

AI-Generated Deepfakes and Civil Liability Under Article 1365 of the Civil Code and Human Rights Protection

Yuliasara Isnaeni¹⁾ & Ricky Hendra Gutama²⁾

¹⁾Universitas Jayabaya, Jakarta, Indonesia, E-mail: yuliasara.isnaeni@jayabaya.ac.id

²⁾Universitas Jayabaya, Jakarta, Indonesia, E-mail: rickyhendrag@gmail.com

Abstract. *The rapid advancement of Artificial Intelligence (AI) has facilitated the emergence of deepfake technology, which enables the creation of highly realistic manipulated audio, image, and video content. While deepfakes offer various beneficial applications, their misuse poses significant legal challenges, particularly regarding civil liability and the protection of fundamental rights. This study aims to analyze whether the creation and dissemination of AI-generated deepfake content fulfill the elements of an unlawful act under Article 1365 of the Indonesian Civil Code and to examine the evidentiary mechanisms applicable in civil litigation involving deepfakes. This research employs normative legal research using statutory, conceptual, and case approaches. The findings indicate that the unauthorized creation and distribution of deepfake content may satisfy all elements of an unlawful act, namely the existence of an act, unlawfulness, fault, damage, and a causal relationship between the act and the resulting harm. The study concludes that Article 1365 of the Indonesian Civil Code can be applied progressively to deepfake cases, although more comprehensive regulations are necessary to ensure effective legal protection and accountability in the era of artificial intelligence.*

Keywords: *Artificial Intelligence; Civil Liability; Deepfake; Human Rights Protection; Unlawful Act.*

1. Introduction

The development of Artificial Intelligence (AI) technology has brought major changes to human life because it is able to speed up work, increase efficiency, and open up opportunities for innovation in various sectors (Mulya, 2018; Rajawali, 2019; Hardiansyah, 2019). However, at the same time, these technological advances have also given rise to new and increasingly complex legal issues, one of which is the misuse of deepfake technology. Deepfakes are a form of digital manipulation that utilizes AI to alter or manipulate a person's face, voice, expressions, and body movements to appear real and authentic (Putri et al., 2025; Najah, 2026). Technically, deepfake content can be created with such a high degree of similarity that it is difficult for the general

public to distinguish between genuine and fabricated content. This makes deepfakes a dangerous tool because they can be used to spread false information, commit fraud, defame, damage reputations, humiliate victims, and even invade privacy and dignity. In many cases, victims are not involved in the creation or distribution of the content, but their identities, images, and voices are used without their consent. This phenomenon demonstrates that the development of AI not only brings benefits but also poses a real threat to the legal protection of individuals in the digital space (Tavadjio, 2025; Gultom, 2026; Putra, 2026).

In Indonesia, deepfake misuse is not specifically regulated under a single provision that expressly addresses deepfakes or AI, creating challenges for law enforcement in applying existing legal rules. Nevertheless, Article 1365 of the Civil Code may serve as a legal basis when the creation or distribution of deepfakes fulfills the elements of an unlawful act, fault, loss, and causation. The Electronic Information and Transactions Law (*Undang Undang Informasi dan Transaksi Elektronik/ITE Law*) and Personal Data Protection Law are also relevant, particularly concerning the unauthorized distribution of electronic content and misuse of personal data, including facial images and voices (Annisa, 2024; Respati et al., 2024; Yanuafriza & Eluan, 2025). Therefore, Indonesian law still provides legal instruments to assess and address deepfake-related misconduct and establish accountability (Widjaja, 2020; Marwan, 2020; Tavadjio, 2025).

From a human rights perspective, deepfakes cannot be viewed simply as a technical or digital ethical issue, but rather as a violation of the fundamental rights inherent in every person. The use of a person's face, voice, and identity without consent directly affects the rights to privacy, honor, dignity, and security. The right to privacy provides protection so that an individual can control their personal information and representation in public and digital spaces (Putra, 2026). The right to honor and dignity affirms that a person's identity may not be misused for purposes that demean, mislead, or embarrass. Meanwhile, the right to security demands that individuals not be victims of intimidation, harassment, manipulation, or digital attacks that cause fear and psychological distress. Therefore, deepfakes constitute a human rights violation because their impact is not only socially detrimental but also undermines the victim's personal integrity as a legal subject and as a dignified human being.

This situation demonstrates the urgent need to examine whether the creation and distribution of deepfakes meet the elements of an unlawful act under Article 1365 of the Civil Code, and the mechanisms for proving this in civil proceedings (Bakry, 2005; Kusumadi, 2015; BP Lawyers, 2023; Ardiyani, 2024; Maharani, & Mtm, 2025). This discussion is important because in deepfake cases, proof is often a major obstacle. Digital content can be re-manipulated, distributed anonymously, and appears highly convincing, requiring electronic evidence, metadata, digital footprints, and testimony from digital forensic experts to confirm the authenticity of the content and the link between the perpetrator and the victim's losses. Therefore, protecting deepfake victims cannot be viewed solely from the perspective of technological developments, but must be understood as a matter of civil liability and human

rights violations that require serious, comprehensive, and adaptive legal action (Utama, 2022; Wiguna & Aisyah, 2025; Oktavianti et al., 2025; Kurniawan, 2026).

The conceptual framework of this research is built upon the interrelationship among three key concepts: Artificial Intelligence (AI) and deepfake technology, unlawful acts, and human rights protection (Kusumadi, 2015; Nugraha et al., 2025; Gultom, 2026). These concepts provide the analytical foundation for assessing whether the use of AI in creating and disseminating deepfake content can generate civil liability and infringe fundamental rights protected by law. Within this framework, deepfakes are positioned as a legal phenomenon that exists at the intersection of technological innovation, civil law, and human rights protection (Asshiddiqie, 2010; Putri et al., 2025; Silalahi & Dachi, 2026).

From a civil law perspective, Article 1365 of the Indonesian Civil Code establishes the basis for determining liability for unlawful acts through five elements: an act, unlawfulness, fault, damage, and causation. The creation and dissemination of AI-generated deepfakes may fulfill these elements when they cause material or immaterial losses. Deepfake technology enables realistic manipulation of faces, voices, expressions, and identities, making fabricated content appear authentic (Chairani et al., 2024; Haida & Nuriyatman, 2024). Although it has legitimate applications, misuse without consent can cause reputational, financial, psychological, and social harm, making deepfakes potential instruments of unlawful conduct.

The framework also incorporates a human rights perspective, emphasizing the protection of privacy, honor, dignity, and personal data. Deepfakes frequently involve unauthorized use of personal information and identity, potentially violating these rights and causing significant harm to victims (Nugraha et al., 2025; Wiguna & Aisyah, 2025). Accordingly, this research examines deepfakes through two complementary parameters: civil liability under Article 1365 of the Civil Code and the protection of fundamental human rights (Ardiyani, 2024; Putra, 2026; Gultom, 2026). Through this integrated approach, the study seeks to determine whether AI-generated deepfake content can give rise to legal responsibility and how such responsibility may be established through evidentiary mechanisms in civil proceedings (Asshiddiqie, 2010; Eka & Ratna, 2025).

Although previous studies have examined deepfake misuse from the perspectives of unlawful acts, personal data protection, and human rights, limited attention has been given to the application of Article 1365 of the Indonesian Civil Code in establishing civil liability and proving fault, loss, and causation in deepfake-related disputes (Maharani & Mtvm, 2025). Existing discussions tend to focus on the technological and normative risks of deepfakes, while the practical evidentiary challenges in civil proceedings remain insufficiently explored. Therefore, this study seeks to address this gap by analyzing the legal elements of unlawful acts and the evidentiary mechanisms applicable to deepfake-related civil cases in Indonesia.

Based on the problem formulation, this study aims to analyze whether the use of Artificial Intelligence (AI) in the creation and distribution of deepfake content fulfills the elements of an Unlawful Act as regulated in Article 1365 of the Civil Code, and to explain the evidentiary mechanisms that can be used in civil cases related to deepfake, especially regarding the elements of fault, loss, and causal relationship. Theoretically, this study is expected to enrich the development of civil law studies regarding the application of the unlawful acts concept in the context of digital technology and artificial intelligence, while also contributing to the development of civil liability theory in the AI era. Practically, the results of this study are expected to serve as a reference for law enforcement, academics, policymakers, and the public in understanding and handling disputes arising from the misuse of deepfake technology, especially in providing legal protection for victims who suffer losses due to violations of privacy, identity, or honor through the use of AI. The research questions are formulated to examine the legal consequences of deepfake misuse, particularly from the perspective of civil liability and evidentiary mechanisms under Indonesian law.

1. How does the misuse of deepfake technology fulfill the elements of an unlawful act under Article 1365 of the Indonesian Civil Code?
2. How can evidence of fault, loss, and causation be established in civil proceedings involving deepfake misuse?

2. Research Methods

This study employs normative legal research. Normative legal research is used to examine applicable legal norms and assess whether such norms can be applied to the phenomenon of artificial intelligence (AI)-based deepfake content. The research focuses on analyzing legal principles, statutory regulations, and legal doctrines relevant to unlawful acts and the protection of individual rights in the digital environment. This study applies three approaches, namely the statutory approach, conceptual approach, and case approach. The statutory approach is used to examine the provisions of Article 1365 of the Indonesian Civil Code (*Kitab Undang Undang Hukum Perdata/KUHPerdata*), the 1945 Constitution of the Republic of Indonesia (*Undang Undang Dasar Negara Republik Indonesia/UUD NRI 1945*), the Electronic Information and Transactions Law (*Undang Undang Informasi dan Transaksi Elektronik/UU ITE*), and Law Number 27 of 2022 concerning Personal Data Protection. The conceptual approach is employed to analyze the legal concepts of unlawful acts, privacy rights, civil liability, and human rights protection. Meanwhile, the case approach is used to observe the practical misuse of deepfake technology and its legal implications in society.

This research is descriptive-analytical in nature. It not only describes the legal issues arising from deepfake technology but also analyzes the relationship between the elements of unlawful acts, evidentiary mechanisms, and human rights protection within the existing legal framework.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include the Indonesian Civil Code (KUHPerdata), the 1945 Constitution of the Republic of Indonesia, the Electronic Information and Transactions Law (UU ITE), Law Number 27 of 2022 concerning Personal Data Protection, and international human rights instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). These legal sources are relevant because they regulate the protection of honor, privacy, and personal data. Secondary legal materials consist of books, scientific journals, legal articles, and academic writings discussing deepfake technology, unlawful acts, digital evidence, privacy rights, and artificial intelligence. These materials are utilized to strengthen the normative analysis and provide a comprehensive understanding of legal developments related to AI-based technologies. Tertiary legal materials include legal dictionaries, encyclopedias, and other supporting references that assist in explaining technical concepts and terminology, such as artificial intelligence, deepfake technology, electronic evidence, and human rights.

The collection of legal materials is conducted through library research. This method involves reviewing legislation, judicial decisions, scientific journals, books, and other relevant legal literature related to deepfake technology and unlawful acts. The collected legal materials are analyzed qualitatively through systematic and conceptual interpretation. The analysis is carried out by examining the relationship between the legal materials and the elements of unlawful acts under Article 1365 of the Indonesian Civil Code, as well as relevant human rights principles. Through this approach, the study evaluates whether the creation and dissemination of deepfake content using artificial intelligence can give rise to civil liability and constitute an unlawful act under Indonesian law.

3. Results and Discussion

3.1. Fulfillment of the Elements of Unlawful Acts in the Use of Artificial Intelligence for the Creation and Distribution of Deepfake Content

The development of Artificial Intelligence (AI) has brought significant changes to various aspects of life, including digital communications and multimedia content production. One rapidly developing use of AI is deepfake technology, which can manipulate a person's image, voice, or video to produce content that appears authentic, even though it is actually digitally engineered (Farida, 2023; Arvitto, 2025). On the one hand, this technology offers various benefits in the creative, education, and entertainment industries. However, on the other hand, the misuse of deepfake technology raises various legal issues, particularly when used without the consent of the party whose identity is being exploited and causes harm to the victim (Putri et al., 2024). In the context of Indonesian civil law, such actions must be analyzed based on the provisions of Unlawful Acts as stipulated in Article 1365 of the Civil Code (KUHPerdata).

Article 1365 of the KUHPerdata states that any unlawful act that causes harm to another person requires the party whose fault caused the harm to compensate for the resulting loss (Mariam, 2017; Sholikhin, 2026). Based on judicial doctrine and practice, an act can be categorized as unlawful acts if it meets several elements: the existence of the act, its unlawful nature, the perpetrator's fault, the victim's loss, and a causal relationship between the act and the resulting loss. Therefore, to determine whether the use of AI in the creation and distribution of deepfakes is civilly liable, an analysis of each of these elements is necessary.

The initial element concerns the existence of an act (*daad*). In cases involving deepfakes, this element can be relatively readily established because it encompasses tangible actions, including the creation, modification, dissemination, or publication of digital content through artificial intelligence technology (Maharani & Mtm, 2025). Such actions are undertaken by individuals or groups using AI software and algorithms to generate visual or audio content that imitates the appearance or voice of a particular person. Consequently, the creation and distribution of deepfakes may constitute concrete conduct that satisfies the act element under Article 1365 of the Indonesian Civil Code.

The element of unlawfulness constitutes the second element to be examined. Under Indonesian civil law doctrine, unlawfulness extends beyond violations of statutory provisions to include infringements of others' subjective rights, breaches of legal obligations, violations of morality, and conduct contrary to propriety, prudence, and prevailing social norms (Tavadjio, 2025; Maharani et al., 2025). Accordingly, the unauthorized dissemination of deepfake content may constitute an unlawful act because it can infringe upon an individual's privacy, personal data protection, honor, and reputation. Such conduct may also violate applicable legislation, including the Electronic Information and Transactions Law (ITE Law) and Law Number 27 of 2022 concerning Personal Data Protection (*Undang Undang Perlindungan Data Pribadi/PDP Law*). Deepfakes are frequently employed to fabricate misleading information, disseminate defamatory content, facilitate fraud, or produce material that undermines an individual's dignity. Using someone's identity without consent to create visual or audio content that the person neither produced nor expressed may therefore violate legally protected personal rights (Noerman & Ibrahim, 2024; Putra, 2026). Thus, the unlawfulness element may be considered satisfied when deepfake creation or distribution infringes legally protected rights or violates applicable legal and social standards, particularly when undertaken without consent and causes harm to the affected individual.

The element of fault (*schuld*) constitutes the third element in assessing an unlawful act. Under civil law, fault may arise from either intentional conduct (*dolus*) or negligence (*culpa*). In deepfake cases, fault frequently involves intent, as perpetrators deliberately employ AI technology to manipulate an individual's identity, voice, or image, despite being aware that the resulting content does not represent the actual circumstances. Such content may be disseminated to damage someone's reputation, humiliate victims, obtain economic benefits, or influence public opinion. Nevertheless, negligence must also be considered when an individual

distributes deepfake content without adequately verifying its authenticity. In these circumstances, fault may still be established if the individual is proven to have failed to exercise the required standard of care when using digital technology. Accordingly, both intentional conduct (*dolus*) and negligence (*culpa*) may serve as grounds for establishing the element of fault in deepfake cases, depending on the perpetrator's actions, awareness, and compliance with the applicable standard of care.

The fourth element concerns the harm experienced by the victim, which may involve both material and immaterial losses in deepfake cases (Aprillia et al., 2025; Nugraha et al., 2025). Material losses may include job termination, lost business opportunities, reduced income, and other financial consequences resulting from the dissemination of manipulated content. Nevertheless, immaterial harm often constitutes the more significant impact, encompassing psychological distress, trauma, humiliation, diminished public trust, reputational damage, strained social relationships, and a decline in quality of life due to content that defames or misuses the victim's identity. A distinctive characteristic of deepfake-related harm is its extensive and rapid spread through internet platforms and social media. Once such content becomes publicly accessible, victims frequently encounter difficulties in controlling its further distribution (Ardiyani, 2024; Hidayat, 2025). Consequently, the adverse effects may persist over an extended period and affect a broad audience, even after the original content has been removed. These circumstances demonstrate that the misuse of deepfake technology has substantial potential to fulfill the harm element required to establish liability for an unlawful act under Article 1365 of the Indonesian Civil Code.

The element of causation represents the fifth element in establishing liability for an unlawful act. This element requires a demonstrable connection between the perpetrator's conduct and the losses experienced by the victim. In deepfake cases, causation may be established when the harm constitutes a logical and foreseeable consequence of creating or disseminating manipulated content (Haida & Nuriyatman, 2024; Arvitto, 2025). For instance, if an individual loses their employment following the circulation of a deepfake video that damages their reputation, the distribution of the video may be linked to the resulting loss. Although establishing causation in digital cases can be more complicated than in conventional cases, technological developments in digital forensics provide opportunities to identify content sources, dissemination timelines, metadata records, and the parties involved in producing or distributing deepfakes (Noerman & Ibrahim, 2024; Indriawati, 2026). Such evidence can help establish the sequence of events and clarify the relationship between the perpetrator's actions and the victim's losses. Therefore, combining technical forensic analysis with legal assessment can facilitate a more objective determination of causation and support the establishment of liability for unlawful acts under Article 1365 of the Indonesian Civil Code.

Based on the analysis of all these elements, it can be concluded that the use of AI in the creation and distribution of deepfake content can in principle fulfill the elements of an Unlawful Act as stipulated in Article 1365 of the Civil Code. There is a real act committed by the perpetrator,

there is an unlawful nature because it violates the right to privacy and honor, there is an element of fault either in the form of intent or negligence, the occurrence of material and immaterial losses to the victim, and there is a causal relationship between the action and the losses incurred (Pratama, 2024; Pane & Tambe, 2025). Therefore, perpetrators of misuse of deepfake technology can be held civilly responsible to provide compensation to the victim in accordance with the principles of Indonesian civil law.

Table 1. Juridical Construction of Deepfake as an Unlawful Act under Article 1365 of the Indonesian Civil Code

Element of Unlawful Act	Juridical Indicators in Deepfake Cases	Legal Consequences
Unlawful Act	Creation, manipulation, and dissemination of AI-generated deepfake content	Constitutes a legally relevant act capable of producing civil liability
Unlawfulness	Violation of privacy rights, personal data protection, honor, reputation, and provisions of the ITE Law and Personal Data Protection Law	Fulfills the element of unlawfulness under Article 1365 of the Civil Code
Fault	Intentional conduct (<i>dolus</i>) or negligence (<i>culpa</i>) in creating or distributing deepfake content	Establishes the subjective basis for civil responsibility
Damage	Material losses (financial and economic losses) and immaterial losses (psychological trauma, reputational harm, and dignity impairment)	Creates a legal basis for compensation claims
Causal Relationship	Direct linkage between the creation/dissemination of deepfake content and the resulting harm suffered by the victim	Confirms the obligation to compensate for damages

Table 1 presents the juridical construction of deepfake misuse as an unlawful act under Article 1365 of the Indonesian Civil Code by examining five essential elements: unlawful act, unlawfulness, fault, damage, and causal relationship. The table demonstrates that the creation, manipulation, and dissemination of AI-generated deepfake content may constitute legally relevant acts that generate civil liability when they violate privacy, personal data protection, honor, reputation, or applicable legal provisions. Intentional conduct (*dolus*) or negligence (*culpa*) establishes the basis for fault, while material and immaterial losses provide grounds for compensation claims. Furthermore, a direct causal relationship between the deepfake content and the harm suffered by the victim is necessary to establish the perpetrator's obligation to provide compensation. Thus, Table 1 illustrates how each element contributes to determining civil responsibility for deepfake-related misconduct under Article 1365 of the Indonesian Civil Code.

3.2. Deepfake Proof Mechanism and Human Rights Protection from a Civil Law Perspective

The development of Artificial Intelligence (AI) technology, which enables the creation of deepfake content, presents new challenges to the evidentiary system in civil law. Unlike conventional forms of legal violations, which generally leave easily identifiable physical traces, deepfakes are digital products designed to resemble reality in a highly convincing manner. This technology can manipulate a person's face, voice, gestures, and expressions, producing content that is difficult to distinguish from the original recording. Consequently, when such content is used to harm another party, the evidentiary process becomes more complex because a mechanism is required to distinguish between authentic facts and the results of technological manipulation (Chairani et al., 2024; Putri et al., 2025). In the context of an Unlawful Act lawsuit under Article 1365 of the Civil Code, evidence plays a crucial role because the party filing the lawsuit must be able to prove the existence of an act, fault, loss, and a causal relationship between the perpetrator's actions and the loss suffered. Therefore, the successful enforcement of the rights of deepfake victims depends heavily on the legal system's ability to accommodate digital evidence and relevant technological verification methods.

One of the main instruments in proving evidence in deepfake cases is electronic evidence. In the development of Indonesian law, electronic evidence has been recognized as valid evidence through the Electronic Information and Transactions Law (UU ITE) (Lubis, 2026; Silalahi & Dachi, 2026). This provision expands the concept of evidence, previously dominated by physical documents, to include electronic information and electronic documents. In deepfake cases, electronic evidence can include videos, audio recordings, digital images, online conversations, social media posts, emails, or other digital data related to the action in question (Wiguna & Aisyah, 2025; Nainggolan et al., 2026). The existence of electronic evidence allows victims to demonstrate that content was indeed created, distributed, or published to the public. However, the existence of electronic evidence alone is not always sufficient to prove manipulation. Deepfakes are designed to create the illusion of authenticity, requiring a more in-depth evidentiary approach. Therefore, metadata analysis is a crucial element in proving deepfake cases.

Metadata is data that describes the characteristics of a digital file, such as the creation time, modification time, device used, storage location, and data processing history. In the context of deepfakes, metadata can help reveal the origin of content and indicate whether the file has been manipulated. Through metadata analysis, investigators, digital forensic experts, and judges can gain insight into the creation and distribution of the content in question (Tirtakusuma et al., 2025; Oktavianti et al., 2025; Tavadjio, 2025). This information is crucial for linking content to the party suspected of producing it. In addition to metadata, proving deepfake cases also requires digital forensics support. Digital forensics is a scientific method used to identify, collect, examine, and analyze electronic evidence. In deepfake cases, digital forensic experts can perform various tests to detect visual and audio manipulation (Yanuafriza & Eluan, 2025; Nugraha et al., 2025). Modern forensic technology can identify lighting discrepancies, unnatural

facial movement patterns, voice and lip movement desynchronization, and even digital artifacts that often appear in AI-engineered content.

The role of digital forensics is becoming increasingly important as advances in AI technology make deepfakes increasingly difficult for humans to recognize. Content that was relatively easy to identify in the early days of deepfake technology can now be produced with a very high level of realism (Djokosoetono, 2008; Arvitto, 2025). In these circumstances, evidence cannot rely solely on visual perception or subjective judgment but must be based on scientifically sound technical analysis. The results of digital forensic examinations can then be used as a basis for judges to assess the authenticity of content and determine whether manipulation has occurred to the detriment of a particular party.

In addition to electronic evidence and forensic analysis, expert testimony also plays a crucial role in deepfake cases. The complexity of AI technology makes many technical aspects difficult for law enforcement officials and judges to understand. Therefore, the presence of experts in information technology, artificial intelligence, cybersecurity, and digital forensics is necessary to provide explanations regarding how deepfakes work, manipulation detection methods, and the reliability of electronic evidence presented in court (Putri et al., 2024; Indriawati, 2026). Expert testimony also serves to bridge the gap between technological developments and legal understanding. Through expert explanations, judges can gain confidence in the authenticity of evidence and understand the relationship between the technical process of creating deepfakes and the losses suffered by victims. Thus, expert testimony not only strengthens technical evidence but also helps ensure that decisions are based on a comprehensive understanding of the relevant facts and technology.

Beyond establishing the existence of deepfake content and identifying the perpetrator, the evidentiary process must establish a causal connection between the perpetrator's conduct and the harm experienced by the victim. In cases involving unlawful acts, causation plays a crucial role in determining whether legal liability can be imposed (Lany, 2025; Putra, 2026). Accordingly, victims must demonstrate that their losses resulted directly from, or were reasonably foreseeable consequences of, the creation or dissemination of deepfake content. Such a connection may be established by presenting evidence of reputational damage following publication, diminished employment opportunities, disrupted social relationships, or psychological distress arising from the circulation of the manipulated content (Haida & Nuriyatman, 2024; Aprillia et al., 2025). Furthermore, supporting evidence, including screenshots of social media posts, mass media reports, digital communication records, and witness testimony, can help substantiate the relationship between the perpetrator's actions and the resulting harm. Collectively, these forms of evidence strengthen the victim's claim and support the assessment of liability under the applicable civil law framework.

Beyond the evidentiary aspects of civil law, the issue of deepfakes also has a very strong human rights (*Hak Asasi Manusia/HAM*) dimension. The misuse of deepfake technology not only causes

economic or reputational losses but can also violate the fundamental rights of every individual. One of the rights most frequently impacted is the right to privacy. When a person's face, voice, or identity is used without consent to produce certain content, it constitutes an interference in a private space that should be protected by law (Oktavianti et al., 2025; Putri et al., 2025).

In the Indonesian legal system, protection of privacy and security is constitutionally based through Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. This provision guarantees the right of every person to protection of their privacy, family, honor, dignity, and security from threats that incite fear. The distribution of deepfakes depicting individuals in situations that never actually occurred has the potential to undermine all aspects of this protection. Similar protections are also found in various international human rights instruments. The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) affirm that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor shall they be subjected to attacks on their honor and reputation. When deepfake technology is used to create false narratives that damage a person's image, such actions can be considered a violation of the rights to privacy and honor guaranteed by national and international law.

Therefore, the burden of proof in deepfake cases is not only related to the technical aspects of the authenticity of digital content, but also relates to the protection of basic human rights (Chairani et al., 2024; Putri et al., 2025). Electronic evidence, metadata, digital forensics, and expert testimony are crucial tools for proving elements of unlawful acts and ensuring legal accountability. At the same time, a human rights-based approach provides a strong normative foundation for protecting victims from various forms of AI technology abuse. Therefore, strengthening the capacity of law enforcement officials, developing digital forensics methods, refining regulations, and increasing public digital literacy are crucial steps to ensure effective legal protection for deepfake victims in the era of artificial intelligence (Noerman & Ibrahim, 2024).

Table 2. Integrated Framework for Deepfake Evidence and Human Rights Protection

Dimension	Key Components	Function in Deepfake Cases
Electronic Evidence	Digital files, videos, audio recordings, social media content, metadata	Demonstrates the existence and dissemination of deepfake content
Digital Forensics	Frequency analysis, texture analysis, AI signature detection, synchronization analysis, metadata examination	Verifies authenticity and detects AI manipulation
Expert Testimony	Digital forensic experts, AI specialists, cybersecurity experts	Assists courts in understanding technical aspects of deepfake technology

Dimension	Key Components	Function in Deepfake Cases
Human Rights Protection	Privacy rights, honor and reputation, dignity, personal data protection	Establishes the victim's protected legal interests
Right to be Forgotten	Content removal, data erasure, delisting from search engines	Provides restorative remedies for victims
Civil Remedies	Material damages, immaterial damages, content removal orders, corrective statements	Ensures legal recovery and accountability
Future Regulatory Needs	Legal definition of deepfake, multi-actor liability framework, notice-and-takedown obligations, AI-specific legislation	Strengthens legal certainty and victim protection

Table 2 presents an integrated framework for examining deepfake evidence and protecting human rights, complementing the juridical analysis of unlawful acts under Article 1365 of the Indonesian Civil Code outlined in Table 1. While Table 1 identifies the essential elements of civil liability, including unlawfulness, fault, damage, and causal relationship, Table 2 highlights the evidentiary and remedial mechanisms necessary to establish those elements in deepfake cases. Electronic evidence and digital forensics support the identification, verification, and documentation of manipulated content, while expert testimony assists courts in understanding its technical characteristics (Maharani et al., 2025). Human rights protection, including privacy, dignity, reputation, and personal data protection, establishes the legal interests affected by deepfake misuse. Furthermore, the right to be forgotten and civil remedies provide restorative measures through content removal, data erasure, and compensation. Future regulatory development is also necessary to strengthen legal certainty, clarify multi-actor liability, and enhance victim protection.

4. Conclusion

The rapid development of Artificial Intelligence (AI), particularly deepfake technology, has created significant legal challenges for the Indonesian civil law system. This study examined the civil liability arising from the creation and dissemination of deepfake content through the perspective of Article 1365 of the Indonesian Civil Code (*KUHPerdata*), evidentiary mechanisms in civil litigation, and the protection of human rights affected by AI-generated manipulation. The findings demonstrate that existing civil law principles remain relevant and adaptable in addressing harms caused by emerging digital technologies.

First, this study concludes that the creation and dissemination of deepfake content using AI can fulfill all essential elements of an unlawful act under Article 1365 *KUHPerdata*. Deepfake-related conduct constitutes a concrete act through the creation, modification, and distribution of manipulated content. Such conduct may be considered unlawful because it violates privacy

rights, personal data protection, honor, reputation, and human dignity, which are protected under the Constitution, the Electronic Information and Transactions Law (ITE Law), and the Personal Data Protection Law. The element of fault may arise either through intentional conduct, where individuals deliberately create or distribute deceptive content, or through negligence when users fail to exercise reasonable care in handling AI-generated materials. Furthermore, deepfake content may generate both material and immaterial losses, including financial damages, loss of employment opportunities, psychological trauma, reputational harm, and social stigmatization. The existence of a causal relationship between the deepfake act and the resulting harm further supports the application of civil liability principles. Consequently, Article 1365 KUHPerdata can be interpreted progressively to hold creators and distributors of deepfake content accountable for the damages they cause.

Second, the study finds that civil disputes involving deepfake technology can be effectively addressed through existing evidentiary mechanisms, particularly electronic evidence recognized under Indonesian law. Electronic documents, digital files, metadata, access logs, platform records, and other forms of digital traces can serve as important sources of proof. The increasing sophistication of deepfake technology, however, necessitates the use of digital forensic analysis and expert testimony to verify authenticity and identify manipulation. Metadata examination, forensic verification, and proper chain-of-custody procedures play a critical role in ensuring the reliability of digital evidence. Although Indonesian law already recognizes electronic evidence, the growing realism of AI-generated content presents new evidentiary challenges that require enhanced technical capacity among law enforcement agencies, judges, and legal practitioners.

Third, deepfake technology raises substantial human rights concerns. The misuse of an individual's image, voice, or personal data without consent may violate fundamental rights, including the right to privacy, the right to honor and reputation, the right to human dignity, and the right to personal data protection. These rights are protected under Article 28G of the 1945 Constitution, Law No. 39 of 1999 on Human Rights, the Personal Data Protection Law, and international human rights instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Victims of deepfake misuse should therefore be entitled not only to compensation but also to restorative remedies, including content removal, access termination, data deletion, and the implementation of the right to be forgotten.

The study further demonstrates that Indonesian civil law possesses sufficient flexibility to respond to technological developments through dynamic interpretation of Article 1365 KUHPerdata. Nevertheless, the current legal framework remains fragmented because existing regulations do not specifically address the unique characteristics of deepfake technology. The absence of a clear legal definition, specific liability standards, and comprehensive regulatory mechanisms creates uncertainty for victims, law enforcement authorities, and digital platforms.

Accordingly, this study recommends the development of a more comprehensive regulatory framework for AI and deepfake technologies. Such a framework should establish clear legal definitions, allocate responsibility among creators, users, AI service providers, and digital platforms, strengthen notice-and-takedown mechanisms, and harmonize Indonesian regulations with international standards on privacy and data protection. In addition, improving digital literacy, enhancing forensic capabilities, and strengthening institutional preparedness are essential to ensure effective legal protection. Ultimately, a balanced legal approach that combines civil liability, digital evidence standards, human rights protection, and regulatory innovation is necessary to promote digital justice and safeguard individuals against the growing risks posed by AI-generated deepfake technologies.

5. References

Journals:

- Aprillia, N., Khasanah, D. R. A. U., & Pongantung, R. J. (2025). Implikasi hukum tentang penyalahgunaan teknologi deepfake terhadap kejahatan identitas digital. *Dinamika Hukum*, 26(2), 148-157. <https://doi.org/10.35315/dh.v26i2.10209>.
- Ardiyani, N. K. D. I. (2024). Analisis yuridis pertanggungjawaban pidana pelaku deepfake porn berdasarkan hukum positif. *Jurnal Kajian Hukum Dan Kebijakan Publik* | E-ISSN: 3031-8882, 2(1), 603-608. <https://doi.org/10.62379/cs863250>.
- Arvitto, R. S. (2025). Implikasi hukum deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 4(2), 73-82. DOI: 10.35912/jihham.v4i2.3937.
- Chairani, M. A., Yitawati, K., & Pradhana, A. P. (2024). Urgensi pengaturan hukum bagi penyalahgunaan aplikasi deepfake. *Jurnal Rechtsens*, 13(1), 81-96. <https://doi.org/10.56013/rechtsens.v13i1.2668>.
- Eka, P. & Ratna, S. (2025). Analisis Normatif terhadap Penyebaran Deepfake Sebagai Bentuk Pelanggaran Hukum. *Majelis: Jurnal Hukum*, 15(2), 125-145. <https://doi.org/10.62383/majelis.v3i1.1509>.
- Gultom, J. G. N. M. (2026). Pertanggungjawaban Hukum perdata Terhadap Kerugian Korban Penyalahgunaan Artificial Intelligence (AI) dan Deepfake di Indonesia. *Media Hukum Indonesia (MHI)*, 4(2). <https://doi.org/10.5281/zenodo.21000606>.
- Haida, R. S. N., & Nuriyatman, E. (2024). Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence (Ai) Dari Perspektif Hukum Pidana Indonesia. *Jurnal Hukum Respublica*, 24(01). <https://doi.org/10.31849/respublica.v24i01.23327>.
- Indriawati, S. E. (2026). Konstruksi Pertanggungjawaban Pidana atas Pemanfaatan Kecerdasan Buatan dalam Tindak Pidana Berbasis Deepfake. *Judge: Jurnal Hukum*, 6(10), 1933-1943. <https://doi.org/10.54209/judge.v6i10.2295>.
- Kurniawan, D. (2026). Analisis Tanggung Gugat dalam Kasus Deepfake yang Dihasilkan oleh AI Generatif. *Jurnal Hukum Pustaka*, 12(1), 78-95. <https://doi.org/10.59945/jpnm.v4i1.1070>.

- Lany, Arman. "Legal Responsibilities of Notaries in the Era of Artificial Intelligence in Preventing Fraudulent Property Transactions." *Jurnal Pembaharuan Hukum* 12, No 2 (2025): 356-374. DOI: 10.26532/jph.v12i2.47041.
- Maharani, B. A., Rahajeng, H. A., & Arianti, Z. D. (2025). Perlindungan Hukum Masyarakat dari Dampak Negatif Penggunaan AI. *Media Hukum Indonesia (MHI)*, 3(2). <https://doi.org/10.5281/zenodo.15783168>.
- Maharani, R., & Mtvn, S. M. (2025). Ganti rugi akibat penyalahgunaan artificial intelligence (deepfake) pada citra orang terkenal di Facebook berdasarkan Pasal 1365 BW. *Jurnal Hukum Lex Generalis*, 6(4). <https://doi.org/10.56370/jhlg.v6i4.1512>.
- Nainggolan, Bernard, Suwarno Suwarno, Keisha Dearin Dafa. "Reconstructing Copyright Protection for Artificial Intelligence-Generated Works." *Jurnal Hukum Unissula* 42, No 3 (2026): 614-646.
- Najah, R. S. (2026). Tantangan Hukum yang Ditimbulkan oleh Teknologi Deepfake dalam Pemalsuan Alat Bukti Elektronik di Indonesia. *Jurnal Hukum Elektronik*, 10(2), 156-175.
- Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi deepfake di Indonesia sebagai bentuk perlindungan negara. *Jurnal USM Law Review*, 7(2), 603-621. <https://doi.org/10.26623/julr.v7i2.8995>.
- Nugraha, M., Sadina, A. S., Ramadonna, V., & Hidayat, K. A. (2025). Analisis Unsur Perbuatan Melanggar Hukum Atas Penggunaan Artificial Intelligence Dalam Kasus Konten Deepfake. *Legal System Journal*, 2(1), 23-36.
- Oktavianti, R. G., Muqsith, A., & Nadia, I. (2025). Penyalahgunaan Deepfake Era Canggihnya Teknologi Memicu Kejahatan Media Misuse Of Deepfake In The Era Of Advanced Technology Is Triggering Media Crime. *IUS: Jurnal Ilmiah Fakultas Hukum*, 13(01), 114-122.
- Pane, D, P, R., & Tambe, A, W. (2025). Tantangan Penegakan Hukum dan Upaya Mitigasi atas Hadirnya Teknologi Deepfake Porn sebagai Jenis Tindak Pidana Digital pada Era Artificial Intelligence. *Pemuliaan Keadilan*, 2(3), 2345-2360. <https://doi.org/10.62383/pk.v2i3.1055>.
- Putra, M. R. S. (2026). Penyalahgunaan Deepfake Sebagai Perbuatan Melawan Hukum dalam Perspektif Kitab Undang-Undang Hukum Perdata. *Al-IHKAM Jurnal Hukum Keluarga Jurusan Ahwal al-Syakhshiyah Fakultas Syariah IAIN Mataram*, 18(2), 316-333. <https://doi.org/10.20414/alihkam.v18i1.15602>.
- Putri, K. A. R., Saputro, H. D., & Amanita, A. (2025). Pertanggungjawaban Hukum Atas Penggunaan Artificial Intelligence untuk Deepfake Menurut UU Perlindungan Data Pribadi. *Rechtswetenschap: Jurnal Mahasiswa Hukum*, 2(2).
- Putri, N. A., Nurmasitha, N., & Neisya, N. L. (2025). Analisis pertanggungjawaban perdata terhadap penyalahgunaan teknologi artificial intelligence (deepfake). *Jurnal Hukum Lex Generalis*, 6(12). <https://doi.org/10.56370/jhlg.v6i12.2019>.
- Putri, S. M. I., Salsabila, N., & Hosnah, A. U. (2024). Kriminalisasi penggunaan deepfake dalam tindak pidana penipuan dan pencemaran nama baik: Tantangan dan solusi hukum. *Jurnal Hukum Legalita*, 6(2), 83-90. <https://doi.org/10.47637/legalita.v6i2.1453>.

- Respati, A. A., Setyarini, A. D., Parlagutan, D., Rafli, M., Mahendra, R. S., & Nugroho, A. A. (2024). Analisis hukum terhadap pencegahan kasus deepfake serta perlindungan hukum terhadap korban. *Media Hukum Indonesia (MHI)*, 2(2). <https://doi.org/10.5281/zenodo.12508126>.
- Sholikhin, A. (2026). Analisis Pertanggungjawaban Perdata atas Penyalahgunaan Konten Deepfake. *Jurnal Hukum UPN*, 14(2), 234-250.
- Silalahi, W., & Dachi, F. N. (2026). Pertanggung jawaban Hukum Platform Media Sosial terhadap Penyebaran Konten Deepfake Berbasis Artificial Intelligence dalam Kasus Penipuan Berkedok Ritual Uang Gaib Ujang Busthomi. *Politika Progresif: Jurnal Hukum, Politik dan Humaniora*, 3(2), 22-36. <https://doi.org/10.62383/progres.v3i2.3110>.
- Tavadjio, S. N. (2025). Implikasi Legal dari Deepfake: Ganti Rugi Perdata atas Pemalsuan Wajah dan Suara. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(4), 4566-4577. <https://doi.org/10.61104/alz.v3i4.1995>
- Tirtakusuma, Andreas Eno, Eleazar Josiah Josiah Tirtakusuma, and Adino Jedidiah Jedidiah Tirtakusuma. "Artificial Intelligence and the Legal Framework in Preventing Financial Report Manipulation in Indonesia." *Jurnal Pembaharuan Hukum* 12, No 2 (2025): 242-262. DOI: 10.26532/jph.v12i2.47111.
- Wiguna, A., & Aisyah, P. (2025). Perlindungan hukum terhadap perempuan korban deepfake pornography di Indonesia. *Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882*, 3(1), 198-205. <https://doi.org/10.62379/gpq07x87>.
- Yanuafriza, A. Y., & Eluan, F. V. (2025). Pertanggungjawaban Perdata atas Penyalahgunaan Teknologi Deepfake dalam Perspektif Hukum Indonesia. *Indonesian Journal of Social Sciences and Humanities*, 5(2), 294-304.

Books:

- Annisa, R. (2024). *Pertanggungjawaban Perdata dalam Kasus Penyebaran Deepfake Pornografi*. Thesis, Jakarta: Fakultas Hukum Universitas Indonesia.
- Asshiddiqie, S. (2010). *Pengantar Ilmu Hukum*. Jakarta: Konstitusi Press.
- Bakry, A.S. (2005). *Hukum Perdata Indonesia*. Bandung: Mandar Maju.
- Djokosoetono, R. (2008). *Pengajaran Hukum Perdata BATIH Tinggi*. Jakarta: bdding.
- Farida, S. (2023). *Analisis Yuridis Perlindungan Data Pribadi dalam Teknologi AI Generatif*. Disertasi, Yogyakarta: Fakultas Hukum Universitas Gadjah Mada.
- Hardiansyah, D. (2019). *Hukum Teknologi dan Informasi*. Yogyakarta: Pustaka Pelajar.
- Hidayat, A. (2025). *Mekanisme Pembuktian Elektronik dalam Perkara Perdata yang Melibatkan Deepfake*. Thesis, Surabaya: Fakultas Hukum Universitas Airlangga.
- Kusumadi, S. (2015). *Hukum Perdata: Perbuatan Melawan Hukum*. Surabaya: Airlangga University Press.
- Lubis, A. H. (2026). *Hukum Pidana Penipuan Deepfake AI di Indonesia: Jeratan UU ITE dan KUHP Baru*. West Bromwich: AML Law Office.



- Mariam, W. (2017). *Hukum Acara Perdata Indonesia*. Jakarta: Prenadamedia Group.
- Marwan, P. (2020). *Hukum Perlindungan Data Pribadi*. Jakarta: Kencana.
- Mulya, A. (2018). *Hukum dan Teknologi: Tantangan Baru_REGULASI*. Jakarta: Rajawali Pers.
- Pratama, D. (2024). *Tanggung Jawab Platform Digital dalam Penyebaran Konten Deepfake*. Disertasi, Bandung: Fakultas Hukum Universitas Parahyangan.
- Rajawali, A. (2019). *Hukum dan Kecerdasan Buatan*. Jakarta: Prenadamedia Group.
- Utama, R. (2022). *Aspek Hukum Perlindungan Data Pribadi Source Subject terhadap Penggunaan Teknik Deepfake dalam Perspektif Perbuatan Melanggar Hukum*. Skripsi, Fakultas Hukum UNSRI.
- Widjaja, G. (2020). *Hukum Perlindungan Konsumen dan Data Pribadi*. Jakarta: Grasindo.

Internet:

- BP Lawyers. (2023). *Memahami Pasal 1365 KUHPerdata tentang Perbuatan Melawan Hukum*. *BP Lawyers Corporate Law Firms di Jakarta*. Retrieved in July 13, 2026, From <https://bplawyers.co.id/2023/11/02/memahami-pasal-1365-kuhperdata-tentang-perbuatan-melawan-hukum/>.