Vol. 6, No. 1, January 2026
E-ISSN:2723 – 6692
P-ISSN:2723– 6595
http://jiss.publikasiindonesia.id/

Juridical Analysis of Legal Responsibility for the Dissemination of Deepfake Content on Social Media

Harri Prasetyo Rachmatullah
Universitas Pancasila, Indonesia
Email: harriprasetyo1994@gmail.com

KEYWORDS

Deepfake; Legal Liability; Social Media; Normative Legal Research; Legal Protection.

ABSTRACT

Deepfake technology enables the manipulation of audio, images, and videos in a highly realistic manner, making it difficult for the public to distinguish between authentic and fabricated content. The widespread circulation of Deepfake content has the potential to cause serious harm, including damage to personal reputation, violations of privacy and personal data, misinformation, and threats to public trust and social stability. These conditions pose significant difficulties for the Indonesian legal system in providing effective legal protection and ensuring legal certainty. This study aims to analyze the existing legal framework governing the distribution of Deepfake content in Indonesia and to examine the forms of legal liability that may arise from such activities. The research employs a normative legal research method using statutory and literature-based approaches, focusing on relevant laws, legal doctrines, and scholarly opinions related to digital technology and cyber law. The analysis shows that current regulations, including the Law on Electronic Information and Transactions (ITE Law), the Personal Data Protection Law, and provisions of civil law, can be applied to address certain aspects of Deepfake-related violations. However, these regulations have not explicitly regulated Deepfake technology, resulting in legal gaps and interpretative limitations. Therefore, this study highlights the urgent need for the formulation of specific and comprehensive regulations to govern Deepfake technology in order to strengthen legal protection, accountability, and certainty in the digital era.

Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)

INTRODUCTION

The development of artificial intelligence (AI) technology has given birth to the phenomenon of Deepfake, which is audio-visual content that is digitally manipulated to make it look realistic. The spread of Deepfakes on social media poses serious risks to individual privacy, honor, and security, including the potential spread of non-consensual pornographic content and manipulation of public information. Existing regulations such as the ITE Law, the Pornography Law, and the PDP Law have not specifically regulated Deepfake content, so law enforcement officials often face difficulties in enforcing legal accountability. Research shows that this normative ambiguity creates a legal vacuum, which hinders legal protection for victims and legal certainty for law enforcement (Abidin et al., 2023) .

Social media is the main medium for the spread of Deepfake content because of its fast, viral, and difficult to control nature. Digital platforms allow manipulative content to spread massively, causing psychological, social, and economic losses to victims. Several legal studies highlight the lack of obligations of platforms in moderating content and cooperating with law enforcement officials. This causes victims to often have difficulty getting effective restoration of rights. Therefore, an analysis of the role of social media in the context of legal accountability is important (Fauzi et al., 2025) .

The ITE Law is the main legal basis for dealing with cybercrime in Indonesia, but the existing norms are general and have not accommodated the unique characteristics of Deepfake. Law enforcement officials often have to interpret articles that are not explicitly made for Deepfake cases, such as defamation or pornography articles. This kind of approach gives rise to differences in interpretation and legal uncertainty. Legal research shows the need to update norms so that the ITE Law is more responsive to new technological phenomena.

The PDP Law is also relevant in the case of Deepfakes because content manipulation usually involves personal data in the form of the victim's face and voice without consent. Although the PDP Law has provided a data protection framework, there are no specific provisions governing the accountability of Deepfake perpetrators. The absence of this regulation poses legal challenges in upholding the rights of victims. Normative research emphasizes the need for the integration of the PDP Law with cyber regulation to close the legal gap (Aqilah Wiguna & Aisyah Ayu Lestari, 2025) .

Legal liability in the spread of Deepfakes concerns not only the direct perpetrators, but also other parties such as app developers and platform providers. The classic concept of accountability is difficult to apply due to digital anonymity and cross-border deployment. The difficulty of tracking the perpetrators complicates the legal proof process. The research emphasizes the need to adapt the principle of legal accountability to new technologies in order for the law to remain effective (Firdausi et al., 2025) .

From a criminal perspective, the spread of Deepfakes can be qualified as a criminal offense if it meets the elements of intentionality and against the law. However, the ambiguity of the arrangement raises the risk of violating the principle of legal certainty. Law enforcement that only relies on general articles is considered insufficient to protect the interests of victims. Normative juridical analysis needs to explore forms of criminal liability and other legal alternatives. The legal review confirms the urgency of normative reform in dealing with Deepfakes (Syaputra, 2024) .

Civilly, Deepfake victims have the right to claim compensation for the violation of personality rights and immaterial losses. However, proving the connection between the actions of the perpetrator and the victim's loss is often an obstacle. There is no special jurisprudence that handles civil disputes due to Deepfakes, so legal protection for victims is weak. Legal research emphasizes the need for adequate civil mechanisms as a complement to criminal law. This approach is important so that victims can obtain effective restoration of rights (Nugraha Utama et al., 2023) .

The Deepfake phenomenon also raises ethical and social responsibility issues in the use of AI technology. The law not only functions as a tool of repression but also as a means of social control. Adaptive regulation is very important so that the law is able to respond quickly to technological changes. Several studies emphasize the importance of preventive regulation and digital education for the public to reduce the risk of Deepfake abuse (Fauzi et al., 2025) .

Legal research related to Deepfakes in Indonesia is still limited and mostly partial. Many studies only highlight technological or ethical aspects, without comprehensively addressing legal accountability. This opens up opportunities for normative juridical research to identify legal gaps and regulatory weaknesses. The results of the research are expected to make a practical contribution to the development of cyber law in Indonesia (Syaputra, 2024) .

Based on the description above, the spread of Deepfake content on social media raises complex legal issues, especially related to the certainty of regulation and forms of legal accountability. The formulation of the problem in this study is: (1) What is the legal arrangement in Indonesia regarding the spread of Deepfake content on social media. (2) What is the form of legal liability (criminal, civil, or administrative) for the dissemination of Deepfake content. (3) To what extent do the ITE Law, PDP Law, and civil regulations provide protection and remedy for Deepfake victims. (4) What are the normative recommendations to close the legal vacuum in handling Deepfake cases in Indonesia.

This research is expected to provide theoretical and practical benefits in the field of law, particularly in relation to the regulation of Deepfake technology on social media. Theoretically, the study contributes to the development of cyber law by enriching legal analysis on legal responsibility for the dissemination of Deepfake content and clarifying the applicability of existing legal frameworks such as the Electronic Information and Transactions Law, the Personal Data Protection Law, and civil liability provisions. Practically, the findings are expected to serve as a reference for law enforcement agencies, policymakers, and legislators in addressing legal issues arising from Deepfake misuse and in formulating more specific regulations to ensure legal certainty and protection. In addition, this research can increase public awareness regarding the legal risks and consequences of producing and distributing Deepfake content, thereby encouraging more responsible and ethical use of digital technology.

RESEARCH METHOD

This research used normative legal research methods, which is research that views law as a norm or rule written in laws and regulations and legal doctrine. Normative legal research aimed to examine the principles, the systematic nature, and the synchronization of law related to legal accountability for the spread of Deepfake content on social media. This method was chosen because the problems studied related to gaps in norms and legal certainty in Indonesian positive law (Widiarty, 2024).

The type of data used in this study was legal material, which consisted of primary legal material and secondary legal material. Primary legal materials included the Electronic Information and Transaction Law, the Personal Data Protection Law, the Criminal Code, and other relevant laws and regulations. Secondary legal materials consisted of scientific journals, law books, and academic papers that discussed Deepfakes, artificial intelligence, and legal accountability.

This research was carried out through a literature study (library research), so it did not require a field research location. Data collection techniques were carried out by searching, inventorying, and reviewing relevant legal materials through national scientific journals, digital libraries, and official legal sources. The data collected were then analyzed qualitatively and normatively using legal reasoning to assess the adequacy of norms and formulate appropriate legal recommendations. The type of data collected was secondary data, namely data obtained from a review of legal literature, which included laws and regulations, journals, textbooks, doctrines of experts, and other legal sources that could be accessed openly. The data collected were then classified and analyzed based on their relevance to the research issue.

Data analysis was carried out in a normative qualitative manner, namely by interpreting legal norms contained in laws and regulations, legal doctrines, and relevant legal theories to answer the research problems. In this analysis, legal reasoning and content analysis were employed to evaluate the adequacy and consistency of legal norms in dealing with the phenomenon of the spread of Deepfake content. The purpose of the analysis was to formulate normative conclusions and legal recommendations that aligned with the legal framework in Indonesia.

RESULTS AND DISCUSSION

Based on the results of normative legal research through literature studies, it is known that the phenomenon of spreading Deepfake content on social media raises legal problems that have not been comprehensively regulated in the Indonesian legal system. Existing regulations are still general and have not explicitly accommodated the characteristics of Deepfake technology based on artificial intelligence.

This condition causes the application of the law to often be carried out through extensive interpretation of the available norms. As a result, there is potential for legal uncertainty in determining the form of accountability of the perpetrator. Research shows that the legal vacuum is the main obstacle in law enforcement against the spread of Deepfake content. This emphasizes the need for an in-depth juridical analysis of the applicable regulations (Abidin, 2025).

The results of the study also show that social media has a strategic role in accelerating the massive spread of Deepfake content that is difficult to control. The characteristics of social media that are viral and algorithm-based increase the impact of losses experienced by victims. In practice, the legal responsibility of platform providers is still not expressly regulated in Indonesian laws and regulations. This causes the burden of legal liability to be directed more towards individual perpetrators, even though platforms also facilitate the dissemination of content. Legal research confirms that this condition weakens the effectiveness of legal protection for victims. Therefore, a review of the concept of legal accountability in the digital ecosystem is needed (Fauzi et al., 2025).

From the perspective of victim protection, the results of the study show that the spread of Deepfake content has a serious impact on the privacy, dignity, and honor rights of individuals, especially women. Regulations that are not yet specific cause victims to face difficulties in obtaining justice and restoration of rights. Law enforcement that relies on general articles is often not able to provide a deterrent effect for perpetrators. In addition, the absence of an integrated victim protection mechanism exacerbates the social and psychological impact caused. Legal research emphasizes the importance of a victim protection approach in discussing Deepfake's legal liability. This is an important basis for further discussion in the next subchapter (Wiguna & Aisyah, 2025).

Legal Regulations in Indonesia Regarding the Spread of Deepfake Content on Social Media

The development of Artificial Intelligence technology has given birth to the Deepfake phenomenon which has the potential to be abused in various forms of cybercrime. Deepfakes allow for the realistic manipulation of a person's face and voice making it difficult to distinguish from the real content. In the context of Indonesian law, this condition raises serious problems related to the protection of the right to privacy and human dignity. Existing regulations have not specifically regulated Deepfake as a form of criminal act on its own. As a result, law enforcement still relies on the general norms available. This void of norms indicates the need for the renewal of legal arrangements that are more adaptive to technological developments (Afif, 2025) .

The spread of Deepfake content on social media is increasingly massive because it is supported by the ease of access and speed of information distribution. Social media is the main means of spreading manipulative content that can cause great losses to victims. In law enforcement practice, the authorities still have difficulties in qualifying Deepfake acts into existing criminal provisions. This is due to the complex and high-tech Deepfake characters. The unclear legal arrangement has an impact on the weak deterrent effect for perpetrators. This condition shows that the regulation of cyber criminal law in Indonesia is still not optimal (Prayoga & Tuasikal, 2025) .

One of the most troubling forms of Deepfake abuse is Deepfake pornography, including those targeting children. This crime has a serious impact on the victim, both psychologically and socially. The current criminal law regulation in Indonesia has not explicitly regulated Deepfake pornography as a special offense. Law enforcement still relies on general provisions in the ITE Law and regulations related to pornography. However, this approach is considered not to be able to provide maximum protection for victims. Therefore, a more specific formulation of norms is needed to answer the development of this mode of crime (Fauzi et al., 2025)

In addition to the criminal aspect, the spread of Deepfakes is also closely related to the protection of personal data. Face and voice are biometric data that should be protected from misuse. The use of such data without the consent of the data subject has the potential to violate the principle of personal data protection. However, in practice, legal protection of biometric data still faces implementation challenges. Existing regulations do not yet explicitly regulate the use of biometric data in the context of Deepfake. This shows the need to harmonize personal data protection regulations with the development of AI technology (Firdausi et al., 2025) .

The cases of Deepfakes that drag public figures show that these crimes not only have an impact on individuals, but also on social stability and public trust. The spread of Deepfakes can be used as a tool for manipulation of opinion and disinformation. In this context, Indonesia is still lagging behind other countries that have begun to formulate special regulations related to AI. The absence of specific regulations causes legal responses to be reactive and partial. This strengthens the urgency of establishing comprehensive national regulations. Comparison with international regulations shows the importance of national law reform (Tarigan & Rumiartha, 2025) .

From a victim protection perspective, the spread of Deepfake content often causes irreparable losses. Victims not only suffer reputational loss, but also prolonged psychological trauma. The Indonesian legal system has not provided adequate mechanisms for the protection and recovery of victims in the case of Deepfake. Legal handling still focuses on criminalizing perpetrators without paying attention to the rehabilitation aspect of the victim. This condition shows the need for a more victim-oriented legal approach. Victim protection should be an integral part of the Deepfake legal setup (Yudha et al., 2025) .

Based on this description, it can be concluded that the legal arrangements in Indonesia related to the spread of Deepfake content are still fragmentary and have not been integrated. Dependence on general norms leads to weak legal certainty and law enforcement effectiveness. This condition has the potential to increase the risk of misuse of AI technology in the digital space. Therefore, regulatory updates are needed that specifically regulate (Latifatunnisa & Yudha, 2025) Deepfakes as a form of cybercrime. The update must accommodate criminal aspects, personal data protection, and victim protection. The urgency of this legal reform is in line with the needs of society in the current digital era.

Legal Accountability for the Spread of Deepfake Content

Legal accountability for the spread of Deepfake content is basically rooted in the construction of criminal law in countering cybercrime in Indonesia. The development of Deepfake technology has created a new form of crime that is manipulative, difficult to detect, and has the potential to cause serious harm to individuals and society. In the context of criminal law, these acts can be qualified as cybercrimes because they are carried out through electronic systems by utilizing the sophistication of digital technology. National criminal law is required to be able to accommodate these developments through the interpretation and application of adaptive norms. Therefore, the criminal liability of Deepfake perpetrators must be placed within the framework of a criminal law policy that is responsive to the dynamics of information technology (Alif et al., 2025) .

The form of criminal responsibility for Deepfake perpetrators is closely related to the fulfillment of the elements of error in criminal law. The spread of Deepfake content is generally done intentionally, both for the purpose of fraud, defamation, and sexual exploitation. This element of intentionality is the main basis for assessing criminal liability, especially when the perpetrator knows and wants the consequences of his actions. In practice, proving the mistakes of Deepfake perpetrators can be done through digital footprints, the content creation process, and the distribution of the content on social media. Thus, criminal liability of Deepfake perpetrators can be enforced as long as the elements of unlawful acts and mistakes are met (Sonia et al., 2025) .

In addition to general criminal liability, the spread of Deepfake content can also give rise to specific criminal liability, especially when it comes to pornography. The misuse of Deepfake technology to create pornographic content, particularly those involving a person's face without consent, is a serious violation of human dignity and rights. In this context, the perpetrator is not only responsible for the act of digital manipulation, but also for the psychological and social impact experienced by the victim. Law enforcement against the crime of Deepfake pornography requires a firm approach because it includes crimes with a high level of victimization. Therefore, the criminal responsibility of the perpetrator must be enforced to the maximum to provide a deterrent effect (Darmawan et al., 2025) .

Legal accountability for the spread of Deepfakes can also be seen from the perspective of protecting the public interest. The spread of Deepfake content has the potential to mislead the public, undermine public trust, and create massive disinformation. In such conditions, the state has an obligation to ensure that the law is able to provide effective protection for the wider community. Perpetrators of the spread of Deepfakes can be held criminally responsible because their actions threaten public order and social interests. Thus, legal liability is not only oriented to individual victims, but also to the protection of the public interest collectively (Prayoga & Tuasikal, 2025) .

From the perspective of positive Indonesian law, the liability of Deepfake perpetrators can be linked to criminal provisions that regulate content that violates morality and misuse of technology. Although there are no specific regulations regarding Deepfakes, the existing norms can still be applied through systematic and extensive interpretation. This shows that Indonesia's positive law still provides space to ensnare perpetrators of abuse of artificial intelligence technology. Criminal liability of Deepfake perpetrators in pornographic content, for example, can be imposed under provisions that govern decency and victim protection. Thus, positive law can still function as an instrument of social control against Deepfake crimes

In addition to the main perpetrators, a form of legal accountability can also be directed to other parties who play a role in the spread of Deepfake content. Digital platforms and social media have a significant role in the distribution of such content to the public. When platforms are negligent in supervising and controlling content, there is potential for indirect legal liability. This confirms that tackling Deepfake crime is not only focused on individual perpetrators, but also on the digital ecosystem as a whole. Therefore, the regulation regarding the platform's liability is an important part of the Deepfake legal liability system (Chairani et al., 2022) .

Legal accountability for the spread of Deepfakes also relates to victim protection, particularly in the case of pornography. Deepfake victims often experience multiple losses, ranging from psychological, social, to reputational losses. In this context, the law serves not only to punish the perpetrator, but also to restore the rights of the victim. Legal protection for Deepfake victims reflects an increasingly relevant restorative justice approach in modern criminal law. Thus, the legal accountability of Deepfake perpetrators must also be directed to fulfilling the victim's right to justice and restoration.

The absence of specific regulations regarding artificial intelligence and Deepfakes shows a legal vacuum that has an impact on law enforcement. This void poses challenges in determining the limits of the responsibility of the perpetrator and related parties. However, a comparison with international regulations, such as the EU AI Act, shows that strengthening national regulations is an urgent step. Under current conditions, legal accountability for the spread of Deepfakes can still be enforced through existing legal instruments, while encouraging the establishment of specific regulations. Therefore, strengthening the legal framework is key to ensuring the effectiveness of legal accountability in the Artificial Intelligence era (Tarigan & Rumiartha, 2025) .

The ITE Law, PDP Law, and Civil Regulations Provide Protection and Remedy for Deepfake Victims

The development of Deepfake technology has given rise to new forms of law violations that have a direct impact on the rights and interests of individuals, especially victims whose faces, voices, or identities are manipulated without consent. The spread of Deepfake content on social media not only causes reputational damage, but also serious psychological and social damage. In this context, victims are in a vulnerable position because of the difficulty of controlling the circulation of digital content in cyberspace. Therefore, the presence of legal instruments that are able to provide protection and remedies is an urgent need. The national legal system is required to be able to provide a comprehensive response to these artificial intelligence-based crimes (Jiwangga & Budyatmodjo, 2023)

Legal protection for Deepfake victims in Indonesia does not only come from one legal regime, but is spread across several laws and regulations. The Electronic Information and Transaction Law, the Personal Data Protection Law, and the provisions of civil law have complementary roles in providing protection and restoration of victims' rights. Each of these instruments has different protection characteristics, either through criminal sanctions, administrative sanctions, or compensation mechanisms. This multidimensional approach shows that the protection of Deepfake victims cannot be done partially. On the contrary, it requires a complete understanding of the entire applicable legal system.

In a normative legal perspective, protection and remedies for Deepfake victims must be analyzed based on the suitability of legal norms with the characteristics of the act and the impact caused. Although there is no specific regulation that explicitly regulates Deepfakes, existing legal norms can still be used through systematic and extensive interpretation. This confirms that Indonesia's positive law still has adaptability to the development of digital technology. Thus, it is important to examine how the ITE Law, the PDP Law, and civil regulations provide protection and remedies for Deepfake victims in a concrete way. The next discussion will describe the role of each of these legal instruments in more detail.

Protection and Remedies for Deepfake Victims in the ITE Law

The Electronic Information and Transaction Law (ITE Law) is the main legal instrument in dealing with harmful legal acts through electronic systems, including the spread of harmful content such as Deepfakes. The ITE Law provides a legal basis for taking action against acts carried out through digital media that violate the law and harm other parties, such as defamation and the dissemination of misleading information. In the context of Deepfakes that can damage an individual's reputation, the norms of the ITE Law allow victims to sue the perpetrator through relevant articles regarding electronic information and electronic transactions. Research shows that the implementation of the ITE Law in the context of social media often involves defamation norms, but the interpretation of these regulations often faces a dilemma between freedom of expression and the protection of the victim's reputation (Zahsy, 2025) .

Article 27 paragraph (3) jo. Article 45 paragraph (3) of the ITE Law explains the prohibition of disseminating information intended to insult or defame a person through electronic systems. In legal practice, this provision has been implemented to crack down on perpetrators who disseminate digital content that harms other parties. In normative juridical research, the ITE Law was found to be a relevant legal umbrella to address Deepfake acts that impact the good name and honor of individuals, although it was not specifically designed for Deepfake technology. The criminal law contained in the ITE Law serves to provide a criminal remedy for victims through the imposition of sanctions against the perpetrator. However, a consistent interpretation is still needed so that this norm can effectively protect victims in the digital information era.

In addition to criminal sanctions, the ITE Law also provides space for victims to demand restoration of rights (remedy) through civil lawsuits against perpetrators who disseminate harmful content. In several judges' decisions, the norms of the ITE Law are combined with the principle of civil liability to claim compensation for immaterial and reputational losses suffered by the victim. This protection is relevant when Deepfake content causes significant social and psychological impacts for victims. The juridical study underlines the need for synergy between criminal and civil enforcement in the ITE Law so that victims have an adequate recovery path. This shows that the ITE Law is not only a repressive tool but also a remedial instrument for victim recovery.

The biggest obstacle in the effectiveness of the ITE Law is the lack of clarity of the criminal element when faced with new technology violation modes such as Deepfake. Because Deepfakes are not explicitly mentioned in the text of the law, law enforcement officials often have to interpret the general norms for cybercrime. This can result in differences in judicial practices between regions and legal uncertainty, which ultimately impacts victim protection. Normative research emphasizes the importance of contextual interpretations that take into account the characteristics of technology so that the ITE Law can be more responsive to this kind of case.

To strengthen protections for Deepfake victims, some researchers have suggested interpretive guidance or normative amendments to the ITE Law to explicitly include digital manipulation technology. Thus, weaknesses in current norms can be overcome and provide clearer legal certainty for victims and law enforcement. These similar recommendations show that the ITE Law can still be developed to respond to new challenges of digital technology, including efforts to provide stronger remedies for victims of Deepfakes in cyberspace.

Protection and Remedies for Deepfake Victims in the PDP Law

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is an important step in providing protection of individual privacy rights in an increasingly complex digital era. The summary of the PDP Law emphasizes that personal data, including facial and voice images that could potentially be used in the creation of Deepfakes, is a right that must be legally protected. In the context of Deepfakes, this arrangement is relevant because these technologies often take advantage of personal data without the consent of the data subject. The PDP Law provides a framework of legal certainty on how data should be processed, stored, and disseminated with explicit subjective consent (Abdullah et al., 2025) .

The protection of personal data in the PDP Law includes the right of data subjects to obtain information, consent, and the right to withdraw and delete data from electronic systems. In practice, these rights can be an important remedy for Deepfake victims who want to remove content that misuses their personal data. With this kind of right, victims can submit a request for the deletion of data or harmful content based on the PDP Law. In addition, the provisions of administrative and criminal sanctions contained in the PDP Law open legal channels for violations of privacy rights due to Deepfakes.

The legal literature states that the PDP Law is a regulatory answer to the challenges of privacy protection in the era of big data and digital transformation, including the threat of technology abuse such as Deepfake. Research shows that although the PDP Law has provided a clearer legal framework, its implementation faces several challenges such as the capacity of supervisory institutions and public literacy of their rights. Nevertheless, the existence of this legislature emphasizes the state's commitment to provide legal protection for citizens' personal data, including those used in Deepfake content.

The PDP Law also introduces the concept of the principle of minimization and explicit consent, which means that any use of personal data must have a clear legal basis. This provision is important to restrain the spread of harmful Deepfake content because personal data such as face or voice should not be processed without valid consent. The position of this principle in the PDP Law strengthens the victim protection agenda by giving them the authority to determine how their data is used. Thus, the PDP Law adds a new dimension of victim protection that was previously not available in the ITE Law.

Although the PDP Law provides many rights and remedies, there are still obstacles in the effective implementation of data subject rights, such as the lack of public understanding of their rights and low awareness of digital service providers of their legal obligations. Research shows that expanding legal education campaigns and increasing the capacity of supervisory agencies are important steps in ensuring that the PDP Law is not only on paper but can provide a real remedy to victims of Deepfakes and other personal data breaches.

Protection and Remedies for Deepfake Victims through Civil Law

In addition to protection through the ITE Law and the PDP Law, civil law also provides a remedy for victims of the spread of Deepfake content. The concept of unlawful acts (PMH) in the Civil Code (Article 1365) can be applied when the spread of Deepfake content is materially or immaterially harmful. Civil law focuses on the restoration of rights and the provision of compensation to victims, which complements the repressive nature of criminal law. The application of this civil principle provides space for victims to demand financial accountability from the perpetrator (Squirrelly & Danyathi , 2025) .

In an unlawful act, the dissemination of Deepfake content without consent can be seen as a violation of an individual's right to privacy and honor. Juridical studies show that the civil sector can provide a remedy in the form of compensation or restitution for losses suffered by victims due to such practices. In addition, civil law provides preventive protection through the obligation to restore the victim's reputation, for example through a request for the removal of content or an open apology. This legal instrument complements the protection of victims outside the criminal and administrative realms.

Civil law also recognizes the concept of default and third-party liability if the spread of Deepfakes involves a digital service contract or agreement. When a digital service provider fails to maintain the privacy and security of user data, they may be subject to an indemnification obligation based on the principle of default or liability in contract. This is relevant when digital services provide content storage or distribution features that contain personal data without adequate safeguards. Thus, civil law expands the spectrum of remedies for Deepfake victims.

The implementation of civil law in practice requires an analysis of the causal relationship between the actions of the perpetrator and the losses suffered by the victim, including reputational, psychological, and financial losses. Normative juridical research indicates that proving such relationships remains possible with the support of strong digital evidence, such as metadata traces and digital forensic expert evidence. This shows that although Deepfakes are a digital phenomenon, classical civil law principles are still relevant and adaptive to technological challenges.

Thus, legal protection through civil law provides an important dimension of remedy for Deepfake victims who may not be adequately protected by criminal or administrative law alone. The civil approach can fill the gap in financial remedies and restorative justice that are not yet available in the ITE Law or the PDP Law. This shows that the three criminal, administrative, and civil legal instruments must work synergistically to provide comprehensive protection and remedies for victims of the spread of Deepfake content in Indonesia.

Normative Recommendations to Close the Legal Vacuum in Handling Deepfake Cases in Indonesia

First, there needs to be a special legal norm that explicitly regulates Deepfakes in Indonesian laws and regulations. The current legal vacuum causes law enforcement to have to rely on broad interpretations of general norms so that it is prone to legal uncertainty. Research shows that although the ITE Law and the PDP Law provide legal space to crack down on Deepfake-related offenses, both have not been specific enough to address the characteristics of AI technology in the context of digital content manipulation.

Therefore, the formulation of the juridical definition of Deepfake and its regulation can specifically provide legal certainty for the authorities, victims, and the public. Normatively, this approach should include a proportionate classification of impact levels and sanctions for the type of Deepfake offense. Without specific regulation, the potential misuse of this technology will continue to cause legal problems in the future (Tarigan & Rumiartha, 2025) .

Second, the application of the principle of strict liability in the context of Deepfakes needs to be considered in line with the principle of personal data protection. This principle allows the party that produces or disseminates Deepfake content to be held accountable without having to prove elements of conventional wrongdoing. Normative research emphasizes that the PDP Law provides a legal basis for the protection of personal data, but there is still a void related to liability when AI generates Deepfake content that is detrimental to privacy. By applying the principle of absolute accountability to the developer or owner of AI technology, the law can more effectively protect individuals from the misuse of their personal data. This approach also encourages caution in the development and use of potentially misused artificial intelligence technologies. Therefore, a no-fault accountability mechanism must be integrated in the draft new regulation (Putri et al., 2025) .

Third, there needs to be a stricter regulation regarding the obligations of digital platforms in moderating and removing illegal Deepfake content . Social media platforms are often a medium for the spread of Deepfake content, but current Indonesian regulations do not sufficiently regulate the platform's proactive obligations in controlling such content. Legal studies highlight that the liability of makeshift platforms can exacerbate the impact for victims if content is allowed to spread without prompt intervention.

Strong regulations should govern risk-based content moderation obligations, algorithm transparency standards, and clear response times for the removal of harmful content. Through explicit norms, digital platforms will be encouraged to play an active role in protecting Deepfake victims. This is in line with modern legal policy principles that place greater responsibility on technology providers in maintaining a secure digital space (Quratuainniza & Nurkhaerani, 2025) .

Fourth, national criminal law reform needs to consider the addition of special offenses related to Deepfakes in the Criminal Code or its derivative regulations. The current loophole in the provisions of the Criminal Code makes law enforcement officials have to rely on common norms such as defamation or pornography, which do not fully reflect the characteristics of Deepfake's actions. Research shows that without clear deterrents, the prosecution process is often ineffective and does not create a deterrent effect.

Therefore, formulating special criminal provisions that regulate the creation and dissemination of Deepfakes as a criminal act in itself is a significant normative step. This norm can include elements of acts, subjects, and the qualification of sanctions that are adjusted to the level of social impact. Thus, the Criminal Code can be more responsive to the dynamics of digital crimes based on artificial intelligence technology (Syaputra , 2024) .

Fifth, strengthening the mechanism for personal data protection and access to administrative remedies under the PDP Law needs to be realized operationally through technical guidelines and effective enforcement instruments. Although the PDP Law provides for explicit consent and data subject rights for data deletion, its practical implementation still faces obstacles such as low public legal literacy and limited supervisory capacity.

This normative recommendation involves the preparation of technical guidelines for electronic system operators and supervisory agencies to carry out the obligation to delete data related to Deepfakes at the request of victims. In addition, the PDP Law needs to expand administrative sanctions that create strong disincentives for violators of data processing without consent. This will strengthen the position of the rights of the data subject and provide an effective administrative remedy before or in conjunction with criminal action (Maximillian Laza & Karo Karo, 2023)

Sixth, the establishment of a special civil litigation mechanism for Deepfake victims in the civil realm is needed to accommodate claims for immaterial compensation and moral restitution. In civil law, unlawful acts (Article 1365 of the Civil Code) can be the basis for a lawsuit, but its application is often limited to material losses and relational cleanliness between the action and its consequences.

Normative recommendations include the development of guidelines for electronic evidence and the use of legally recognized digital evidence as well as the role of information technology experts in civil proceedings. This would give victims stronger legal access to claim compensation for the widespread impact of Deepfakes, such as reputational damage or psychological trauma. Increasing the capacity of lawyers and courts in handling digital evidence as well as the interpretation of modern civil norms is also part of this recommendation (Tavadjio , 2025) .

Seventh, there is a need for a preventive legal approach through education and national digital literacy programs to reduce the risk of the spread and impact of Deepfakes. This normative strategy emphasizes that legal protection is not only repressive but also preventive through increasing public awareness of the dangers and ways of identifying Deepfake content. The government, in collaboration with educational institutions and technology service providers, needs to develop a digital literacy curriculum that contains components of digital ethics, privacy rights, and the legal consequences of technology abuse. This is an important dimension of modern legal policy oriented towards social control and prevention of harm before it occurs (Chrisjanto & Luhukay, 2025) .

Eighth, strengthening international cooperation in handling Deepfake cases is also an important normative recommendation. Because the spread of Deepfake content is often cross-border, international legal cooperation and information exchange can strengthen the ability of Indonesian law enforcement to track foreign actors and take effective legal action. These recommendations include the harmonization of international rules on AI and data privacy policies, as well as the use of cooperation instruments such as Mutual Legal Assistance (MLA) in cyber law enforcement. This approach will give a strategic dimension to the handling of Deepfakes involving international jurisdictions, so that Indonesian victims do not lose legal opportunities when the perpetrators are abroad. (Fauzyah et al., 2024) .

Ninth, there is a need for periodic evaluation of the policy and effectiveness of Deepfake regulation through independent legal research institutes and legislation committees that can provide recommendations for improvement. This evaluation should include the impact of criminal, administrative, and civil remedy mechanisms, including challenges to electronic evidence and victims' access to remediation. The development of transparent evaluation indicators will encourage the dynamics of improving legal regulations in accordance with technological developments. In addition, the involvement of various stakeholders, including academics, legal practitioners, and civil society in the evaluation, is important to ensure that social, technological, and ethical aspects are addressed comprehensively (Latifatunnisa & Yudha, 2025) .

The overall normative recommendations above show that the handling of Deepfake laws in Indonesia requires a multifaceted approach, including the update of criminal law norms, personal data protection, civil regulations, platform obligations, and international literacy and cooperation. The inadequacy of existing norms shows that national laws are still in the stage of adapting to the challenges of digital technology. By implementing the above normative measures, it is hoped that Indonesia's positive law can close the legal vacuum and provide certainty and optimal protection for Deepfake victims. This normative approach also encourages the evolution of positive laws that are proactive in dealing with future technologies, not just responsive to cases that have already occurred.

CONCLUSION

This study concludes that the rise of AI-based Deepfake technology poses serious legal challenges for Indonesia's legal system, as its misuse in defamation, privacy violations, pornography, and misinformation reveals inadequacies in positive law, including the Electronic Information and Transactions Law, Personal Data Protection Law, and civil provisions, which lack explicit norms for Deepfake's technical traits, leading to evidentiary hurdles, unclear accountability, and suboptimal victim protection across criminal, civil, and administrative domains. A legal vacuum persists, underscoring the urgent need for multidimensional reforms like specific Deepfake regulations, enhanced platform duties, stronger data protections, improved civil remedies, digital literacy initiatives, and international collaboration to foster legal certainty and justice amid digital transformation. For future research, scholars could empirically investigate law enforcement practices in Deepfake cases through case studies or surveys to validate these normative gaps and assess reform implementation.

REFERENCES

Abdullah, C., Durand, N., & Moonti, R. M. (2025). Digital Transformation and the Right to Privacy: A Critical Review of the Implementation of the 2022 Personal Data Protection Law (PDP) in the Big Data Era. Amendment: Indonesian Journal of Defense, Political and Legal Sciences, 2(3), 233–241. Https://Doi.Org/10.62383/Amandemen.V2i3.1073

Abidin, M. I., Adha, A. F., Yuniyanti, S. S., & Chairunnisa, C. (2023). Legal Review Of Liability From Deepfake Artificial Intelligence That Contains Pornography. MIMBAR : Journal of Social and Development. Https://Doi.Org/10.29313/Mimbar.V39i2.2965

Afif, M. (2025). Deepfake Pornography Crime in Indonesia: A Juridical Analysis of the Norm Void in the Criminal Code and the ITE Law. Multidisciplinary Scientific Journal, 3(2), 27–35. Https://Doi.Org/10.62017/Merdeka

Alif, S. S. Al, Rindiani, A., & Marhayati, C. (2025). Construction of Criminal Law in Countering Cybercrime Based on Deepfake Technology in Indonesia. Legal Standing: Journal of Legal Sciences, 9(5), 1169–1183. Https://Doi.Org/10.24269/Ls.V9i5.12406

Aqilah Wiguna, A., & Aisyah Ayu Lestari, P. (2025). Legal Protection for Women Victims of Deepfake Pornography in Indonesia. Journal of Legal and Public Policy Studies, 3(1). Https://Doi.Org/10.24843/JMHU.2025.V14.I03

Chairani, M. A., Pradhana, A. P., & Purnama, T. Y. (2022). The Urgency Of Developing Law As A Legal Basis For The Implementation Of Artificial Intelligence In Indonesia. Law And Justice, 7(1), 35–45. Https://Doi.Org/10.23917/Laj.V7i1.760

Chrisjanto, E., & Luhukay, R. S. (2025). Legal Protection Of Artificial Intelligence (Ai) In Indonesia). Journal of Legal Reasoning, 7(2), 224–248.

Darmawan, Muh. T., Junaidi, A., & Khaerudin, A. (2025). Law Enforcement Against Deepfake Abuse in Child Pornography in the Era of Artificial Intelligence in Indonesia. Serambi Hukum Journal, 18(1).

Fauzi, S. S., Rusmana, I. P. E., Darma, I. M. W., & Wulandari, N. G. A. A. M. T. (2025). Criminal sanctions are regulated against perpetrators of pornographic content creators using deepfake technology in Indonesia. Al-Zayn: Journal of Social and Legal Sciences, 3(6), 9612–9623. Https://Doi.Org/10.61104/Alz.V3i5.2661

Fauzyah, R. N., Hafidati, P., & Sunarya, S. (2024). Legal protection for victims of the crime of making fake pornographic videos (deepfake porn) based on artificial intelligence (AI) in Indonesia. In Lex Veritatis (Vol. 3, Issue 3). Https://Www.Dradio.Id/2024/02/16/Pengguna-Ai-

Firdausi, A., Nur Abadi, F., Yogi Dwi Amelia, T., & Duta Bangsa Surakarta, U. (2025). Ethical and legal review of personal data protection amid the rise of deepfake content on social media. Journal of Law and Citizenship, 12(5). Https://Doi.Org/10.3783/Causa.V2i9.2461

Jiwangga, V. A., & Budyatmodjo, W. (2023). The application of defamation provisions on social media in the judge's decision. Journal of Criminal Law and Crime Management, 12(1).

Latifatunnisa, R., & Yudha, M. W. (2025). The Urgency of Regulatory Reform in Tackling the Misuse of Artificial Intelligence and Deepfake Technology in Indonesia: A Perspective on Privacy Rights Protection. Journal of Law and Citizenship, 11(1).

Maximillian Laza, J., & Karo, R. (2023). Legal Protection of Artificial Intelligence in the Aspect of Abuse of Deepfake Technology from the Perspective of the PDP Law and GDPR. Lex Prospicit, 2. Https://Doi.Org/10.19166/Lp.V1i2.7368

Nugraha Utama, A., Tusta Kesuma, P., & Hidayat, R. M. (2023). Legal analysis of efforts to prevent deepfake porn cases and public awareness education in the digital environment. Journal of Tambusai Education, 7(3), 26179–26187.

Prayoga, H., & Tuasikal, H. (2025). The Spread of Deepfake Content as a Criminal Offense: A Critical Analysis of Law Enforcement and Public Protection in Indonesia. Abdurrauf Law And Sharia, 2(1), 22–38. Https://Doi.Org/10.70742/Arlash.V2i1.194

Putri, K. A. R., Saputro, H. D., & Amanita, A. (2025). Legal Liability for the Use of Artificial Intelligence for Deepfakes under the Personal Data Protection Law. Legal Sciences: Journal of Law Students, 2(2). Https://Doi.Org/10.29303/Jkh.V5i2.49

Quratuainniza, H. S., & Nurkhaerani, E. (2025). Artificial Intelligence Regulation to Address the Abuse of Deepfakes in Indonesia. ALLAH: Journal of Politics, Social, Law and Humanities, 4(1).

Sonia, Sudarti, E., & Erwin. (2025). Artificial Intelligence (AI)-Based Deepfake Porn Crime in Indonesian Law. PAMPAS: Journal Of Criminal Law, 6(3), 342–354. Http://Journals.Usm.Ac.Id/Index.Php/Julr/Article/View/8995/0.

Syaputra, R. (2024). The Urgency of Regulating Legal Protection for Deepfake Victims through Artificial Intelligence (AI) from the Perspective of Indonesian Criminal Law. Https://Doi.Org/10.55606/Khatulistiwa.V3i3

Tarigan, E. P., & Rumiartha, I. N. P. B. (2025). AI Legal Vacuum in Indonesia: The Deepfake Case Against Sri Mulyani and the Comparison of the EU AI ACT. Journal of Academic Media (JMA), 3(11). Https://Doi.Org/10.62281

Tavadjio, S. N. (2025). Legal implications of deepfakes: civil damages for falsification of faces and voices. Al-Zayn: Journal of Social and Legal Sciences, 3(4). Https://Doi.Org/10.61104/Alz.V3i4.1995

Widiarty, W. S. (2024). Textbook of Legal Research Methods (M. Tajuddin, Ed.; 1st ed.). Published by Global Media.

Yudha, M., Purwanda, S., Amir, A., Kairuddin, K., Syahril, Muh. A. F., Samiruddin, S., & Latif, A. (2025). Legal protection for victims of deepfake use in pornography crimes. Indonesian Journal Of Law And Shariah, 2(1), 24–37. Https://Ejournal.Unu.Ac.Id/Index.Php/Ijls

Zahsy, V. Al. (2025). The Crime of Defamation on Social Media: Between Freedom of Expression and ITE Legal Restrictions. Journal of Legality, 3(2), 68–79. Https://Doi.Org/10.58819/Jle.V3i2.172