INDONESIA LEGAL ADVANCED JOURNAL
Vol 1 Issue 2 Tahun 2026

Behind the Advancement of Artificial Intelligence Lies Deepfake as a Threat of Modern Digital Fraud

Zulfikar Anugrah[1], Nurul Qamar[2], Sutiawati Sutiawati[3]

[1,2,3] Faculty of Law, Universitas Muslim Indonesia, Indonesia

Surel Koresponden: anugrahzulfikar11@gmail.com

***Abstrak**: Perkembangan kecerdasan buatan (Artificial Intelligence/AI) telah membawa berbagai kemudahan dalam kehidupan modern, terutama dalam bidang komunikasi, otomasi, dan pengolahan data. Namun, di balik kemajuan tersebut muncul ancaman baru berupa teknologi deepfake, yaitu manipulasi audio, gambar, dan video berbasis AI yang mampu meniru identitas seseorang secara realistis. Penelitian ini bertujuan untuk menganalisis keberadaan deepfake sebagai bentuk penipuan digital modern, dampaknya terhadap masyarakat, serta upaya pencegahan yang dapat dilakukan. Metode yang digunakan adalah pendekatan kualitatif melalui studi literatur dengan mengkaji berbagai jurnal, artikel ilmiah, dan laporan terkait perkembangan deepfake. Hasil kajian menunjukkan bahwa deepfake dimanfaatkan dalam berbagai modus kejahatan, seperti pencurian identitas, penipuan finansial, penyebaran hoaks, pemerasan, dan manipulasi opini publik. Tingginya kualitas hasil rekayasa deepfake menyebabkan masyarakat sulit membedakan konten asli dan palsu, sehingga meningkatkan risiko kerugian material maupun nonmaterial. Oleh karena itu, diperlukan sinergi antara pemerintah, penyedia platform digital, pengembang teknologi, dan masyarakat dalam meningkatkan literasi digital, memperkuat regulasi, serta mengembangkan sistem deteksi deepfake yang lebih akurat. Dengan demikian, kemajuan AI perlu diimbangi dengan pengawasan dan pemanfaatan yang bertanggung jawab agar tidak menjadi sarana kejahatan digital.*

***Kata Kunci:** Kecerdasan Buatan, Deepfake, Penipuan Digital, Keamanan Siber, Literasi Digital.*

Abstract: The development of artificial intelligence (AI) has brought various conveniences to modern life, particularly in the fields of communication, automation, and data processing. However, behind this progress has emerged a new threat in the form of deepfake technology, namely AI-based audio, image, and video manipulation that can realistically imitate a person's identity. This study aims to analyze the existence of deepfakes as a form of modern digital fraud, their impact on society, and possible preventative measures. The method used is a qualitative approach through literature study by reviewing various journals, scientific articles, and reports related to the development of deepfakes. The results of the study indicate that deepfakes are used in various crime modes, such as identity theft, financial fraud, the spread of hoaxes, blackmail, and manipulation of public opinion. The high quality of deepfake engineering results makes it difficult for the public to distinguish genuine content from fakes, thereby increasing the risk of material and non-material losses. Therefore, synergy is needed between the government, digital platform providers, technology developers, and the public to improve digital literacy, strengthen

regulations, and develop more accurate deepfake detection systems. Thus, the progress of AI needs to be balanced with responsible supervision and use to prevent it from becoming a means of digital crime.

Keywords: Artificial Intelligence, Deepfake, Digital Fraud, Cybersecurity, Digital Literacy.

A. INTRODUCTION

The development of information and communication technology in the digital era has brought fundamental changes to various aspects of human life. The digital transformation, marked by the increasing use of the internet, social media, cloud computing, and smart devices, has created a new ecosystem that enables the exchange of information quickly, widely, and without geographical boundaries. In this context, artificial intelligence (AI) has emerged as one of the most influential innovations, driving efficiency, automation, and innovation in various sectors, such as education, healthcare, the creative industry, security, business, and government. The use of AI enables machines to mimic human cognitive processes, including pattern recognition, language processing, decision-making, and autonomously generating digital content. While this technology has provided significant benefits for modern civilization, it has also created new challenges in the form of misuse for harmful purposes.(Wanda & Putri, 2025)

One of the most prominent developments in AI in recent years is deepfake technology. Deepfake is an artificial intelligence-based media synthesis technique used to manipulate images, videos, and audio to realistically resemble specific individuals. This technology generally utilizes deep learning methods, specifically Generative Adversarial Networks (GANs), autoencoders, and voice synthesis models capable of learning facial characteristics, lip movements, voice intonation, expressions, and gestures. The resulting deepfakes often have such high visual and audio quality that they are difficult for the general public to distinguish from the original content.(Informasi et al., 2026) Initially, this technology was developed for positive purposes, such as film production, cultural preservation, digital voice-overs, educational simulations, and interactive marketing innovations. However, the increasingly open and accessible nature of the technology has made deepfakes vulnerable to misuse by irresponsible parties.(Andalas, 2026)

The misuse of deepfakes has shifted the pattern of crime from conventional crime to modern cybercrime based on digital identity manipulation. While previously fraud was carried out through document forgery, signature imitation, or direct impersonation, now perpetrators can use convincing-sounding fake videos and voices to deceive victims.(Noerman & Ibrahim, 2024)

This modus operandi has evolved into various forms, such as requests for money transfers using fake voices of company executives, fake videos of public figures to influence public opinion, the distribution of non-consensual pornographic content with the victim's face, and even relationship-based fraud via social media. By exploiting the victim's predisposition to trust visual and audio evidence, deepfakes have become a highly effective fraudulent tool.(Respati et al., 2024)

This phenomenon is increasingly dangerous because the public generally still places a high degree of trust in videos and audio recordings. In many situations, people are more likely to believe information conveyed through videos than plain text. When criminals are able to present a convincing visual and audio representation of a person, the line between fact and manipulation becomes blurred. This situation poses a serious threat to digital security, information integrity, and public trust in modern communication systems. The impact of deepfake abuse not only causes economic losses but also social, psychological, and legal harm. Economically, victims can lose money due to fake money transfers, fraudulent investments, or misuse of identities for illegal transactions. Socially, victims can experience defamation, damaged social relationships, and even loss of trust within their communities. Psychologically, victims often experience trauma, stress, anxiety, and mental distress due to the spread of manipulative content that attacks their personal reputation. Legally, evidence is difficult to establish because perpetrators can operate anonymously, use overseas servers, and utilize digital platforms across jurisdictions.

Furthermore, the threat of deepfakes also has the potential to disrupt social and political stability. Deepfake content depicting public figures or state officials can be used to spread disinformation, incite horizontal conflict, influence election results, or undermine the legitimacy of state institutions. In the context of national security, this technology can be exploited as a tool for propaganda and information warfare. Therefore, deepfakes are not merely an individual issue but a public issue with broad impacts on the social order. In Indonesia, the rapid growth of internet and social media usage has led to The public is vulnerable to the spread of AI-based manipulative content.(Sharif & Atif, 2025) Unequal digital literacy levels mean that many internet users lack the skills to verify the authenticity of digital content. This situation creates fertile ground for digital fraudsters to exploit deepfake technology. Meanwhile, the Indonesian legal system still focuses on general provisions regarding fraud, defamation, personal data protection, and cybercrime, without specific provisions regarding the characteristics of deepfake-based crimes.

Relevant regulations include the Criminal Code (KUHP), the Electronic Information and Transactions Law, the Personal Data Protection Law, and various regulations related to broadcasting and telecommunications. However, these provisions do not specifically define deepfakes, criminal elements related to AI-based digital identity manipulation, platform liability, victim redress mechanisms, or digital forensic evidence standards for synthetic content. This regulatory gap poses serious challenges in law enforcement practices. Law

enforcement officials often face difficulties determining the appropriate construction of articles, tracing perpetrators, collecting digital evidence, and assessing the validity of manipulated recordings. In academic studies, several previous studies have discussed deepfake technology from various perspectives. The first study highlighted deepfakes as a threat to privacy and personal data security. The study asserted that the unauthorized use of a person's face and voice constitutes a violation of privacy rights and potentially violates the principles of personal data protection. However, this study focused more on privacy aspects and did not fully examine deepfakes as an instrument of digital fraud with significant economic and social harm.

The second study examined deepfakes in the context of political disinformation and democratic security. The results showed that deepfake content can be used to manipulate public opinion, attack political opponents, and undermine public trust in democratic institutions. While important, this study focused on political and media threats and therefore did not comprehensively outline legal protections for individual victims of fraud or defamation through deepfakes. The third study examined the use of artificial intelligence in cybercrime in general, including automated phishing, intelligent malware, and social engineering-based attacks. In its discussion, deepfakes were identified as a new trend in digital crime. However, this study still positioned deepfakes as a subset of general cybercrime and did not make them a primary object of analysis with distinct legal characteristics. Furthermore, the study does not yet provide specific regulatory recommendations regarding perpetrator accountability, platform responsibility, and victim redress mechanisms. Based on these three studies, there are important research gaps that require further study. First, there are few studies that specifically address deepfakes as a form of digital fraud based on identity manipulation, rather than simply a privacy or disinformation issue. Second, there are still limited studies analyzing the adequacy of Indonesian positive law in addressing deepfake crimes. Third, there is no comprehensive formulation regarding the legal protection model for victims, whether in the form of prevention, prosecution, or redress. Fourth, few studies link the development of AI technology with the urgency of establishing adaptive regulations that can keep pace with rapid technological evolution.

Based on these gaps, this study is relevant and urgent. This study aims to analyze legal protection for victims of artificial intelligence misuse in the form of deepfakes, particularly those used as a means of modern digital fraud. Furthermore, this study aims to examine the urgency of establishing specific regulations that can address the challenges posed by the development of AI-based synthetic technology. This research is expected to provide both theoretical and practical contributions. Theoretically, this research can enrich the body of legal knowledge, particularly cyber law and technology law. Practically, the research findings can serve as a reference for legislators, law enforcement officials, digital platform providers, and the public in formulating protection strategies against the threat of deepfakes. The novelty of this research lies in its focus on deepfakes as a form of modern digital fraud based on identity

manipulation that is not yet specifically regulated in the Indonesian legal system, as well as its emphasis on the importance of a victim protection model and regulatory framework.

B. METHOD

This study employs a normative legal research method with a statutory, conceptual, and comparative approach. The statutory approach examines various legal provisions related to digital fraud, cybercrime, personal data protection, and regulations regarding the use of artificial intelligence technology in Indonesia. The conceptual approach examines the concept of deepfakes as a form of digital identity manipulation and its legal implications for victim protection. The comparative approach compares legal regulations in several countries that have begun to respond to the threat of deepfakes through specific policies or regulations. The types and sources of legal materials used include primary, secondary, and tertiary legal materials obtained through literature review. All legal materials are analyzed qualitatively using descriptive-analytical methods to identify the suitability of existing legal norms, identify legal gaps, and formulate recommendations for more adaptive regulations to the development of deepfake technology as a modern digital fraud threat.(Hehanussa et al., 2023)

C. DISCUSSION

1. Legal Protection for Victims of the Misuse of Artificial Intelligence in Deepfake Videos

The development of artificial intelligence (AI) has brought about significant changes in modern society. The use of AI is no longer limited to the industrial and research sectors, but has also penetrated the fields of communication, education, healthcare, security, commerce, and everyday activities. This technology can improve work efficiency, accelerate data analysis, and generate digital innovations that were previously difficult to achieve. However, behind these benefits, the development of AI also brings new consequences in the form of increasingly complex forms of digital crime. One of the most significant threats is the emergence of deepfake technology, an AI-based system capable of manipulating images, videos, and voices to realistically resemble specific individuals. The emergence of deepfakes demonstrates that technological progress does not always equate to social progress, because without adequate oversight and legal regulation, such innovations can actually turn into tools for modern crime.(Respati et al., 2024)

Deepfake basically works through machine learning algorithms that study a person's visual and audio characteristics, then reconstruct that identity in digital form.(Sharif & Atif, 2025) This system is capable of imitating a person's facial structure, expressions, lip movements, voice intonation, and even communication habits with a high degree of precision. Therefore, the results of deepfake engineering are often very difficult to distinguish from genuine content, especially for the general public who lack technical skills in digital forensics. Initially, this technology was developed for positive purposes, such as film production, visual effects creation, the preservation of historical figures in educational media, synthetic voice-

based cross-language translation, and innovation in the entertainment industry. However, increasingly open access to deepfake software and the low cost of producing digital content make this technology easily misused by parties with economic or criminal motives.(Alkhatib, 2025) The misuse of deepfakes as a tool for digital fraud demonstrates the evolution of criminal modus operandi in the cyber era. While previously fraud was mostly carried out through traditional methods such as document forgery, face-to-face identity impersonation, or fake text communications, perpetrators can now utilize convincing visual and audio evidence. Criminals can create videos of individuals appearing to give orders, make confessions, offer investments, or request fund transfers. In other forms, perpetrators can also imitate the voices of family members to request emergency assistance or impersonate company executives to instruct financial staff to disburse funds. Because people tend to trust voices and images as representations of truth, the success rate of deepfake-based fraud is much higher than that of conventional fraud.(Tahaoglu, 2025)

This phenomenon demonstrates that deepfake technology is not merely a tool for media manipulation but has evolved into a highly effective social engineering tool. In modern digital crime, perpetrators no longer simply attack computer systems but also target human perception and psychology. Victims are convinced by seemingly authentic visual and audio displays, leading them to perform certain actions without further verification. This situation makes deepfakes a serious threat because they target the weakest point in digital security: human trust. Even robust security systems can be breached if users believe the requests they receive come from a legitimate party. From the perspective of Indonesian positive law, legal protection for victims of deepfake abuse is essentially normative, although the provisions are still scattered across various regulations and do not specifically mention deepfakes as a separate legal object. The 2023 Criminal Code, through Article 492, regulates the crime of fraud. The fundamental element of fraud is the intention to unlawfully benefit oneself or another person through deception or a series of lies. In the context of deepfakes, this deception is realized through the creation of a false digital identity that resembles another person. Thus, the use of synthetic video or audio to gain economic advantage, deceive victims, or take property can be qualified as a criminal act of fraud.

In addition to the Criminal Code, Law Number 1 of 2024 concerning Electronic Information and Transactions is also relevant to addressing the misuse of deepfakes, particularly when false content is disseminated through electronic media and causes harm to the public. Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) provides a legal basis for the spread of false and misleading news that harms consumers in electronic transactions. In practice, deepfakes can be used to promote fake investments, advertise fictitious products, impersonate famous figures for fake endorsements, or spread false information that encourages the public to make certain economic decisions. Therefore, the misuse of deepfakes is not only related to identity forgery but also closely related to the crime of false information in the digital space. Furthermore, aspects of protecting the identity and privacy of victims are regulated through Law Number 27 of 2022 concerning Personal Data Protection. A person's face, voice, biometric image, and personal information are personal data inherent in an individual's identity. When this data is taken, processed, modified, and

used without consent for certain purposes, a violation of the right to privacy has occurred. In deepfake cases, perpetrators typically take photos, videos, or voice recordings of victims from social media, the internet, or other digital sources and then use them to train AI systems. This practice demonstrates that deepfake victims are not only harmed by fraud but also by the exploitation of their personal data. Therefore, personal data protection instruments are crucial as a basis for additional legal protection for victims.

Despite the availability of a general legal framework, law enforcement against deepfake crimes still faces numerous obstacles. The most fundamental issue is the difficulty of establishing evidence. New-generation deepfake technology is capable of producing high-quality visual and audio manipulations with minimal digital defects, and can mimic natural expressions and intonation. This makes it increasingly difficult to distinguish between genuine and fake content. Law enforcement officials require robust digital forensic capabilities to analyze file metadata, compression patterns, lighting discrepancies, lip movement anomalies, sound spectrum, and other algorithmic traces. Without adequate digital forensic laboratory support, the process of establishing evidence in court will be extremely difficult. Furthermore, deepfake crimes are transnational and anonymous. Perpetrators can create content in one jurisdiction, use servers in another country, use fake identities, and then distribute it to victims in Indonesia through global platforms. This situation raises issues of legal jurisdiction, cross-border data exchange, mutual legal assistance, and limits national authority over foreign technology companies. In many cases, the process of identifying perpetrators requires lengthy and complex international cooperation. Meanwhile, the victims' losses are swift and tangible. Thus, the effectiveness of law enforcement often lags behind the speed of digital crime itself.

From the victim's perspective, the impact of deepfakes is not only economic, but also social and psychological. Fraud victims can lose funds, assets, or access to digital accounts. However, more difficult-to-recover losses often include defamation, damaged professional reputations, family conflict, loss of public trust, and psychological trauma. If someone is depicted in a fake video containing immoral content, hate speech, or criminal activity, the social stigma can persist even if the content is proven to be fake. In the digital space, information trails spread rapidly and are difficult to completely erase. Once content goes viral, copies can continue to circulate across various platforms. This leaves victims with long-term consequences that cannot always be resolved through criminal prosecution of the perpetrator alone. This situation demonstrates that a legal protection model that focuses solely on punishing the perpetrator is inadequate. The legal approach needs to be expanded towards comprehensive victim protection. The state must ensure the availability of rapid reporting mechanisms, blocking and removing fake content, free legal aid for victims, restoration of good reputations, and psychological support. Furthermore, victims need to be given access to civil lawsuits to obtain compensation for reputational damage, economic loss, and immaterial suffering.

From a preventative perspective, improving the public's digital literacy is crucial. The public needs to be educated that video and audio can no longer always be considered absolute proof

of truth. The public must be accustomed to double-checking money transfer requests, emergency messages, and sensitive information received through digital media. Educational institutions, the government, and digital platforms need to work together to raise awareness about the characteristics of manipulative content and the risks of AI abuse. This education-based prevention is crucial because fraud victims often suffer from a lack of understanding of new crime methods. Meanwhile, digital platform providers must also assume greater responsibility. Social media platforms, instant messaging apps, and video service providers need to develop automated detection systems for synthetic content, label AI-generated media, and respond quickly and transparently to victim reports. Without active platform participation, the spread of deepfakes will continue to outpace the process of handling them. Therefore, future regulations need to mandate due diligence for digital platforms to prevent AI abuse. Thus, the misuse of deepfakes demonstrates that advances in artificial intelligence have a real dark side in the form of the threat of modern digital fraud. Technology, which should be a tool for progress, can turn into a means of exploitation if not balanced with ethics, oversight, and adaptive regulation. Therefore, more specific legal reforms regarding deepfakes, increased capacity of law enforcement, strengthened victim protection, and the development of digital literacy in the community are needed so that the benefits of artificial intelligence can continue to be enjoyed without sacrificing security and social justice.

2. The Urgency of Establishing Specific Regulations on the Misuse of Deepfake Artificial Intelligence.

The development of artificial intelligence (AI) in the digital era has brought about major changes in almost all sectors of human life. This technology is used in healthcare to aid disease diagnosis, in education for personalized learning, in industry for production automation, and in digital communications to improve efficiency and service quality. AI is also a key driver of the transformation of the global digital economy through its rapid data analysis capabilities, market behavior prediction, and the creation of technology-based innovations. One of the most prominent branches of AI development is generative technology, namely systems capable of automatically generating text, images, sound, and video. In this context, deepfakes are one of the products of generative technology that are developing very rapidly and have a broad impact on social, economic, and legal life. Deepfakes are AI-based technology that can manipulate a person's face, voice, gestures, and expressions to produce digital content that appears realistic and convincing. Through the use of machine learning algorithms such as deep learning and Generative Adversarial Networks (GAN), deepfake systems can learn from a person's visual and audio data, then produce a simulation that resembles that individual.(Zhang et al., 2025) In its early development, this technology was seen as a creative innovation beneficial to the film industry, game development, advertising, education, and cultural preservation. For example, it could be used to reconstruct historical figures in educational media or to assist with more natural dubbing across languages. However, as public access to deepfake software and the ease of use of AI

technology increased, these benefits came with a growing potential for serious abuse. Today, deepfakes have become a real threat in the form of modern digital crime. Criminals can use this technology to create fake videos depicting individuals performing certain actions, create fake voice recordings to deceive victims, or spread manipulative content to damage an individual's reputation. Globally, numerous cases of financial fraud have been discovered using the voices of company executives to order the transfer of funds to specific accounts. Furthermore, there are numerous cases of deepfakes being used for non-consensual pornography, the spread of political hoaxes, the manipulation of public opinion, and even blackmail based on fake content. This phenomenon demonstrates that deepfakes are no longer simply a technological issue but have become a social and legal issue that urgently requires specific regulation.(Fayyaz & Jumani, 2026)

The urgency of developing specific regulations regarding deepfakes stems from the fact that the characteristics of this technology differ from traditional forms of digital crime. Conventional cybercrime typically focuses on system hacking, data theft, malware distribution, or text-based fraud and regular communications. Meanwhile, deepfakes work by exploiting a person's identity through highly convincing visual and audio simulations.(Amerini et al., 2025) In other words, the core threat of deepfakes lies not simply in false information, but in creating a false reality that resembles reality. This is what makes the impact of deepfakes so much more dangerous, as people tend to believe what they see and hear. Therefore, common law approaches are often inadequate to address the complexities of this technology. (Politik et al., n.d.) In the Indonesian context, several regulations exist that can be used to address the misuse of deepfakes, such as the Criminal Code, the Electronic Information and Transactions Law, and the Personal Data Protection Law. However, these three legal instruments are sectoral in nature and have not been specifically designed to address the challenges of AI-based synthetic technology. For example, regulations on fraud only emphasize the element of deception, while ITE regulations focus on the distribution of false information, and personal data protection regulations emphasize the misuse of individual data. Yet, deepfakes often combine all of these elements: fraud, information manipulation, and the exploitation of personal data. This lack of comprehensive regulation creates legal uncertainty for victims, law enforcement officials, and technology industry players.

The importance of specific regulations is also related to the need for a clear legal definition. To date, the term "deepfake" is still used more in the technology realm than in the legal realm. The lack of a legal definition makes it difficult to identify the object of regulation, the limits of prohibited actions, and the scope of legal liability. New regulations need to provide clear definitions of deepfakes, synthetic media, biometric manipulation, digital impersonation, and the non-consensual use of AI. Clear definitions will help law enforcement officials, judges, academics, and the public understand and consistently apply the rules. Furthermore, specific regulations are essential to classify various forms of deepfake misuse. Not all uses of

deepfakes are unlawful; in the entertainment or educational sectors, this technology can be used legitimately and beneficially. Therefore, the law needs to distinguish between legitimate and harmful uses. Forms of misuse that need to be regulated include financial fraud, identity theft, non-consensual pornography, defamation, political manipulation, blackmail, national security threats, and non-consensual use for commercial purposes. This classification is crucial to ensure that law enforcement is proportionate and does not stifle legitimate innovation. Victim protection is also a key reason for the need for specific regulations. Deepfake victims often experience multidimensional losses. Economically, victims can lose money due to fraudulent transfers, fake investments, or manipulated digital transactions. Socially, victims can lose their reputation, public trust, jobs, or family relationships. Psychologically, victims can experience severe stress, depression, trauma, and a sense of insecurity due to their identities being used without permission. Even when the perpetrator is apprehended, the victim's losses are not immediately remedied because the fake content can continue to circulate online. Therefore, specific regulations must include victims' rights to request content removal, restoration of their good name, compensation, psychological rehabilitation, and further identity protection. Beyond individual victims, the wider community is also harmed by the misuse of deepfakes. The distribution of fake videos or audio involving public figures can cause social unrest, divide communities, trigger horizontal conflict, or disrupt the democratic process.

During elections, for example, deepfakes can be used to portray certain candidates as making controversial statements. If such content is widely disseminated before verification, the impact can affect public opinion and the legitimacy of democracy. Therefore, specific regulations aim not only to protect individuals but also to maintain public order and public trust in digital information. The importance of specific regulations is also closely related to the responsibilities of technology developers and digital platforms. Many deepfake applications are openly available online, with increasingly sophisticated and user-friendly features.(Riset & Edukasi, 2026) Meanwhile, social media and video-sharing platforms have become the primary means of disseminating manipulative content. In this context, the law needs to place responsibility on parties with structural roles in the digital ecosystem. Technology developers should be required to implement safeguards, digital watermarks, usage restrictions, and abuse reporting systems. Digital platforms should be required to moderate content, automatically detect, label synthetic media, and expeditiously remove unlawful content. Without clear legal obligations, the spread of deepfakes will consistently outpace efforts to address them. From a law enforcement perspective, specific regulations are also needed to strengthen digital evidence standards. Modern deepfake content is extremely difficult to detect with the naked eye. Therefore, law enforcement officials need a legal basis to use digital forensic methods, obtain access to platform log data, seek the assistance of AI experts, and admit certain electronic evidence in judicial proceedings. Specific regulations can govern digital media authentication standards, procedures for

verifying the authenticity of video and audio, and procedures for the legitimate collection of electronic evidence. This is crucial to ensure that the law enforcement process is not hampered by procedural gaps.

Furthermore, deepfake crimes are cross-border in nature. Perpetrators can be located abroad, use foreign servers, and distribute content to victims in Indonesia within seconds. This situation raises issues of jurisdiction, extradition, mutual legal assistance, and cooperation between national authorities. National regulations need to be designed in line with international standards so that Indonesia can actively participate in combating AI-based crimes globally. Without international coordination, perpetrators will continue to exploit loopholes between countries to avoid legal accountability. From a future legal policy perspective, specific regulations for deepfakes should ideally contain several key elements. First, a legal definition of deepfakes and AI-based synthetic media. Second, limits on permitted and prohibited uses. Third, classification of criminal acts and administrative, civil, and criminal sanctions. Fourth, responsibilities of application and digital platform developers. Fifth, mechanisms for victim protection and recovery. Sixth, standards for digital forensics and evidence. Seventh, mechanisms for international cooperation and regular updates in line with technological developments. With this design, regulations will not only be reactive, but also preventive and adaptive. Ultimately, establishing specific regulations regarding the misuse of deepfake artificial intelligence is a legal necessity that cannot be postponed. The development of AI technology will continue to move rapidly, while the law cannot lag too far behind. The state must be present to ensure that technological innovation continues within the bounds of ethics, security, and justice. Specific regulations are not obstacles to progress, but rather instruments to prevent technological advancement from becoming a threat to society. With clear regulations, strong victim protection, effective law enforcement, and the accountability of all stakeholders, the benefits of artificial intelligence can continue to grow without compromising basic human rights and social stability.

D. CONCLUSION

Based on this discussion, it can be concluded that the development of artificial intelligence has brought significant benefits to modern life, but on the other hand, it has also given rise to serious threats in the form of misuse of deepfake technology as a form of modern digital fraud. Deepfakes allow for realistic manipulation of a person's face, voice, and identity, which can be used for financial fraud, defamation, privacy violations, the spread of disinformation, and even the disruption of public trust. Although Indonesian positive law already has general instruments through the Criminal Code, the Electronic Information and Transactions Law, and the Personal Data Protection Law, these regulations have not been able to comprehensively address the increasingly complex, cross-border, and difficult-to-prove characteristics of deepfake crimes. Therefore, special regulations are needed that address definitions, forms of prohibition, legal liability, victim protection, digital platform responsibility, forensic evidence standards, and international cooperation. Therefore, the establishment of special regulations is an urgent step

to ensure that the advancement of artificial intelligence remains within the legal and ethical corridors and protects the public from the threat of modern digital crime..

E. REFERENCE

Alkhatib, M. (2025). *A Multifaceted Deepfake Prevention Framework Integrating Blockchain , Post-Quantum Cryptography , Hybrid Watermarking , Human Oversight , and Policy Governance*. 1–28.

Amerini, I., Barni, M., Battiato, S., Bestagini, P., Boato, G., Bruni, V., Caldelli, R., Natale, F. De, Nicola, R. De, Guarnera, L., Orrù, G., Ortis, A., Perazzo, P., Puglisi, G., & Purnekar, N. (2025). *Deepfake Media Forensics : Status and Future Challenges*. 1–42.

Andalas, U. (2026). *Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.1 (2026) Tema/Edisi : Hukum Internasional dan Perbandingan Hukum (Bulan Kesatu) https://jhlg.rewangrencang.com/*. *7*(1), 1–28.

Fayyaz, U., & Jumani, T. A. (2026). *A Comprehensive Review of Deepfake Detection Techniques : From Traditional Machine Learning to Advanced Deep Learning Architectures*.

Hehanussa, D. J. A., Sopacua, M. G., Surya, A., Titahelu, J. A. S., Monteiro, J. M., Siregar, R. A., Bagenda, C., Rinaldi, K., Rifa'i, I. J., Nurwandri, A., Aidil, A. M., Hasanuddin, H., Zaleha, Z., Satory, A., & Irwanto, I. (2023). *METODE PENELITIAN HUKUM* (E. Jaelani (ed.)). CV WIDINA MEDIA UTAMA.

Informasi, D. U., Transaksi, D. A. N., Data, P., Uu, P., Di, P. D. P., Fitriani, N. A., & Wahyudi, E. (2026). *KEBIJAKAN FORMULASI TINDAK PIDANA DEEPFAKE ELEKTRONIK (UU ITE) DAN UNDANG-UNDANG*. *12*(1), 157–169. https://doi.org/10.55809/tora.v12i1.647

Noerman, C. T., & Ibrahim, A. L. (2024). *Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara Criminalization of Deepfake in Indonesia as a Form of State Protection hakikatnya dapat memberikan kemudahan dalam melakukan apapun . Artificial intelligence*. *7*(2), 1–4.

Politik, A. J., Humaniora, H., Nomor, V., Quratuainniza, H. S., & Nurkhaerani, E. (n.d.). *Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan Deepfake di Indonesia Fakultas Hukum , Universitas pembangunan Nasional " Veteran " Jakarta melakukan Tindakan kejahatan maupun sebagai objek dari kejahatan tersebut . 4*.

Respati, A. A., Setyarini, A. D., Parlagutan, D., & Rafli, M. (2024). *Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban*. *2*(2), 586–592.

Riset, J., & Edukasi, M. (2026). *Dampak teknologi ai terhadap pola kejahatan*. *3*, 304–316.

Sharif, H., & Atif, A. (2025). *Deepfake-Style AI Tutors in Higher Education : A Mixed-Methods Review and Governance Framework for Sustainable Digital Education*. 1–27.

Tahaoglu, G. (2025). *Robust DeepFake Audio Detection via an Improved NeXt-TDNN with Multi-Fused Self-Supervised Learning Features*. *Vc*, 1–25.

Wanda, D., & Putri, S. (2025). *Perlindungan hak privasi dalam penyalahgunaan teknologi*. *14*, 195–210.

Zhang, B., Cui, H., Nguyen, V., & Whitty, M. (2025). *Audio Deepfake Detection : What Has Been Achieved and What Lies Ahead*.