipulation of images, audio, and video, making it increasingly difficult to distinguish authentic digital content from fabricated material. While this technology offers legitimate applications in entertainment, education, and digital media, its misuse has facilitated a wide range of criminal activities, including fraud, identity theft, defamation, non-consensual intimate image creation, election manipulation, cyber extortion, and the dissemination of disinformation. These developments expose significant weaknesses in existing criminal law, which was primarily designed to address conventional forms of criminal conduct rather than AI-generated digital deception. This article examines the criminal liability arising from the misuse of deepfake technology through a normative juridical approach supported by comparative legal analysis. It analyzes the adequacy of existing criminal law doctrines concerning actus reus, mens rea, causation, accomplice liability, and corporate responsibility, while evaluating emerging regulatory frameworks in selected jurisdictions. The findings indicate that current legal frameworks remain fragmented and insufficient to address the complex distribution of responsibility among developers, platform providers, content creators, and end users. Accordingly, this study proposes a Risk-Based Deepfake Criminal Liability Framework integrating criminal responsibility, platform accountability, technological safeguards, victim protection, and judicial oversight to strengthen criminal law responses while preserving innovation, freedom of expression, and digital rights in the age of artificial intelligence.



©2026; This is an Open Access Research distributed under the term of the Creative Commons Attribution Licensee (<https://creativecommons.org/licenses/by-sa/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original works is properly cited.

INTRODUCTION

The rapid advancement of artificial intelligence (AI) has fundamentally transformed the digital ecosystem by enabling machines to perform increasingly sophisticated cognitive and creative tasks.¹ Among the most significant innovations is deepfake technology, which employs deep learning algorithms, particularly generative adversarial networks (GANs) and other advanced machine learning models, to produce highly realistic synthetic images, audio recordings, and videos. Unlike conventional digital editing techniques, deepfakes are capable of generating fabricated content that closely resembles authentic human appearances, voices, and behaviors, making it increasingly difficult for individuals, institutions, and law enforcement agencies to distinguish manipulated media from genuine digital evidence. As deepfake technology becomes more accessible through publicly available software and cloud-based AI services, its societal impact has expanded far beyond technological experimentation into the domains of politics, criminal justice, finance, cybersecurity, and public administration.

Although deepfake technology offers legitimate applications in filmmaking, digital entertainment, education, historical preservation, accessibility services, and virtual communication, its rapid proliferation has simultaneously created significant legal and ethical concerns. The same technological capabilities that facilitate innovation can also be exploited to commit various forms of criminal conduct. Deepfake-generated materials have increasingly been used to perpetrate identity theft, financial fraud, political disinformation, cyber extortion, non-consensual intimate image creation, reputational attacks, market manipulation, and social engineering schemes. Consequently, deepfakes have emerged not merely as a technological phenomenon but as a growing threat to individual rights, public trust, democratic institutions, and national security.²

The criminal implications of deepfake technology are particularly significant because digital manipulation fundamentally alters traditional evidentiary assumptions. Criminal justice systems have historically relied upon photographs, audio recordings, and video footage as reliable forms of documentary evidence capable of supporting investigations and judicial proceedings. However, advances in artificial intelligence now permit fabricated digital content to achieve levels of realism that frequently exceed ordinary human capacity for detection. This development undermines the evidentiary value of digital media while increasing the risk of wrongful accusations, fabricated evidence, witness intimidation, and obstruction of justice. Consequently, courts and law enforcement agencies must confront new challenges concerning the authenticity, admissibility, and forensic verification of digital evidence.³

These technological developments expose important limitations within contemporary criminal law. Traditional criminal law was primarily developed to regulate physical acts committed by identifiable offenders operating within clearly defined territorial jurisdictions. By contrast, crimes involving deepfake technology frequently involve decentralized digital platforms, anonymous users, transnational networks, automated content generation, and multiple actors contributing to the creation, dissemination, and commercialization of manipulated media. Such characteristics complicate the application of conventional criminal law doctrines concerning *actus reus*, *mens rea*, causation, participation, and criminal liability. As a result, existing legal frameworks often struggle to allocate responsibility effectively within

¹ Marina Aleksandrovna Efremova and Evgeniy Aleksandrovich Russkevich, "Deepfake and Criminal Law," *Bull. Kazan L. Inst. MIA Russ.* 15 (2024): 97.

² Deeksha Kumari, "Deepfake Technology and Legal Issues," *LawFoyer Int'l J. Doctrinal Legal Rsch.* 2 (2024): 234.

³ Yvonne Apolo and Katina Michael, "Beyond A Reasonable Doubt? Audiovisual Evidence, AI Manipulation, Deepfakes, and the Law," *IEEE Transactions on Technology and Society* 5, no. 2 (June 2024): 156–68, <https://doi.org/10.1109/TTS.2024.3427816>.

increasingly complex digital ecosystems.

One of the most pressing legal questions concerns the attribution of criminal liability. Deepfake-related offenses frequently involve multiple participants, including AI developers, software providers, online platforms, content creators, distributors, and end users. While the individual who intentionally creates or disseminates harmful deepfake content may bear direct criminal responsibility, legal uncertainty persists regarding the potential liability of developers who design AI systems, platform operators who facilitate distribution, or commercial entities benefiting from AI-generated content. The collaborative and technologically mediated nature of deepfake production therefore challenges the traditional assumption that criminal responsibility can easily be attributed to a single identifiable offender.⁴

These challenges have encouraged governments and international organizations to reconsider the adequacy of existing criminal law frameworks. Several jurisdictions, including the United States, the European Union, the United Kingdom, China, Singapore, and Australia, have introduced or proposed regulatory measures addressing synthetic media, platform accountability, election integrity, cybercrime, privacy protection, and artificial intelligence governance. International initiatives developed by organizations such as the Council of Europe, UNESCO, the Organisation for Economic Co-operation and Development (OECD), and the European Union likewise emphasize the need for trustworthy AI, transparency obligations, human oversight, and accountability mechanisms. These developments demonstrate an emerging international recognition that deepfake technology requires legal responses extending beyond traditional cybercrime regulation.⁵

Indonesia has likewise experienced rapid digital transformation accompanied by increasing public access to artificial intelligence technologies. The widespread use of social media platforms, digital communication networks, and AI-powered applications has accelerated the circulation of manipulated digital content across multiple sectors of society. Although Indonesia possesses legal instruments capable of addressing certain consequences of deepfake misuse—such as the Criminal Code (KUHP), the Electronic Information and Transactions Law, the Personal Data Protection Law, and sector-specific regulations—no comprehensive legal framework specifically governs criminal liability arising from AI-generated synthetic media.⁶ Consequently, law enforcement agencies frequently rely upon fragmented statutory provisions that were enacted before the emergence of sophisticated generative AI technologies, thereby creating significant uncertainty concerning criminal responsibility and legal enforcement.

The absence of a comprehensive regulatory framework also raises broader constitutional and human rights concerns. Effective legal regulation of deepfake technology must balance competing interests, including freedom of expression, technological innovation, privacy protection, reputation, cybersecurity, electoral integrity, and public security. Excessively restrictive criminal regulation may inhibit legitimate research, artistic expression, satire, journalism, and educational applications of synthetic media.⁷ Conversely, insufficient regulation may permit widespread misuse capable of causing severe personal, economic, political, and societal harm. Accordingly, contemporary criminal law must develop balanced

⁴ . Mohamed Hassan Mekki, "The Challenges of Digital Evidence Usage in Deepfake Crimes Era," *Journal of Law and Emerging Technologies* 3, no. 2 (November 23, 2023): 176–232, <https://doi.org/10.54873/jolets.v3i2.123>.

⁵ Jandrie Sembiring and Sunny Ummul Firdaus, "Criminal Liability for Misuse of Artificial Intelligence (Ai) in Deepfake Crimes," *International Journal of Multi Science* 5, no. 01 (2025): 1–9.

⁶ Aleksandra Nowak, Bálint Tóth, and Andrei Ionescu, "Legal Challenges of Deepfakes: Liability, Harm, and Regulatory Responses," *Legal Studies in Digital Age* 2, no. 2 SE-Articles (n.d.): 49–60, <https://jlsda.com/index.php/lsda/article/view/306>.

⁷ David Schultz, "Personhood, Crimes, and Criminal Liability in the Age of Artificial Intelligence," *Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law* 18, no. Suppl (2025): 301–8.

regulatory mechanisms capable of protecting fundamental rights while preserving opportunities for responsible technological innovation.

Despite the growing body of scholarship concerning artificial intelligence, cybercrime, and digital governance, important research gaps remain. Existing studies frequently focus on individual legal issues such as misinformation, privacy violations, election interference, or cybersecurity without comprehensively examining the broader implications of deepfake technology for criminal liability. Moreover, much of the current literature concentrates on ethical governance or technological detection mechanisms while paying comparatively limited attention to the doctrinal foundations of criminal responsibility, institutional accountability, and comparative criminal law.⁸ Consequently, there remains a need for an integrated legal analysis capable of reconciling established principles of criminal law with the unique characteristics of AI-generated digital deception.⁹

This study addresses these gaps by examining the legal implications of deepfake technology for contemporary criminal liability through a normative juridical approach supported by comparative legal analysis. It evaluates the adequacy of existing criminal law doctrines—including actus reus, mens rea, causation, accomplice liability, and corporate criminal responsibility—in addressing offenses involving AI-generated synthetic media. Building upon this analysis, the study proposes a Risk-Based Deepfake Criminal Liability Framework that integrates criminal responsibility, platform accountability, technological safeguards, victim protection, regulatory oversight, and judicial review into a coherent governance model. The proposed framework argues that effective criminal law in the era of artificial intelligence should not merely punish offenders after harm occurs but should also establish preventive legal mechanisms that promote responsible AI development, strengthen digital trust, protect fundamental rights, and preserve the integrity of democratic society.

RESEARCH METHODS

This study employs a normative juridical research design using doctrinal and comparative legal approaches to examine the criminal liability arising from the misuse of deepfake technology in the context of contemporary criminal law.¹⁰ A normative legal methodology is appropriate because the research focuses on analyzing legal norms, criminal law doctrines, statutory regulations, judicial interpretations, and emerging regulatory frameworks governing artificial intelligence and synthetic media. The doctrinal approach is utilized to examine the applicability of fundamental principles of criminal law, including actus reus, mens rea, causation, criminal participation, accomplice liability, corporate criminal responsibility, and the principle of legality in addressing offenses involving deepfake technology. In addition, the comparative legal approach evaluates how selected jurisdictions have responded to deepfake-related crimes through legislative reform, judicial practice, and AI governance policies. Primary legal materials consist of international legal instruments, national legislation, judicial decisions, and regulatory documents relating to criminal law, cybercrime, artificial intelligence, digital evidence, privacy protection, and platform governance. These include, among others, the Budapest Convention on Cybercrime, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, the European Union Artificial Intelligence Act, Indonesia's Criminal Code (KUHP), the

⁸ Shambhu Prasad Chakrabarty and Shrabana Chattopadhyay, "Criminal Liability of Artificial Intelligence-Generated Deepfakes in India," 2025, 233–50, https://doi.org/10.1007/978-981-97-8457-8_16.

⁹ Leo S.F. Lin, "Examining the Role of Deepfake Technology in Organized Fraud: Legal, Security, and Governance Challenges," *Frontiers in Law* 4 (April 16, 2025): 6–17, <https://doi.org/10.6000/2817-2302.2025.04.02>.

¹⁰ John Creswell and J David Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Sage publications, 2017).

Electronic Information and Transactions Law, the Personal Data Protection Law, and other relevant statutory and regulatory instruments. Secondary legal materials comprise scholarly books, peer-reviewed journal articles, official reports, policy papers, and academic commentaries discussing artificial intelligence, cybercrime, criminal liability, digital forensics, and technology regulation.

The collected legal materials were analyzed qualitatively through doctrinal legal interpretation supported by functional comparative analysis. The doctrinal analysis evaluates whether existing criminal law principles remain adequate for addressing emerging forms of AI-enabled criminal conduct, particularly regarding criminal intent, evidentiary standards, attribution of responsibility, and liability among multiple actors involved in the creation, dissemination, and commercialization of deepfake content. Subsequently, the comparative analysis identifies similarities, differences, regulatory innovations, and best practices across selected jurisdictions concerning platform accountability, criminal sanctions, technological safeguards, victim protection, and judicial oversight. The findings are interpreted using the theoretical perspectives of criminal law, digital governance, and responsible artificial intelligence to assess the capacity of current legal frameworks to balance technological innovation, freedom of expression, public security, and the protection of fundamental rights. Based on this analysis, the study develops a Risk-Based Deepfake Criminal Liability Framework that integrates criminal responsibility, preventive regulation, platform accountability, technological due diligence, victim-oriented remedies, and judicial oversight into a comprehensive model for governing deepfake-related offenses. This framework is intended to provide normative guidance for future criminal law reform while ensuring that legal responses remain effective, proportionate, and adaptable to the evolving challenges of artificial intelligence in the digital era.

ANALYSIS AND DISCUSSION

Legal Foundations of Deepfake Technology and Criminal Liability in Contemporary Criminal Law

The rapid evolution of artificial intelligence has fundamentally transformed the digital environment by enabling machines to generate highly realistic synthetic content that closely resembles authentic human communication.¹¹ Among the most influential developments is deepfake technology, which utilizes advanced deep learning algorithms to manipulate or generate images, audio, and videos that are often indistinguishable from genuine digital media. Unlike traditional editing software that requires extensive manual intervention, deepfake systems automate the creation of synthetic content through sophisticated computational models capable of reproducing facial expressions, vocal characteristics, gestures, and contextual interactions with remarkable accuracy. Consequently, deepfake technology has emerged as one of the most disruptive innovations in the field of digital communication, presenting both significant opportunities and profound legal challenges.

The technological foundation of deepfake systems lies in the rapid advancement of artificial intelligence and deep learning, particularly neural network architectures capable of learning complex statistical relationships from massive datasets. One of the earliest breakthroughs was the development of Generative Adversarial Networks (GANs), which consist of two competing neural networks—a generator and a discriminator—that continuously improve the realism of synthetic outputs through adversarial training. More recently, the emergence of foundation models and generative artificial intelligence has

¹¹ Asri Gresmelian Eurike Hailtik and Wiwik Afifah, "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia," *Asian Journal of Social and Humanities* 2, no. 4 (January 22, 2024): 776–95, <https://doi.org/10.59888/ajosh.v2i4.222>.

significantly enhanced the capability of deepfake systems by integrating multimodal learning, enabling the simultaneous generation of text, speech, images, and video within unified computational architectures. These technological developments have expanded the accessibility and sophistication of synthetic media while reducing the technical expertise previously required to produce manipulated digital content.

The growing availability of deepfake applications has accelerated the proliferation of synthetic media across numerous sectors, including entertainment, education, healthcare, journalism, marketing, and public administration. In legitimate contexts, synthetic media can support film production, historical reconstruction, language translation, accessibility for persons with disabilities, and immersive virtual communication. Nevertheless, the same technological capabilities can be exploited to produce deceptive digital content capable of misleading individuals, damaging reputations, manipulating public opinion, and facilitating criminal conduct. This dual-use characteristic distinguishes deepfake technology from many previous digital innovations because its beneficial applications coexist alongside substantial risks to public security, democratic governance, and individual rights.¹²

The criminal implications of deepfake technology are increasingly evident in the emergence of diverse forms of AI-enabled digital crime. One of the most common offenses involves identity theft, whereby synthetic audio or visual content is used to impersonate individuals for fraudulent or malicious purposes. Deepfake-generated impersonations may deceive financial institutions, employers, government agencies, or private individuals into disclosing confidential information or authorizing unauthorized transactions. The capacity to replicate facial features and vocal characteristics with extraordinary precision substantially increases the effectiveness of social engineering attacks while complicating traditional methods of identity verification.

Deepfake technology has likewise become an important instrument in fraud and financial crimes. Criminal actors increasingly employ AI-generated videos and voice recordings to impersonate corporate executives, government officials, or business partners in order to authorize fraudulent financial transfers or obtain sensitive commercial information. In addition, deepfake content has been utilized to facilitate investment scams, securities manipulation, and cryptocurrency fraud through fabricated endorsements or false corporate announcements. The economic consequences of such activities extend beyond individual financial losses by undermining confidence in digital transactions and weakening institutional trust within increasingly interconnected digital economies.¹³

Beyond financial offenses, deepfake technology poses serious threats to personal dignity and social stability through defamation, non-consensual intimate image creation, cyber extortion, election manipulation, and disinformation campaigns. AI-generated synthetic media may be used to fabricate compromising videos, spread false political statements, manipulate electoral discourse, or coerce victims through threats involving fabricated intimate content. Such activities frequently produce severe psychological, reputational, and economic harm while simultaneously disrupting democratic processes and eroding public confidence in authentic information. These developments illustrate that deepfake-related offenses often transcend traditional criminal categories by combining elements of cybercrime, privacy violations, fraud, and psychological abuse within a single technological mechanism.

¹² Songyang Sai and Zifan Wang, "Criminal Regulatory Approaches to Deepfake-Related Offenses: Focusing on the Crime of Fraud," *International Journal of Asian Social Science Research* 3, no. 1 (January 6, 2026): 20–31, <https://doi.org/10.70267/ijassr.260301.2031>.

¹³ K.M. Beaver, "International and Domestic Legal Frameworks on Online Fraud and Deepfake Technologies: A Comparative Criminal Law Analysis," *Bulletin of the L.N. Gumilyov Eurasian National University. Law Series* 152, no. 3 (2025): 212–28, <https://doi.org/10.32523/2616-6844-2025-152-3-212-228>.

Addressing these emerging forms of criminality requires careful examination of the fundamental doctrines of criminal liability.¹⁴ Contemporary criminal law traditionally establishes liability through the interaction of *actus reus* (the prohibited conduct) and *mens rea* (the requisite mental element). In the context of deepfake technology, identifying the prohibited act may involve the creation, modification, dissemination, commercialization, or intentional use of synthetic media for unlawful purposes. However, determining criminal intent becomes substantially more complex because multiple individuals—including developers, platform operators, commercial users, and distributors—may contribute to the production and circulation of harmful deepfake content. Consequently, conventional criminal law doctrines must adapt to increasingly decentralized forms of technologically mediated criminal conduct.

The doctrines of causation, attempt, criminal participation, and corporate criminal liability become equally important in regulating deepfake-related offenses. Criminal liability cannot always be attributed solely to the individual directly generating manipulated content because harmful outcomes frequently arise through collaborative digital ecosystems involving software developers, cloud service providers, online platforms, and commercial intermediaries. Determining legal causation therefore requires evaluating whether each participant materially contributed to the commission of the offense or possessed sufficient knowledge regarding the unlawful use of AI technologies. Likewise, corporations providing AI services may bear responsibility where organizational negligence, inadequate compliance measures, or reckless commercialization facilitate criminal misuse of deepfake technologies.

Recognizing these challenges, the international community has begun developing regulatory frameworks addressing artificial intelligence, cybercrime, and digital governance. The Budapest Convention on Cybercrime remains the principal international instrument governing cyber-enabled criminal activities, establishing mechanisms for criminalization, digital evidence collection, and international cooperation. Although the Convention predates the emergence of generative AI, many of its provisions concerning computer-related fraud, illegal access, data interference, and digital investigations remain relevant to offenses involving synthetic media. Nevertheless, the Convention does not specifically regulate deepfake technology, illustrating the broader challenge of applying traditional cybercrime frameworks to rapidly evolving AI-generated content.

More recent international initiatives have sought to address these regulatory gaps. The Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law emphasizes the need to ensure that AI systems operate consistently with fundamental rights, democratic values, and legal accountability. Similarly, the European Union Artificial Intelligence Act introduces a risk-based regulatory model requiring enhanced obligations for high-risk AI systems, including transparency, documentation, risk management, and human oversight. Complementing these developments, the UNESCO Recommendation on the Ethics of Artificial Intelligence and the OECD AI Principles advocate responsible AI governance based on transparency, accountability, fairness, human-centered design, and the protection of fundamental rights. Collectively, these instruments establish important normative foundations for addressing the criminal implications of deepfake technology while promoting trustworthy artificial intelligence.

Indonesia has also initiated legal and policy responses relevant to deepfake-related offenses, although no comprehensive regulatory framework currently exists. Existing legal protection is primarily derived from the Indonesian Criminal Code (KUHP), the Electronic Information and Transactions Law, the Personal Data Protection Law, and the Criminal Procedure Code, each addressing particular aspects of unlawful digital conduct. These

¹⁴ Lauren LePage, “Criminal Defenses in the Age of AI: An Examination of How Technological Advancements Are Challenging Traditional Duress and Mistake of Fact Defenses,” 2025.

instruments provide legal mechanisms for prosecuting offenses involving fraud, defamation, unlawful dissemination of electronic information, privacy violations, and unauthorized access to digital systems. Furthermore, Indonesia's National Artificial Intelligence Strategy demonstrates governmental commitment to fostering responsible AI innovation while encouraging technological development across multiple sectors. However, these regulatory instruments remain fragmented and were largely developed before the widespread emergence of sophisticated deepfake technologies, leaving important issues relating to AI-generated synthetic media, platform accountability, developer responsibility, and digital forensic verification insufficiently addressed.

The foregoing analysis demonstrates that deepfake technology has fundamentally transformed the nature of digital crime by enabling highly realistic forms of deception that challenge conventional assumptions regarding evidence, identity, criminal conduct, and legal responsibility. While technological innovation has rapidly expanded the capabilities of artificial intelligence, contemporary criminal law continues to rely predominantly on doctrines developed for conventional offenses involving identifiable human actors and tangible forms of misconduct. As a result, significant normative gaps remain concerning the attribution of criminal liability within increasingly complex AI ecosystems involving multiple participants and automated content generation. These findings underscore the urgent need to rethink contemporary criminal law by developing integrated legal frameworks capable of balancing technological innovation, public security, individual rights, and democratic governance while ensuring that criminal liability remains effective, proportionate, and adaptable to the evolving realities of artificial intelligence.

Comparative Analysis of Criminal Liability for Deepfake-Related Offences

The rapid proliferation of deepfake technology has significantly complicated the application of traditional criminal law because AI-generated synthetic media frequently involve multiple actors, sophisticated technological processes, and transnational digital platforms.¹⁵ Conventional criminal law was primarily designed to identify and punish individual offenders who directly commit unlawful acts. In contrast, deepfake-related offences often emerge from complex technological ecosystems in which developers, AI service providers, online platforms, commercial users, and end users collectively contribute to the creation, dissemination, and monetization of harmful content. Consequently, comparative legal analysis demonstrates that many jurisdictions are gradually shifting from an offender-centered model of criminal liability toward more integrated governance frameworks capable of addressing the distributed nature of AI-enabled criminal conduct.

The first point of comparison concerns the attribution of criminal liability, which determines who should bear legal responsibility for deepfake-related offences. In Indonesia, criminal liability remains predominantly grounded in a conventional offender-oriented approach. The Indonesian Criminal Code generally attributes criminal responsibility to the individual who directly performs the prohibited conduct and possesses the requisite criminal intent. Accordingly, prosecution tends to focus on the creator or distributor of unlawful digital content. While this approach provides legal certainty in conventional criminal cases, it becomes increasingly difficult to apply where deepfake technologies involve multiple actors operating across different jurisdictions and technological infrastructures.¹⁶

International legal developments increasingly recognize the necessity of a multi-actor

¹⁵ Sara Rezaei and Mohammad Amini, "Criminal Liability in Deepfake-Related Image Identity Forgery," 2024.

¹⁶ Zhiwen Hao, "Criminal Law Regulation of AI Face-Swapping Crimes: Responsible Subjects, Theoretical Integration and Comprehensive Governance Framework," in *2025 4th International Conference on Public Management, Digital Economy and Internet Technology (ICPDI 2025)* (Atlantis Press, 2025), 149–70.

liability model. Rather than limiting criminal responsibility exclusively to the individual producing deepfake content, emerging regulatory approaches evaluate the respective contributions of AI developers, technology providers, digital platforms, commercial intermediaries, and users. Liability is allocated according to each actor's degree of control, knowledge, negligence, and participation in facilitating harmful outcomes. This broader approach reflects the reality that deepfake-related offences frequently result from interconnected technological ecosystems rather than isolated individual actions. Consequently, responsibility is increasingly viewed as a distributed legal obligation shared among multiple participants within the AI value chain.¹⁷

The second area of comparison concerns criminal intent (*mens rea*). Indonesian criminal law traditionally requires proof that an offender acted intentionally or, in certain circumstances, negligently. *Mens rea* is evaluated through conventional principles emphasizing subjective knowledge and volition at the time the offence was committed. However, deepfake technology complicates this assessment because AI-generated content may be created, modified, or disseminated through partially automated processes involving multiple participants with varying degrees of awareness regarding the unlawful consequences of their actions. Existing criminal law provides limited guidance concerning how intent should be assessed where AI systems significantly influence the commission of criminal acts.

By contrast, international regulatory discussions increasingly adopt an AI-assisted intent assessment capable of evaluating different levels of human involvement throughout the AI life cycle. Rather than focusing solely on the final user, this approach considers whether developers knowingly designed systems without adequate safeguards, whether platforms ignored foreseeable risks, or whether commercial users recklessly employed AI-generated content despite recognizing its unlawful potential.¹⁸ Accordingly, criminal intent may be evaluated through broader concepts of knowledge, recklessness, willful blindness, or gross negligence, depending upon the particular factual circumstances. This functional interpretation enables criminal law to respond more effectively to technologically mediated forms of criminal conduct.

The third point of comparison concerns platform responsibility, which has become increasingly significant given the central role of digital intermediaries in distributing synthetic media. Indonesian legislation contains only limited provisions specifically governing the obligations of online platforms concerning deepfake content. Existing regulations primarily address unlawful electronic information through general intermediary obligations without establishing comprehensive standards for AI-generated synthetic media. Consequently, platform operators possess relatively broad discretion regarding content moderation, detection technologies, and removal procedures, while legal accountability remains comparatively limited.¹⁹

International practice demonstrates a considerably stronger model of intermediary accountability based upon preventive governance and due diligence obligations. Regulatory initiatives increasingly require online platforms to implement effective content moderation systems, risk assessments, transparency reporting, user complaint mechanisms, and AI-

¹⁷ Andre Arya Pratama, Fikri Rosyad Fathurrahman, and Rani Lestari, "Criminal Liability Model for Deepfake AI Developers: European Union Inspiration for Indonesia's Legal Framework," *Ius Poenale* 6, no. 1 SE-Articles (January 15, 2026): 67–76, <https://doi.org/10.25041/ip.v6i1.4612>.

¹⁸ Rofi Aulia Rahman and Rizaldy Anggriawan, "Deepfake and Electoral Crimes: Criminal Law Perspectives from Indonesia, India, Pakistan, and the US," *Indonesian Comparative Law Review (ICLR)* 7, no. 2 (2025): 132–46.

¹⁹ Ikama Dewi Setia Triana, Aniek Periani, and Arka Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China," *Kosmik Hukum* 26, no. 2 (May 7, 2026): 465–81, <https://doi.org/10.30595/kosmikhukum.v26i2.25751>.

assisted detection technologies capable of identifying manipulated media. Rather than imposing automatic criminal liability upon platforms, these frameworks emphasize proactive compliance measures designed to reduce foreseeable harm while preserving freedom of expression and technological innovation. This preventive approach reflects the growing recognition that digital intermediaries occupy a strategic position in limiting the societal impact of harmful deepfake content.

A fourth area of comparison concerns developer liability, which remains one of the least developed aspects of criminal regulation. Indonesian law does not expressly regulate the potential criminal responsibility of AI developers whose technologies are subsequently misused for unlawful purposes. Consequently, developers generally avoid direct criminal liability unless they intentionally participate in criminal conduct or otherwise satisfy existing requirements concerning accomplice liability. The absence of explicit statutory obligations regarding safety-by-design, risk mitigation, or AI governance creates significant uncertainty concerning the legal responsibilities of technology developers operating within rapidly evolving AI ecosystems.²⁰

International legal developments increasingly explore developer due diligence as a mechanism for strengthening accountability without discouraging innovation. Emerging regulatory approaches encourage developers to incorporate safety measures, risk assessments, documentation requirements, transparency obligations, and misuse prevention mechanisms throughout the design and deployment of AI systems. Although criminal liability generally remains limited to situations involving intentional misconduct or gross negligence, these evolving standards recognize that responsible AI development requires proactive legal obligations extending beyond traditional software engineering practices. Such developments illustrate a gradual shift from reactive criminal enforcement toward preventive technological governance.

The fifth comparative issue concerns digital evidence and forensic challenges, which represent one of the most significant procedural consequences of deepfake technology. Indonesian criminal procedure continues to rely upon conventional evidentiary principles while gradually incorporating digital evidence into judicial proceedings. Nevertheless, AI-generated synthetic media present unprecedented challenges regarding authenticity, admissibility, reliability, and evidentiary weight. Establishing whether photographs, audio recordings, or videos have been manipulated frequently requires sophisticated forensic analysis unavailable in many investigative settings. Furthermore, maintaining an unbroken chain of custody for digital evidence becomes increasingly difficult where manipulated files can be replicated, modified, or disseminated instantaneously across digital networks.

International best practices have responded by strengthening digital forensic verification through advanced authentication technologies, expert examination, metadata analysis, blockchain-supported verification mechanisms, and standardized forensic methodologies. Courts increasingly require technical expert testimony to evaluate the authenticity of AI-generated evidence before determining its admissibility or evidentiary value. These procedural safeguards reinforce legal certainty while reducing the risk of wrongful convictions or fabricated evidence influencing criminal proceedings. The integration of AI-assisted forensic tools further illustrates the necessity of adapting procedural law alongside substantive criminal law to address the unique characteristics of synthetic media.

The final area of comparison concerns victim protection, which extends beyond criminal punishment toward safeguarding individual rights and providing effective remedies.

²⁰ Ruben Nicholas Alfredo Tobing and Yuliana Yuli, "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media," *Eduvest - Journal of Universal Studies* 6, no. 2 (February 6, 2026): 1302–14, <https://doi.org/10.59188/eduvest.v6i2.52738>.

Indonesian law offers partial protection through criminal sanctions, civil remedies, privacy regulations, and electronic information legislation; however, comprehensive mechanisms specifically addressing victims of deepfake-related offences remain limited. International approaches increasingly adopt a more holistic model incorporating privacy protection, reputation restoration, rapid content removal, compensation mechanisms, psychological assistance, and restorative justice. Collectively, the comparative analysis indicates that many jurisdictions are gradually embracing a risk-based and multi-layered model of criminal liability in which responsibility is distributed among offenders, developers, platforms, and other relevant actors while integrating preventive regulation, technological safeguards, victim-centered remedies, and institutional accountability. By contrast, Indonesia continues to rely predominantly on a traditional offender-centered criminal law framework characterized by fragmented AI governance, limited intermediary obligations, developing forensic capabilities, and partial victim protection.²¹ These findings underscore the need for future criminal law reform capable of integrating conventional criminal liability doctrines with emerging principles of responsible artificial intelligence governance in order to address the evolving challenges posed by deepfake technology.

Developing a Risk-Based Deepfake Criminal Liability Framework for Contemporary Criminal Law

The comparative analysis presented in the previous sections demonstrates that contemporary criminal law is increasingly confronted with legal challenges that cannot be adequately addressed through conventional offender-centered doctrines alone.²² Deepfake technology has transformed the structure of criminal conduct by introducing artificial intelligence into the production, dissemination, and commercialization of deceptive digital content. Criminal liability is therefore no longer confined to the actions of a single perpetrator but often involves a complex network of actors, technological infrastructures, and digital intermediaries. To respond to these developments, this study proposes a Risk-Based Deepfake Criminal Liability Framework as its principal theoretical contribution. The framework integrates traditional principles of criminal law with contemporary AI governance to establish a comprehensive normative model capable of balancing technological innovation, public security, legal certainty, and the protection of fundamental rights.

The proposed framework is founded upon the premise that criminal law should move beyond a purely reactive model based solely on punishment after harm has occurred.²³ Instead, criminal liability should incorporate preventive governance capable of identifying legal risks throughout the life cycle of deepfake technology. Such an approach recognizes that artificial intelligence systems may create foreseeable risks long before criminal conduct materializes. Consequently, effective regulation requires the integration of criminal law doctrines, technological safeguards, institutional accountability, and procedural protections within a unified governance structure. The proposed model is illustrated as follows:

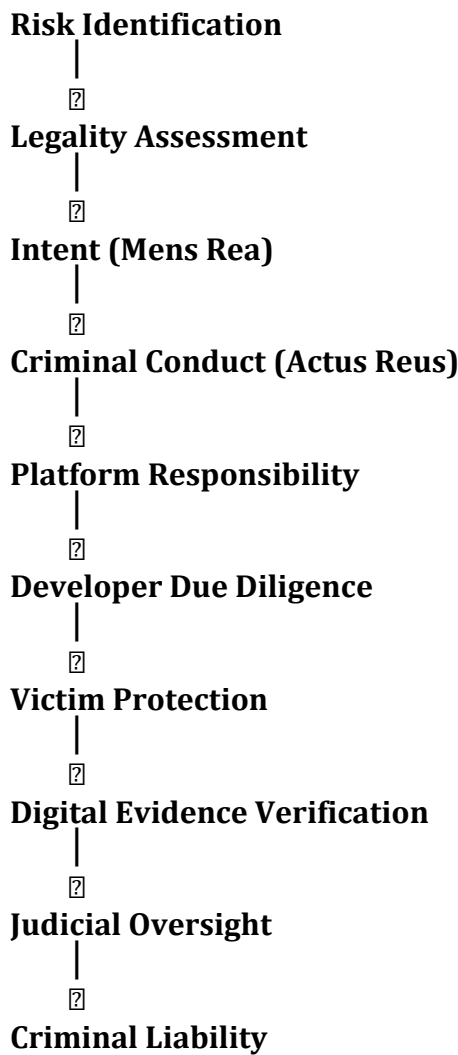
Deepfake Creation

2

²¹ Luca Ettore Perriello, "Blurred Realities: Legal Strategies for the Deepfake Era," *Maastricht Journal of European and Comparative Law*, March 27, 2026, <https://doi.org/10.1177/1023263X261433380>.

²² Asri Pakerti, Fero Sanjaya, and Herlita Eryke, "CRIMINAL LIABILITY IN ARTIFICIAL INTELLIGENCE-BASED CRIMES: AN ANALYSIS OF THE NORMS IN INDONESIAN CRIMINAL LAW," *Syiah Kuala Law Journal* 10, no. 1 (2026).

²³ Maria Fernanda Santos Sugahara, "Non-Consensual Dissemination of Pornographic Deepfakes," 2026.



The first component of the framework is risk identification, which serves as the preventive foundation of criminal law in the era of artificial intelligence. Not every application of deepfake technology poses the same level of legal risk. Accordingly, AI systems should be classified according to the severity of the potential harm they may generate. High-risk applications—including synthetic political disinformation, biometric identity manipulation, financial fraud, non-consensual intimate image creation, and deepfake-assisted cyber extortion—require enhanced regulatory scrutiny before deployment. Preventive legal assessment enables legislators and regulatory authorities to identify emerging criminal risks while reducing the likelihood of serious societal harm before criminal offenses occur.

Following risk identification, the framework emphasizes the principle of legality as the constitutional basis for criminal responsibility. The legality principle requires that criminal liability be imposed only where prohibited conduct has been clearly defined through statutory law.²⁴ Because deepfake technology continuously evolves through technological innovation, legal certainty becomes essential to prevent arbitrary criminal prosecution while ensuring effective enforcement. Legislative reform should therefore establish explicit statutory provisions defining prohibited forms of AI-generated deception, the scope of criminal liability, and the respective responsibilities of developers, platforms, commercial users, and individual offenders. Such legal clarity strengthens both the rule of law and public confidence in emerging

²⁴ Raphael Ramos Monteiro de Souza, “Legal Remedies and Regulatory Frameworks to Combat Ai-Driven Deepfakes,” in *Mitigating the Risks of AI Deepfakes* (CRC Press, 2026), 94–116.

AI regulation.

The third component concerns criminal intent (*mens rea*), which remains a fundamental prerequisite for criminal responsibility.²⁵ The proposed framework recognizes that deepfake-related offenses may involve varying degrees of culpability, including intentional misuse, recklessness, and, where expressly provided by law, criminal negligence. Intentional creation or dissemination of synthetic media for purposes such as fraud, extortion, election interference, or identity theft should attract the highest degree of criminal liability. At the same time, reckless deployment of AI systems without reasonable safeguards may also justify criminal sanctions where foreseeable harm could have been prevented. This graduated approach enables criminal law to distinguish between legitimate technological innovation and culpable misuse of artificial intelligence.

Closely related is the fourth component concerning criminal conduct (*actus reus*). Traditional criminal law generally associates prohibited conduct with direct physical actions performed by individual offenders. However, deepfake-related offenses require a broader conception of criminal conduct encompassing the creation, distribution, commercial exploitation, facilitation, and intentional dissemination of AI-generated synthetic media. Criminal liability should therefore extend beyond the individual who produces manipulated content to include those who knowingly facilitate its unlawful circulation or derive commercial benefit from criminal exploitation. This broader understanding reflects the collaborative and technologically mediated nature of contemporary digital crime.

The fifth component introduces platform responsibility, recognizing the increasingly influential role of online intermediaries in the dissemination of deepfake content. Digital platforms possess significant technical capacity to detect, limit, and remove manipulated media before substantial harm occurs. Accordingly, the proposed framework recommends mandatory content moderation systems, notice-and-action procedures, transparency reporting, and AI-assisted detection mechanisms capable of identifying synthetic media. Platform responsibility should not impose absolute liability for all user-generated content but should instead require reasonable due diligence proportional to the platform's technological capabilities and degree of operational control. Such obligations encourage preventive governance while preserving innovation and freedom of expression.

Complementing platform responsibility is the sixth component concerning developer due diligence. AI developers occupy a strategic position because they determine the technical architecture, safety features, and operational safeguards embedded within generative AI systems. Consequently, developers should implement safety-by-design principles throughout the software development process, incorporating misuse prevention mechanisms, watermarking technologies, authentication tools, and continuous risk monitoring. Compliance obligations should further require periodic risk assessments, documentation, auditing, and regulatory reporting for high-risk AI applications. By integrating preventive safeguards during technological development, criminal law can reduce foreseeable risks without unnecessarily restricting legitimate scientific research and technological innovation.

The seventh component emphasizes victim protection, which constitutes an essential objective of modern criminal justice. Victims of deepfake-related offenses frequently experience significant psychological trauma, reputational damage, financial loss, privacy violations, and long-term social consequences extending far beyond the commission of the offense itself. Accordingly, criminal law should provide comprehensive remedies including rapid removal of unlawful content, financial compensation, psychological assistance, restoration of privacy rights, and access to restorative justice mechanisms where appropriate.

²⁵ Tayeb Belouadah, "The Criminal Law Challenges in Confronting AI Crimes," *المجلة الجزائرية للحقوق والعلوم السياسية* 10, no. 1 (2025): 1157–72.

Strengthening victim-oriented legal protection enhances public trust while reinforcing the human rights dimension of contemporary criminal law.

The eighth component concerns digital evidence verification, reflecting the increasing importance of forensic reliability within criminal proceedings involving artificial intelligence. Because deepfake technology directly undermines the credibility of digital evidence, courts require advanced verification procedures capable of distinguishing authentic media from AI-generated fabrications. The proposed framework therefore recommends the adoption of AI-assisted forensic tools, standardized authentication protocols, metadata analysis, blockchain-supported verification mechanisms, and independent expert examination. These procedural safeguards strengthen evidentiary integrity while reducing the risks of fabricated evidence, wrongful conviction, and judicial error within increasingly digital criminal justice systems.

The ninth component is judicial oversight, which ensures that criminal liability remains subject to constitutional safeguards and procedural fairness. Independent judicial review is necessary to evaluate the legality of investigations, the admissibility of AI-generated evidence, the proportionality of criminal sanctions, and the protection of due process rights. Courts should also possess authority to review compliance with platform obligations, developer responsibilities, and investigative procedures involving artificial intelligence technologies. Judicial oversight therefore functions as an institutional safeguard preventing arbitrary enforcement while maintaining the legitimacy of criminal justice in technologically complex cases.

The principal novelty of this study lies in the development of the Risk-Based Deepfake Criminal Liability Framework, which integrates traditional criminal law doctrines with contemporary principles of artificial intelligence governance into a unified normative model. Unlike previous scholarship that primarily examines isolated issues such as misinformation, cybercrime, platform liability, digital evidence, or AI ethics independently, the proposed framework systematically combines risk identification, legality, criminal intent, criminal conduct, platform responsibility, developer due diligence, victim protection, digital evidence verification, and judicial oversight within a comprehensive architecture of criminal liability. This integrated approach reflects the multidimensional nature of deepfake-related offenses while recognizing that effective criminal regulation must extend beyond punishment to encompass prevention, accountability, institutional coordination, and technological governance.²⁶

The proposed framework provides a normative roadmap for the future development of criminal law in response to rapidly evolving artificial intelligence technologies. By integrating preventive regulation with established doctrines of criminal responsibility, the framework seeks to preserve legal certainty while accommodating technological innovation and protecting fundamental rights. Its human-centered and risk-based orientation ensures that criminal law remains capable of responding proportionately to AI-generated synthetic media without undermining legitimate scientific research, freedom of expression, or digital innovation. Accordingly, the Risk-Based Deepfake Criminal Liability Framework offers a comprehensive theoretical foundation for reforming contemporary criminal law and contributes to the broader fields of AI regulation, cybercrime law, digital governance, and criminal justice in the era of artificial intelligence.

²⁶ Hao, "Criminal Law Regulation of AI Face-Swapping Crimes: Responsible Subjects, Theoretical Integration and Comprehensive Governance Framework."

CONCLUSION

This study demonstrates that the rapid advancement of deepfake technology has fundamentally transformed the landscape of digital crime and exposed significant limitations within contemporary criminal law. Powered by artificial intelligence and deep learning, deepfake technology enables the creation of highly realistic synthetic media that can be exploited for identity theft, financial fraud, cyber extortion, defamation, election manipulation, non-consensual intimate image creation, and large-scale disinformation campaigns. The comparative analysis reveals that existing criminal law frameworks, including those in Indonesia, continue to rely predominantly on conventional offender-centered doctrines emphasizing individual criminal responsibility through the traditional concepts of *actus reus* and *mens rea*. While these principles remain essential to criminal justice, they are insufficient to address the increasingly complex distribution of responsibility among AI developers, platform providers, commercial users, and digital intermediaries involved in the creation and dissemination of deepfake content. By contrast, international regulatory developments increasingly adopt a risk-based and multi-actor governance approach that integrates preventive regulation, intermediary accountability, developer due diligence, digital evidence verification, and enhanced victim protection. These findings indicate that technological innovation has evolved more rapidly than criminal law, thereby creating substantial normative and institutional gaps in responding to AI-generated criminal conduct.

Building upon these findings, this study proposes the Risk-Based Deepfake Criminal Liability Framework as its principal theoretical contribution to the development of contemporary criminal law. The framework integrates nine interrelated components—risk identification, legality assessment, criminal intent (*mens rea*), criminal conduct (*actus reus*), platform responsibility, developer due diligence, victim protection, digital evidence verification, and judicial oversight—into a coherent normative model capable of addressing the unique legal challenges posed by deepfake technology. Rather than relying solely on punitive mechanisms after criminal harm has occurred, the proposed framework emphasizes preventive governance, technological accountability, procedural fairness, and the protection of fundamental rights throughout the life cycle of AI-generated synthetic media. Accordingly, future criminal law reform should establish clear statutory rules governing deepfake-related offences, strengthen institutional responsibilities for digital platforms and AI developers, improve forensic capacities for authenticating digital evidence, and ensure accessible legal remedies for victims. By harmonizing traditional criminal law doctrines with emerging principles of artificial intelligence governance, the proposed framework provides a comprehensive roadmap for developing a modern, adaptive, and human-centered criminal justice system capable of responding effectively to the challenges of the digital era while preserving technological innovation, legal certainty, democratic values, and the rule of law.

REFERENCES

- Alfredo Tobing, Ruben Nicholas, and Yuliana Yuli. "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media." *Eduvest - Journal of Universal Studies* 6, no. 2 (February 6, 2026): 1302–14. <https://doi.org/10.59188/eduvest.v6i2.52738>.
- Apolo, Yvonne, and Katina Michael. "Beyond A Reasonable Doubt? Audiovisual Evidence, AI Manipulation, Deepfakes, and the Law." *IEEE Transactions on Technology and Society* 5, no. 2 (June 2024): 156–68. <https://doi.org/10.1109/TTS.2024.3427816>.
- Beaver, K.M. "International and Domestic Legal Frameworks on Online Fraud and Deepfake Technologies: A Comparative Criminal Law Analysis." *Bulletin of the L.N. Gumilyov Eurasian National University. Law Series* 152, no. 3 (2025): 212–28.

- <https://doi.org/10.32523/2616-6844-2025-152-3-212-228>.
- Belouadah, Tayeb. "The Criminal Law Challenges in Confronting AI Crimes." *المجلة الجزائرية للحقوق والعلوم السياسية* 10, no. 1 (2025): 1157–72.
- Chakrabarty, Shambhu Prasad, and Shrabana Chattopadhyay. "Criminal Liability of Artificial Intelligence-Generated Deepfakes in India," 233–50, 2025. https://doi.org/10.1007/978-981-97-8457-8_16.
- Creswell, John, and J David Creswell. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage publications, 2017.
- Efremova, Marina Aleksandrovna, and Evgeniy Aleksandrovich Russkevich. "Deepfake and Criminal Law." *Bull. Kazan L. Inst. MIA Russ.* 15 (2024): 97.
- Eurike Hailtik, Asri Gresmelian, and Wiwik Afifah. "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia." *Asian Journal of Social and Humanities* 2, no. 4 (January 22, 2024): 776–95. <https://doi.org/10.59888/ajosh.v2i4.222>.
- Hao, Zhiwen. "Criminal Law Regulation of AI Face-Swapping Crimes: Responsible Subjects, Theoretical Integration and Comprehensive Governance Framework." In *2025 4th International Conference on Public Management, Digital Economy and Internet Technology (ICPDI 2025)*, 149–70. Atlantis Press, 2025.
- Kumari, Deeksha. "Deepfake Technology and Legal Issues." *LawFoyer Int'l J. Doctrinal Legal Rsch.* 2 (2024): 234.
- LePage, Lauren. "Criminal Defenses in the Age of AI: An Examination of How Technological Advancements Are Challenging Traditional Duress and Mistake of Fact Defenses," 2025.
- Lin, Leo S.F. "Examining the Role of Deepfake Technology in Organized Fraud: Legal, Security, and Governance Challenges." *Frontiers in Law* 4 (April 16, 2025): 6–17. <https://doi.org/10.6000/2817-2302.2025.04.02>.
- Mohamed Hassan Mekki, . "The Challenges of Digital Evidence Usage in Deepfake Crimes Era." *Journal of Law and Emerging Technologies* 3, no. 2 (November 23, 2023): 176–232. <https://doi.org/10.54873/jolets.v3i2.123>.
- Nowak, Aleksandra, Bálint Tóth, and Andrei Ionescu. "Legal Challenges of Deepfakes: Liability, Harm, and Regulatory Responses." *Legal Studies in Digital Age* 2, no. 2 SE-Articles (n.d.): 49–60. <https://jlsda.com/index.php/lstda/article/view/306>.
- Pakerti, Asri, Fero Sanjaya, and Herlita Eryke. "CRIMINAL LIABILITY IN ARTIFICIAL INTELLIGENCE-BASED CRIMES: AN ANALYSIS OF THE NORMS IN INDONESIAN CRIMINAL LAW." *Syiah Kuala Law Journal* 10, no. 1 (2026).
- Perriello, Luca Ettore. "Blurred Realities: Legal Strategies for the Deepfake Era." *Maastricht Journal of European and Comparative Law*, March 27, 2026. <https://doi.org/10.1177/1023263X261433380>.
- Pratama, Andre Arya, Fikri Rosyad Fathurrahman, and Rani Lestari. "Criminal Liability Model for Deepfake AI Developers: European Union Inspiration for Indonesia's Legal Framework." *Ius Poenale* 6, no. 1 SE-Articles (January 15, 2026): 67–76. <https://doi.org/10.25041/ip.v6i1.4612>.
- Rahman, Rofi Aulia, and Rizaldy Anggriawan. "Deepfake and Electoral Crimes: Criminal Law Perspectives from Indonesia, India, Pakistan, and the US." *Indonesian Comparative Law Review (ICLR)* 7, no. 2 (2025): 132–46.
- Rezaei, Sara, and Mohammad Amini. "Criminal Liability in Deepfake-Related Image Identity Forgery," 2024.
- Sai, Songyang, and Zifan Wang. "Criminal Regulatory Approaches to Deepfake-Related Offenses: Focusing on the Crime of Fraud." *International Journal of Asian Social Science Research* 3, no. 1 (January 6, 2026): 20–31. <https://doi.org/10.70267/ijassr.260301.2031>.
- Schultz, David. "Personhood, Crimes, and Criminal Liability in the Age of Artificial Intelligence."

Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law 18, no. Suppl (2025): 301–8.

Sembiring, Jandrie, and Sunny Ummul Firdaus. "Criminal Liability for Misuse of Artificial Intelligence (Ai) in Deepfake Crimes." *International Journal of Multi Science* 5, no. 01 (2025): 1–9.

Souza, Raphael Ramos Monteiro de. "Legal Remedies and Regulatory Frameworks to Combat Ai-Driven Deepfakes." In *Mitigating the Risks of AI Deepfakes*, 94–116. CRC Press, 2026.

Sugahara, Maria Fernanda Santos. "Non-Consensual Dissemination of Pornographic Deepfakes," 2026.

Triana, Ikama Dewi Setia, Aniek Periani, and Arka Atyanta. "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China." *Kosmik Hukum* 26, no. 2 (May 7, 2026): 465–81. <https://doi.org/10.30595/kosmikhukum.v26i2.25751>.