DEVOTION
Journal of Research and Community Service
Volume 7, Number 6, June 2026
e-ISSN: 2797-6068 and p-ISSN: 2777-0915

Criminal Liability for the Spread of Deep Fake-Based Pornographic Content on Social Media

Rangga Agin Wijaya, Endang Sutrisno, M. Noupel
Universitas Swadaya Gunung Jati, Indonesia
Email: ranggaaginw25@gmail.com, Endang.Sutrisno@ugj.ac.id, mnoupel@ugj.ac.id

Keywords:
deepfake, pornography, criminal liability, artificial intelligence, criminal law.

Abstract
The development of artificial intelligence (AI) technology has given rise to various digital innovations, one of which is deepfake technology, which can manipulate images, videos, or audio to make them appear authentic. In addition to providing benefits, this technology also has the potential to be misused to create and disseminate pornographic content without the victim's consent. Such actions can harm the victim's honor, privacy, reputation, and psychological well-being, thereby creating legal issues that require adequate regulation and enforcement. This study aims to analyze the legal regulation and criminal liability of perpetrators involved in the dissemination of deepfake-based pornographic content in Indonesia. The method used is normative legal research with statutory and conceptual approaches. The research data were obtained through a literature review of laws and regulations, legal literature, scientific journals, and other relevant legal sources, and were then analyzed qualitatively. The results of the study show that the dissemination of deepfake-based pornographic content essentially fulfills the elements of a criminal offense and that perpetrators may be held criminally liable. Although there is no specific regulation on deepfakes, these acts may be prosecuted under the Pornography Law, the Electronic Information and Transactions Law, the Criminal Code, and the Personal Data Protection Law. However, law enforcement still faces obstacles related to regulatory limitations, digital evidence, and the identification of perpetrators. Therefore, more adaptive legal reform and the strengthening of law enforcement capacity are needed to ensure legal certainty and effective protection for victims.

INTRODUCTION

The development of information and communication technology in the digital era has created significant transformations in various aspects of people's lives, especially in the ways people communicate and disseminate information. Social media is no longer used merely as a tool for interaction but has also evolved into a digital public space that enables everyone to create and disseminate information quickly, widely, and without limitation. On the other hand, these developments have also been accompanied by the emergence of various forms of technology-based crime, or cybercrime, which are increasingly complex and difficult for the applicable legal system to control (Ballakur & Arya, 2020; Chen et al., 2020; Choi, 2018).

One form of technological development that raises new legal problems is deepfake technology, which is based on artificial intelligence (AI) (Cui et al., 2020; Depuru et al., 2024; Jatavallabha et al., 2024). This technology enables realistic visual and audio manipulation of a person by utilizing machine learning algorithms. Although it was initially developed for positive purposes, such as in the entertainment and education industries, in practice, this

technology is often misused, especially in the creation and dissemination of pornographic content involving the manipulation of a person's identity without consent (Fauzi et al., 2025).

In Indonesia, the dissemination of deepfake-based pornographic content has increasingly shown an alarming trend, especially through various social media platforms. This kind of content is generally created by placing the victim's face onto pornographic material, thereby creating a false representation that appears real. The ease of access to deepfake technology, both through free and paid applications, makes this practice possible for anyone, even without special skills (Kasumba et al., 2025; Kulkarni et al., 2021). In addition, the characteristics of social media, which allow the rapid and massive dissemination of content, make such content difficult to control, as it may continue to circulate even after being removed from its original source (Law, 2024).

The impact caused by the dissemination of such content cannot be considered a minor problem. Victims not only suffer legal harm but also experience psychological distress, reputational damage, and prolonged social stigma (Ain, 2024; Aini et al., 2023; Anupkumar, 2023). In addition, the use of biometric data in the form of facial images without consent constitutes a violation of the right to privacy and can lead to further forms of crime, such as extortion or digital exploitation (No et al., 2025).

The problem becomes increasingly complex when associated with the aspect of criminal law enforcement in Indonesia. To date, there has been no specific regulation that explicitly governs deepfakes. Law enforcement still relies on general provisions, such as the Pornography Law, the Electronic Information and Transactions Law, and the Personal Data Protection Law (Babar et al., 2022; Kalman et al., 2025). However, these provisions have not been fully able to address the characteristics of deepfakes as content produced through technological manipulation that is not real but has real consequences. This raises problems in determining the elements of criminal offenses and the culpability of perpetrators, including in the evidentiary process (Arvitto, 2025).

This condition indicates a mismatch between technological development and the development of criminal law. The absence or ambiguity of legal norms has the potential to cause legal uncertainty, both for law enforcement officials and for the public. In addition, previous studies have tended to discuss pornography or cybercrime in general, so they have not examined in depth the aspect of criminal liability in the context of the dissemination of deepfake-based pornographic content on social media (Fauzi et al., 2025).

Based on this description, a more comprehensive and focused study is needed to examine how the concept of criminal liability can be applied to perpetrators involved in the dissemination of deepfake-based pornographic content on social media. This research is important because it aims to assess the extent to which the applicable legal provisions are aligned with the increasingly rapid development of technology and to identify weaknesses in existing regulations. Therefore, the research findings are expected to contribute to the development of criminal law that is more responsive and adaptive to current developments, while also providing optimal legal protection for victims in the digital era (Darmawan et al., 2025).

METHOD

In this study, legal materials were collected through library research by examining various relevant legal sources, including laws and regulations, legal literature, scientific journals, and other supporting references. In addition, information from online mass media was used to obtain factual descriptions of cases related to the dissemination of pornographic content based on artificial intelligence technology, particularly deepfakes.

Based on the results of a review of several news reports, a case was identified in the Cirebon area involving the dissemination of immoral photos manipulated using artificial intelligence technology. The case attracted public attention because it involved students as both suspected perpetrators and victims. The local police conducted an investigation after receiving reports regarding the circulation of photos that had been manipulated to display inappropriate content. In this incident, the victim's photo was allegedly taken from a social media account without permission and then processed using an AI-based application to produce an image that appeared realistic.

Furthermore, the analyzed sources indicated that the perpetrators' actions did not stop at the manipulation process but continued with the dissemination of the content through digital media. There were also indications that the content was circulated through certain platforms for specific purposes, thereby expanding its impact. The number of victims in this case was not limited to one individual but involved several others, some of whom had not yet reported the incidents they experienced.

In terms of impact, the case showed that the victims experienced significant psychological pressure, including shame, fear, and disruption to their social lives. This was caused by public perception, as not all members of the public understood that the circulating content was the result of digital manipulation. Therefore, although the content was not real, the harm experienced by the victims remained real and serious.

In addition, the involvement of students as perpetrators added complexity to the handling of the case. The law enforcement process did not only focus on the criminal aspect but also needed to consider a rehabilitative approach in accordance with the juvenile criminal justice system. Thus, the handling of this type of case required more comprehensive attention.

Based on this explanation, information obtained from online media could be categorized as secondary legal material that played an important role in supporting the research analysis. These sources provided a concrete illustration of how the dissemination of deepfake pornography occurred in society, including the patterns of the perpetrators' actions, the impact on victims, and the obstacles faced in the law enforcement process.

Through the collection of these legal materials, the researchers were able to gain a deeper understanding of the phenomenon under study. This understanding served as a basis for analyzing the criminal liability of perpetrators and assessing the extent to which existing laws were able to address the increasingly rapid development of technology.

RESULT AND DISCUSSION

The Phenomenon of Spreading Deepfake-Based Pornography on Social Media: A Case Study and Analysis of Criminal Accountants in Cirebon

The development of digital technology in recent years has had a significant impact on changes in crime patterns in society, including in the Cirebon area. Based on the findings of

the research obtained through the study of various developing cases, as well as supported by the analysis of legal literature and relevant news, it can be seen that there is a tendency to emerge new forms of crime that utilize artificial intelligence (AI), especially in the form of manipulation of visual content that leads to deepfake-based pornography.

The findings show that there has been a shift in the character of crime from the previous conventional to a much more complex digital technology-based crime. This development also presents its own challenges, especially in terms of the process of identifying, proving, and enforcing the law against the perpetrators of these crimes.

In the last five years, especially in 2025, there have been cases involving the use of deepfake technology against students in the Cirebon area. In this case, at least two victims, who were high school students, were subjected to photo manipulation by three perpetrators who also came from the same neighborhood. The victim's photo was taken from a social media account without consent, then processed using an artificial intelligence (AI) application to produce an image that resembled pornographic content. This case was then reported to the police and became one of the initial indications of the development of deepfake crime in the area.

In addition, based on the study of various cases that have developed, it can be seen that similar practices do not only occur on a limited scale, but also involve a wider number of victims. In several incidents, it was found that there was more than one victim who experienced image manipulation with a relatively similar pattern, namely the use of photos taken from social media to then be processed into immoral content. This condition shows that the phenomenon has a tendency to occur repeatedly with a similar pattern. Furthermore, it is possible that the actual number of cases is much larger, considering that there is a tendency for victims not to report the events they experience due to psychological factors and social pressures faced.

This situation indicates that the practice of deepfake pornography can be qualified as a criminal act within the framework of criminal law. When viewed through the theory of criminal responsibility, the series of actions of the perpetrators starting from obtaining, processing, to distributing the content is a form of real act (actus reus). Meanwhile, the existence of awareness and the will of the perpetrator in carrying out the act shows the fulfillment of the element of guilt (mens rea). Therefore, even though the content produced is the result of digital engineering, the act can still be held criminally liable because it has fulfilled the elements of acts and mistakes as constructed in the theory of criminal liability.

When reviewed based on positive law in Indonesia, the act can basically be qualified as a criminal act as reflected in the provisions of Article 27 paragraph (1) of the Electronic Information and Transaction Law and the provisions in the Pornography Law. However, the lack of regulations specifically regulating deepfakes poses various obstacles, especially in terms of proving and determining clear boundaries between real content and content that is the result of digital engineering (Herman & Fernhout, 2023; Levi & Smith, 2022).

Patterns of Acquisition and Use of Victim Data through Social Media

The results of the study show that social media has a significant role in the emergence of deepfake pornography crimes. Based on literature review and analysis of various cases that have been published, it is known that perpetrators generally obtain victim data through various social media platforms, such as Instagram, WhatsApp, and other platforms that provide access to users' personal photos.

In practice, the perpetrator did not make direct contact with the victim in the early stages. They tend to only collect photos that they deem appropriate, then leverage them to process using artificial intelligence-based applications. This condition shows that deepfake crimes have different characteristics from conventional crimes, because they do not require direct interaction or psychological approaches to the victim.

Furthermore, from the results of a review of various sources of legal literature and news, the ease of accessing personal data through social media is one of the factors that encourage the occurrence of these crimes. Not a few users are not aware that the photos they upload have the potential to be misused by other parties for adverse interests. This indicates that there are weaknesses in personal data protection, which are then used by perpetrators to commit unlawful acts.

Thus, it can be understood that social media not only serves as a means of communication, but also has the potential to be a source of data that can be misused to commit technology-based crimes, including deepfake pornography.

The Process of Manipulating and Spreading Deepfake Content

After the victim's data was obtained, the perpetrator then carried out the manipulation stage by utilizing an artificial intelligence-based application. Based on a literature review and a study of a number of cases that have occurred, this process is carried out with technology that allows the merging of the victim's face with other parts of the body, resulting in a visual that looks convincing and resembles real conditions.

These technological advances have made engineering results increasingly difficult to distinguish from the original images by the general public. This poses an obstacle in proof, because certain technical skills are required to determine whether a content is the result of digital manipulation or not.

After the manipulation process is completed, the content is then disseminated through various digital means. Its distribution can be limited, for example through certain groups, or extended through online platforms. In practice, this content is often used to degrade the dignity, mock, or humiliate the victim.

In addition, from an analysis of the pattern of information dissemination in digital media, it is known that the speed of distribution is a factor that aggravates the impact of this crime. In a short time, content can spread widely and is difficult to control, resulting in greater losses to victims.

The impact experienced by the victim

The crime of deepfake pornography is not only related to the legal aspect, but also has a fairly wide impact on the psychological condition and social life of the victim. Based on literature review and tracing of various cases that have been published, victims generally experience emotional distress, such as shame, anxiety, and decreased confidence.

In addition, victims often face negative assessments from the surrounding environment. This happens because not all parties understand that the content circulating is the result of digital engineering, not an actual event. As a result, victims can experience disturbances in carrying out daily activities, both in the educational environment and in their social life.

Furthermore, there is a tendency that some victims choose not to continue the legal process. This is influenced by disturbed psychological conditions and the perceived social

pressure. The situation shows that the impact of deepfake crime does not only occur in the short term, but can also continue for a long time.

Therefore, deepfake pornography can be viewed as a serious form of offense, as it not only causes legal harm, but also has a significant impact on the psychological state and overall social life of the victim.

Law Enforcement Against Deepfake Pornography in Cirebon

From the perspective of law enforcement, the handling of deepfake pornography crimes is still faced with a number of obstacles. Based on a review of the legal literature and a study of law enforcement practices that have been published, one of the main obstacles lies in the lack of regulations that specifically regulate the use of deepfake technology.

In its application, law enforcement against these acts still relies on general provisions, such as the Electronic Information and Transaction Law, the Pornography Law, and the Personal Data Protection Law. However, these provisions have not been fully able to accommodate the typical characteristics of crimes involving deepfake technology.

In addition, the process of identifying perpetrators is also a challenge in itself, considering that perpetrators can relatively easily hide their identities in digital spaces. On the other hand, proving a case is also not simple, because it requires certain technical skills to distinguish between the original content and the manipulated content.

Therefore, even though law enforcement against deepfake pornography crimes has been carried out through existing legal instruments, it is still necessary to strengthen, both in terms of regulation and capacity building of law enforcement officials to be able to keep up with increasingly rapid technological developments.

General Analysis of Research Results

In general, deepfake pornography crimes show a relatively systematic pattern, which begins with the collection of victim data through social media, then continues with the manipulation process using artificial intelligence-based technology, until finally disseminated through various digital platforms.

When compared to conventional crime, this form of crime does not require direct interaction between the perpetrator and the victim, so its existence tends to be more difficult to detect from the initial stage. In addition, the impact is also more complex, because it not only touches on the legal aspect, but also affects the psychological, social, and reputational conditions of the victim.

On the other hand, law enforcement efforts against this crime still face a number of obstacles, both related to regulatory aspects and technical obstacles. This condition reflects that technological developments are progressing faster than legal readiness in anticipating new forms of crime that emerge (Burke et al., 2019; Dwisari et al., 2023).

Therefore, more comprehensive steps are needed, both through regulatory reforms, increasing the capacity of law enforcement officials, and strengthening public awareness regarding the importance of personal data protection. These efforts are important so that the handling of deepfake pornography crimes can be carried out more effectively and be able to provide optimal protection for victims (Kruse & Beane, 2023).

Normative Provisions in the Dissemination of Pornographic Content

Based on this description, it can be understood that the act in the crime of deepfake pornography has in essence fulfilled the elements of criminal acts in positive criminal law in Indonesia. The act of obtaining, processing, and disseminating immoral content through electronic media can be qualified as an act that is contrary to the provisions of the Electronic Information and Transaction Law, especially Article 27 paragraph (1), as well as the provisions in the Pornography Law. When viewed from the perspective of criminal law, the act has basically fulfilled the elements of criminal acts, especially those related to moral violations and defamation. In this case, the use of the Electronic Information and Transaction Law can be used as a legal basis, especially related to the act of distributing or transmitting content that contains content that violates morality through electronic media. In addition, the Pornography Law can also be used to assess these acts as actions that are contrary to the moral norms that apply in society. However, the existence of content produced through digital engineering poses its own challenges in classifying these acts legally (Ramadhani, 2025).

When associated with the theory of legal certainty, this condition shows that Indonesia's positive law is still not fully able to provide clarity in regulating new technology-based crimes. This ambiguity can have an impact on the law enforcement process, both in the investigation, prosecution, and court examination stages. Therefore, legal reforms are needed that are able to accommodate technological developments, especially those related to the use of artificial intelligence in digital crime (Dwiandari & Arifin, 2025).

In a theoretical framework, this condition can be analyzed through the thinking of Prof. Dr. Endang Sutrisno who emphasizes that law cannot be seen as a static system, but must function as a means of social change that is adaptive to the development of society. In his article entitled Role of Law in Construction and Development of Small Scale Industries Through Normative Perspective, Sutrisno emphasized that law has an important role in creating a balance between certainty, justice, and utility, and must be able to adapt to evolving social dynamics (Sutrisno, 2010).

This view becomes very relevant in looking at the phenomenon of deepfake pornography, where technological developments are much faster than legal developments. Under such conditions, the criminal law that is still conventional has not been fully able to reach new forms of crime based on artificial intelligence. This shows that there is a gap between technological developments and legal readiness to regulate them, so a more responsive and adaptive legal approach is needed (Wafi & Wisnubroto, 2025).

In addition, from the perspective of legal culture, Prof. Endang Sutrisno also emphasized that the effectiveness of the law is greatly influenced by the legal awareness of the community. Low digital literacy and a lack of public understanding of the risks of misuse of technology are one of the factors that encourage the occurrence of deepfake pornography crimes. In many cases, perpetrators take advantage of the ease of access to digital data available on social media, while victims are unaware that the data can be misused (Sutrisno, 2010).

In addition to the normative aspect, another obstacle faced in law enforcement against deepfake pornography is the technical aspect. Based on the results of the research, law enforcement officials experienced difficulties in identifying the perpetrators and collecting relevant evidence. This is due to the characteristics of cybercrime that allow perpetrators to hide identities as well as use various means to eliminate digital traces. On the other hand, the

technology used in creating deepfakes is increasingly sophisticated, requiring special expertise to distinguish between genuine content and manipulated content (Sy, 2025).

From a criminological perspective, this phenomenon can be categorized as a form of modern crime that is influenced by technological developments. The crime of deepfake pornography is not only driven by individual factors, but also by the ease of access to technology and the lack of oversight in the use of digital media. This shows that such crimes cannot be dealt with only through a legal approach, but also require a social and educational approach.

On the other hand, the impact it has on victims suggests that the crime of deepfake pornography has serious consequences. Victims not only suffer legal losses, but also face quite heavy psychological pressure, such as shame, fear, and disruptions in social life. In some cases, victims even choose not to report the incident they experienced for fear of the stigma that might arise. This condition shows that deepfake crimes have a wider impact compared to conventional crimes.

Thus, based on the analysis that has been carried out, it can be understood that the problem of deepfake pornography in Indonesia is not only related to the fulfillment of criminal elements, but also concerns the limitations of legal regulation, technical obstacles in law enforcement, and low public legal awareness. Therefore, in accordance with the thinking of Prof. Dr. Endang Sutrisno, it is necessary to reform the law more adaptively and increase the legal awareness of the community, so that criminal law can function effectively in providing protection to victims and ensnare the perpetrators of technology-based crimes (Sutrisno, 2010)

CONCLUSION

Based on the results of the research, it can be concluded that the development of artificial intelligence (AI) technology, especially deepfake technology, has given rise to a new form of crime involving the dissemination of pornographic content through digital media. This act is carried out by utilizing the victim's personal data to produce manipulated content that appears realistic, thereby causing harm to the victim's honor, privacy, and reputation.

From a criminal law perspective, the dissemination of deepfake-based pornographic content essentially fulfills the elements of a criminal offense, and perpetrators may be held criminally liable. Although there is no specific regulation concerning deepfakes, the provisions of the Electronic Information and Transactions Law, the Pornography Law, the Criminal Code, and the Personal Data Protection Law may be used as legal bases to prosecute perpetrators. However, obstacles remain in law enforcement, particularly in relation to evidentiary issues and technological developments that progress more rapidly than legal reform.

Therefore, legal reform that is more responsive to the development of digital technology is needed, along with the strengthening of law enforcement officials' capacity to handle crimes based on artificial intelligence. This step is important to ensure legal certainty, provide optimal protection for victims, and guarantee the effectiveness of law enforcement against deepfake-based pornography crimes in Indonesia.

REFERENCES

Aini, H., School, N., Tekhnologi, T., & Yogyakarta, K. (2023). Analysis of delay management due to weather related to operational technicalities at Citilink Airlines at Komodo Labuan Bajo Airport. *Journal of General Studies and Research, 1*(4), 71–83.

Ain, N. (2024). Navigating passenger compensation: Implications for airlines and consumers. *Journal of Air Law and Commerce, 89*(3), 507.

Anupkumar, A. (2023). Investigating the costs and economic impact of flight delays in the aviation industry and the potential strategies for reduction.

Arvitto, R. S. (2025). Implikasi hukum deepfake: Telaah terhadap UU ITE dan UU PDP (Legal implications of deepfake: A review of the ITE Law and the PDP Law). *Jurnal Hukum*, 4(2), 73–82.

Ballakur, A. A., & Arya, A. (2020). Empirical evaluation of gated recurrent neural network architectures in aviation delay prediction. *IEEE Transactions on Aerospace and Electronic Systems, 56*(3), 1890–1902.

Babar, Z., et al. (2022). Consumer's perception towards electricity theft: A case study. *Energy Policy*.

Burke, P. J., Widnyana, J., Anjum, Z., Aisbett, E., Resosudarmo, B. P., & Baldwin, K. G. H. (2019). Overcoming barriers to solar and wind energy adoption in two Asian giants: India and Indonesia. *Energy Policy, 132*, 1216–1228.

Chen, H., Jiang, L., Yang, H., Lu, Z., Fu, Y., Li, L., & Yu, Z. (2020). An efficient hardware architecture with adjustable precision and extensible range to implement sigmoid and tanh functions. *Electronics, 9*(10), 1739.

Choi, C. (2018). Time series prediction with recurrent neural networks in presence of missing data. *Journal of Machine Learning Research, 19*(1), 1–25.

Cui, Z., Ke, R., Pu, Z., & Wang, Y. (2020). Stacked bidirectional and unidirectional LSTM recurrent neural network for predicting network-wide traffic state with missing values. *Transportation Research Part C: Emerging Technologies*, *118*, 102674.

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan hukum terhadap penyalahgunaan deepfake pada pornografi anak di era artificial intelligence di Indonesia. *Jurnal Hukum*, 18(01), 42–54.

Depuru, S., et al. (2024). Enhancing flight delay prediction and classification using a hybrid Bi-LSTM. *Communications on Applied Nonlinear Analysis, 31*(6S), 15–28.

Dwiandari, A. S., & Arifin, R. (2025). Criminal law enforcement on digital identity misuse in AI era for commercial interests in Indonesia.

Dwisari, V., Sudarti, S., & Yushardi, Y. (2023). Pemanfaatan energi matahari: Masa depan energi terbarukan. *OPTIKA Jurnal Pendidikan Fisika, 7*(2), 376–384.

Fauzi, S. S., Rusmana, I. P. E., & Darma, I. M. W. (2025). Pengaturan sanksi pidana terhadap pelaku pembuat konten pornografi dengan menggunakan teknologi deepfake di Indonesia.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Herman, H., & Fernhout, F. J. (2023). Maximum limitation of fines for economic crimes in Law Number 1 of 2023. *Jurnal IUS, 11*(2).

Jatavallabha, A., Gerlach, J., & Naresh, A. (2024). Deciphering air travel disruptions: A machine learning approach. *arXiv*.

Kalman, R., Kusno, K., & Siregar, A. (2025). Legal study of criminal acts of electricity theft.

Kasumba, D., et al. (2025). Electricity theft and its impact on quality of service.

Kruse, C. S., & Beane, A. (2023). Health information technology continues to show positive effect on medical outcomes: Systematic review. *Journal of Medical Internet Research, 25*, e41277.

Kulkarni, Y., et al. (2021). EnsembleNTLDetect: An intelligent framework for electricity theft detection.

Levi, M., & Smith, R. G. (2022). Fraud and economic crime in public utilities. *Journal of Financial Crime*.