Lex Recta: Journal of Law and Normative Justice
Vol 1 No 2 June 2026, Hal 86-97
ISSN: 3163-4567 (Print) ISSN: 3163-4559 (Electronic)
Open Access: https://sovereignresearch.org/lex-recta

Reconceptualizing Legal Protection Against Deepfake Technology: A Normative Analysis of Privacy, Personality Rights, and Digital Evidence

Azka Syifaul Maula[1*], Ali Hardana[2]
[1] UIN Sunan Kalijaga Yogyakarta, Indonesia
[2] Universitas Islam Negeri Syekh Ali Hasan Ahmad Addary Padangsidimpuan, Indonesia
email: azkasyifaulmaula@gmail.com[1]

Article Info :
Received:
22-05-2026
Revised:
26-05-2026
Accepted:
12-06-2026

Abstract

The rapid development of deepfake technology has generated significant challenges for contemporary legal systems by destabilizing traditional conceptions of privacy, personal identity, and evidentiary authenticity. This study aims to reconceptualize legal protection against deepfake technology through a normative and doctrinal analysis of privacy rights, personality rights, and digital evidence. Employing a non-empirical legal research methodology, the study examines international human rights instruments, statutory regulations, judicial developments, legal doctrines, and comparative regulatory approaches concerning artificial intelligence and synthetic media governance. The analysis demonstrates that existing legal frameworks remain fragmented because privacy regulations primarily focus on informational control, personality-rights doctrines have not fully adapted to synthetic identity replication, and evidentiary regimes continue to rely upon assumptions of authenticity that are increasingly vulnerable to algorithmic manipulation. Deepfake technology creates a multidimensional legal injury that simultaneously affects identity integrity, individual autonomy, dignity, and procedural justice. The study argues that effective legal protection requires an integrated normative framework that recognizes synthetic identity harms as violations of interconnected legal interests. Such a framework strengthens legal certainty, enhances rights protection, and supports the development of more reliable evidentiary standards in digitally mediated societies.

Keywords: *Deepfake Technology, Privacy Rights, Personality Rights, Digital Evidence, Synthetic Identity.*

INTRODUCTION

The accelerated convergence of generative artificial intelligence, synthetic media architectures, and large-scale computational modeling has transformed the epistemological foundations of digital communication, creating unprecedented challenges for contemporary legal systems that were originally designed around assumptions of authenticity, verifiability, and human authorship. Deepfake technology, which enables the production of highly realistic synthetic representations of individuals through machine-learning algorithms, has evolved from an experimental computational tool into a pervasive socio-technical phenomenon capable of altering public discourse, manipulating reputational interests, violating informational self-determination, and undermining evidentiary reliability across digital environments. Current global debates increasingly recognize that the legal implications of deepfakes extend far beyond conventional concerns regarding misinformation, reaching into the core domains of privacy protection, personality rights, human dignity, identity autonomy, and procedural justice. The emergence of increasingly sophisticated deepfake applications has consequently generated a paradigmatic shift in legal scholarship, requiring a reassessment of the normative assumptions underlying rights-based protections in digital societies. Existing studies have documented how deepfake technologies facilitate unauthorized identity appropriation, non-consensual image manipulation, reputational exploitation, and technology-mediated harassment, revealing the growing inadequacy of traditional legal frameworks when confronted with algorithmically generated representations that blur the distinction between reality and fabrication (Kusnadi & Putri, 2025; Rohmawati et al., 2024; Nurmiati & Rizqi, 2026).

The expanding body of scholarship on deepfake governance demonstrates a notable progression from concerns regarding technological misuse toward broader inquiries into legal accountability and regulatory design. Recent studies have emphasized the necessity of strengthening legal protection

mechanisms against privacy violations arising from synthetic media manipulation, while simultaneously highlighting the vulnerability of victims whose personal identities become objects of unauthorized digital reconstruction (Kusnadi & Putri, 2025). Parallel research has examined the relationship between deepfake dissemination and online gender-based violence, arguing that synthetic content functions not merely as a technological artifact but as a structural instrument of power capable of reproducing digital harms with significant psychological and social consequences (Rohmawati et al., 2024). Other scholars have focused on the criminal-law dimension of deepfake misuse, emphasizing the urgency of criminalization strategies and legislative reform to address emerging forms of cyber-enabled misconduct that are insufficiently regulated under existing legal doctrines (Meliana, 2025; Basah et al., 2025; Nurkholisah et al., 2025). Complementary analyses concerning child pornography, non-consensual synthetic pornography, and commercial exploitation have further illustrated how deepfake technologies challenge established legal categories by creating novel forms of victimization that transcend traditional distinctions between tangible and intangible harms (Darmawan et al., 2025; Pitaloka, 2025; Putri, 2025).

Despite the richness of these contributions, the contemporary literature remains characterized by a fragmented analytical orientation that frequently isolates criminal liability, cybercrime regulation, victim protection, publicity rights, or ethical governance as separate doctrinal concerns rather than examining deepfake-related harms through an integrated framework of privacy, personality rights, and evidentiary legitimacy. Much of the existing scholarship approaches deepfakes primarily as objects of criminalization, producing a regulatory discourse that privileges punitive responses while paying comparatively limited attention to the deeper normative tensions between informational autonomy, identity integrity, and the legal recognition of digitally constructed personhood (Meliana, 2025; Basah et al., 2025; Nurkholisah et al., 2025). Research addressing privacy protection frequently concentrates on the existence of regulatory gaps without sufficiently interrogating how privacy itself must be reconceptualized when personal identity can be replicated, altered, and disseminated independently of an individual's consent or control (Kusnadi & Putri, 2025). Studies concerning synthetic pornography and commercial exploitation similarly reveal important dimensions of harm but often treat such manifestations as sector-specific problems rather than symptoms of a broader doctrinal crisis affecting the conceptual foundations of legal personality in digital environments (Pitaloka, 2025; Putri, 2025).

The limitations of current scholarship become even more pronounced when viewed through the lens of digital evidence and procedural law. While considerable attention has been devoted to the substantive regulation of deepfake-related misconduct, relatively little research has explored the implications of synthetic media for evidentiary reliability, authenticity assessment, and judicial truth-finding processes. The growing sophistication of deepfake generation technologies creates a scenario in which digital recordings, images, and audiovisual materials can no longer be presumed authentic merely because they appear credible, thereby destabilizing traditional evidentiary assumptions that underpin both civil and criminal adjudication. Existing analyses concerning online harassment, cybercrime, and digital victimization implicitly acknowledge the risks associated with fabricated content, yet they rarely engage with the broader question of how legal systems should recalibrate standards of proof, authentication mechanisms, and evidentiary presumptions in an era where synthetic representations increasingly approximate reality (Rohmawati et al., 2024; Darmawan et al., 2025; Nurmiati & Rizqi, 2026). This omission generates a significant conceptual gap because the effectiveness of legal protection ultimately depends not only on substantive rights recognition but also on the procedural capacity to establish truth in digitally mediated disputes.

The unresolved nature of these issues carries profound scientific and practical implications. From a theoretical perspective, the rise of deepfake technology exposes the inadequacy of conventional legal categories that treat privacy, personality rights, and evidentiary integrity as distinct domains governed by separate doctrinal logics. From a practical perspective, the absence of a coherent normative framework increases legal uncertainty for victims, courts, regulators, and digital platform operators confronted with increasingly sophisticated forms of synthetic identity manipulation. The challenge is no longer limited to determining whether deepfake-related conduct should be prohibited; the more fundamental question concerns how legal systems should conceptualize the relationship between human identity and digitally reproduced representations in environments where technological capabilities systematically undermine traditional assumptions regarding authenticity, consent, and attribution. Addressing this challenge requires moving beyond fragmented regulatory analyses toward a

comprehensive legal framework capable of explaining how privacy interests, personality rights, and evidentiary legitimacy interact within the broader architecture of digital governance.

This research positions itself within that unresolved intersection by reconceptualizing legal protection against deepfake technology through a normative analysis that integrates privacy theory, personality-rights doctrine, and the law of digital evidence into a unified analytical framework. The study aims to examine the extent to which existing legal concepts remain capable of responding to synthetic identity manipulation and to develop a more coherent normative foundation for protecting individuals against emerging forms of algorithmically generated harm. Its principal theoretical contribution lies in advancing an integrated understanding of deepfake-related injuries as violations of both personal autonomy and legal personhood rather than merely instances of technological misuse. Its methodological contribution lies in employing a comprehensive normative legal approach that bridges substantive rights analysis with evidentiary theory, thereby offering a more holistic model for evaluating legal protection in the age of synthetic media.

RESEARCH METHODS

This study employs a non-empirical legal research design grounded in a normative and doctrinal methodology to examine the adequacy of existing legal frameworks in addressing the challenges posed by deepfake technology. The research is based primarily on secondary legal materials consisting of international human rights instruments, data protection regulations, privacy and personality-rights doctrines, electronic transactions legislation, and legal norms governing digital evidence and evidentiary admissibility. Primary legal sources are complemented by secondary materials, including scholarly articles, legal commentaries, judicial decisions, policy papers, and interdisciplinary literature on artificial intelligence, digital identity, and synthetic media governance. A comparative dimension is incorporated to identify convergences and divergences among contemporary regulatory approaches concerning privacy protection, personality rights, and the authentication of digital evidence in the context of emerging deepfake technologies.

The analytical framework combines doctrinal legal analysis with a normative-conceptual approach to evaluate the coherence, sufficiency, and adaptability of existing legal principles in responding to synthetic identity manipulation. Legal materials are examined through systematic interpretation employing textual, systematic, teleological, and comparative methods in order to identify the normative foundations underlying privacy rights, personality rights, and evidentiary reliability within digital environments. The study further utilizes conceptual analysis to assess whether traditional legal categories remain capable of accommodating technologically mediated harms generated through deepfake systems and to formulate a reconceptualized framework of legal protection. The validity of the analysis is strengthened through doctrinal triangulation, whereby statutory provisions, legal principles, jurisprudential developments, and academic scholarship are critically compared and synthesized to ensure analytical consistency and normative rigor.

RESULTS AND DISCUSSION

Reconceptualizing Privacy Rights in the Age of Deepfake Technology: From Informational Control to Digital Identity Integrity

The normative architecture of privacy law was historically developed upon the assumption that personal information could be distinguished from fabricated representations through observable criteria of authenticity, an assumption that becomes increasingly unstable in the context of deepfake technology. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights establish legal protection against arbitrary interference with privacy, family, and reputation. Contemporary deepfake systems complicate these guarantees because algorithmically generated content frequently creates harms without relying upon the disclosure of authentic personal data. The legal injury emerges through synthetic reconstruction rather than direct extraction of information. Existing doctrinal interpretations of privacy consequently require conceptual expansion beyond informational secrecy toward the protection of identity integrity within digitally mediated environments (Malik, Surbhi, & Roy, 2024; Mansoor, 2024).

Privacy regulation within contemporary legal systems increasingly recognizes the autonomy interests of data subjects, yet substantial uncertainty remains regarding synthetic identity manipulation. Article 4 paragraph (1) of Indonesia's Law Number 27 of 2022 concerning Personal Data Protection

defines personal data through an identifiable-person framework that presupposes a factual connection between information and the data subject. Deepfake-generated representations frequently combine authentic biometric characteristics with fabricated audiovisual elements, producing legal ambiguity concerning whether the resulting content constitutes personal data, derivative personal data, or an entirely distinct legal object. Grammatical interpretation of statutory provisions offers only limited guidance because the legislative text was drafted before the widespread diffusion of generative artificial intelligence systems. Teleological interpretation indicates that the legislative objective of protecting informational self-determination extends logically to synthetic representations that undermine an individual's capacity to control manifestations of identity (Salsabilla, 2026; Kusnadi & Putri, 2025).

Comparative legal analysis reveals that privacy protection frameworks increasingly move toward recognizing identity-based harms rather than merely information-based harms. The European regulatory model established through the General Data Protection Regulation adopts a broad conception of personal data that encompasses identifiers capable of directly or indirectly identifying a natural person. Deepfake technologies challenge even this expansive framework because synthetic outputs may generate recognizable likenesses without reproducing identifiable data in a conventional sense. Legal scholarship increasingly argues that the decisive issue concerns the exploitation of identity attributes rather than the technical provenance of the underlying information. The distinction between informational privacy and identity privacy becomes increasingly significant when evaluating algorithmically generated content (Singh, 2024; Lodhi et al., 2024).

Doctrinal scholarship addressing deepfake harms demonstrates a growing consensus that privacy violations occur even when fabricated content lacks factual accuracy. Deepfake pornography illustrates this doctrinal evolution because victims frequently experience reputational, psychological, and social harms despite the artificial nature of the underlying content. Legal injury derives from the unauthorized appropriation of identity markers rather than from the dissemination of truthful information. Existing privacy doctrines grounded exclusively in secrecy and confidentiality fail to fully explain these forms of harm. Scholarly analyses increasingly advocate a rights-based approach that emphasizes dignity, autonomy, and personal identity as central objects of legal protection (Pitaloka, 2025; Apriana & Nugroho, 2025).

Systematic interpretation of Indonesian legislation further demonstrates the fragmentation of existing legal protections against deepfake-related privacy violations. Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 amending the Electronic Information and Transactions Law, and Law Number 12 of 2022 concerning Sexual Violence Crimes each address different dimensions of digital harm. None of these instruments explicitly conceptualize synthetic identity manipulation as an autonomous legal category.

Regulatory gaps become evident when courts must determine whether fabricated audiovisual representations constitute personal data misuse, defamation, electronic manipulation, or sexual violence. Fragmented statutory classifications risk producing inconsistent legal outcomes for functionally similar forms of victimization (Rohmawati, Junaidi, & Khaerudin, 2024; Apriana & Nugroho, 2025). The normative divergence among existing legal instruments may be illustrated through the following comparative framework.

Table 1. Comparative Mapping of Legal Instruments Governing Privacy Protection and Deepfake-Related Identity Harms

Legal Instrument	Relevant Provision	Protected Interest	Deepfake-Related Limitation
Law No. 27/2022 on Personal Data Protection	Article 4, Article 65	Personal Data and Informational Autonomy	No explicit regulation of synthetic identities
Law No. 1/2024 on Electronic Information and Transactions	Article 27A, Article 28	Electronic Integrity and Reputation	Focuses on dissemination rather than identity replication

Legal Instrument	Relevant Provision	Protected Interest	Deepfake-Related Limitation
Law No. 12/2022 on Sexual Violence Crimes	Relevant provisions on image-based abuse	Sexual Autonomy and Dignity	Limited applicability beyond sexualized content
GDPR (EU)	Articles 4 and 5	Data Subject Rights	Ambiguity regarding fully synthetic outputs

The table demonstrates that contemporary legal systems protect related interests through distinct doctrinal pathways while lacking a unified framework for addressing synthetic identity harms. Legal fragmentation creates interpretative uncertainty concerning the precise juridical basis of protection. Judicial actors consequently face difficulties in classifying deepfake-related injuries within existing statutory categories. Normative coherence requires the integration of privacy, identity, and dignity considerations into a single analytical structure.

The emergence of deepfake harassment further exposes limitations within traditional privacy jurisprudence. Harms generated through synthetic media frequently involve reputational degradation, psychological coercion, and identity distortion rather than unauthorized access to confidential information. Existing doctrines focused upon secrecy inadequately capture these dimensions because victims often suffer substantial injury despite the absence of private information disclosure. Legal scholarship increasingly characterizes deepfake harassment as an attack upon personal autonomy and identity sovereignty. Such conceptual developments support a transition from informational privacy toward identity-centered legal protection (Nurmiati & Rizqi, 2026; Huang, Arora, & Zarzycka, 2026).

International human rights law provides additional normative support for this reconceptualization. Article 8 of the European Convention on Human Rights protects private life in a manner that has been interpreted expansively by the European Court of Human Rights to include personal identity and individual development. Systematic interpretation of human dignity principles suggests that identity integrity constitutes an essential component of private life. Deepfake technologies directly interfere with this protected sphere by generating representations that distort personal self-definition. Human rights jurisprudence consequently offers a doctrinal foundation for extending privacy protections beyond informational paradigms (Shirish & Komal, 2024; Malik, Surbhi, & Roy, 2024).

The relationship between privacy and biometric security introduces an additional layer of legal complexity. Contemporary deepfake systems increasingly exploit facial recognition data, voice patterns, and behavioral characteristics that function simultaneously as identifiers and components of individual identity. Financial institutions, digital platforms, and authentication systems rely upon these attributes as proxies for trust and authenticity. Deepfake-enabled impersonation undermines the reliability of biometric verification mechanisms while exposing individuals to identity-based harms that transcend conventional data breaches. Legal responses focused exclusively upon unauthorized data access fail to adequately address this broader threat to identity integrity (Fernandez, 2025; Olasiyan & Olasiyan, 2026).

Normative reconstruction of privacy law requires recognition that deepfake technology challenges not merely the confidentiality of information but the juridical status of identity itself. Existing statutory frameworks continue to treat privacy primarily as a matter of informational control despite the emergence of technologies capable of manufacturing convincing digital replicas independent of direct data disclosure. Conceptual integration between privacy rights, dignity interests, and identity integrity provides a more coherent doctrinal basis for legal protection against synthetic representations. Such an approach aligns with evolving international human rights standards and comparative regulatory developments. The resulting framework establishes the foundation for examining how personality rights may further strengthen legal protection against deepfake-related harms.

Personality Rights and the Legal Status of Synthetic Identity: Reconstructing Individual Autonomy in the Era of Deepfake Replication

The emergence of deepfake technology has fundamentally altered the legal relationship between individuals and representations of their identity by enabling the creation of highly realistic digital

replicas that operate independently from the consent, control, and participation of the person being represented. Traditional legal doctrines concerning personality rights were developed to safeguard essential attributes of human individuality, including name, image, voice, reputation, honor, and personal identity. Deepfake systems challenge these doctrines because they permit the extraction, reproduction, and manipulation of identity markers without requiring physical interaction with the rights holder. The resulting legal conflict extends beyond privacy violations and enters the domain of personality rights, where the primary concern involves the unauthorized commodification, distortion, or appropriation of legally protected aspects of personhood. Contemporary legal scholarship increasingly recognizes that synthetic identity replication raises questions regarding the ontological boundaries of legal personality itself (Boothe, 2022; Jurcys, Kozuka, & Fenwick, 2026).

Personality rights possess a distinct juridical character because they protect the external manifestations of individual identity rather than merely the confidentiality of information. Civil law traditions generally conceptualize personality rights as inalienable rights derived from human dignity and personal autonomy. Deepfake-generated representations frequently interfere with these interests by producing synthetic audiovisual content that appears attributable to a real person despite lacking any authentic act of expression or participation. Legal injury arises from the false attribution of conduct, speech, or appearance to the affected individual. Systematic interpretation of personality-rights doctrine demonstrates that unauthorized identity replication constitutes a direct infringement of the individual's authority to determine how personal identity is represented within social and legal spaces (Singh, 2024; Mansoor, 2024).

Comparative legal developments reveal an increasing recognition that technological reproduction of identity attributes requires stronger legal protection than conventional intellectual property frameworks can provide. Copyright law protects creative works, while trademark law protects commercial identifiers. Personality rights protect the human person as the legal subject from whom identity attributes originate. Deepfake technology exposes the inadequacy of relying exclusively upon intellectual property mechanisms because the central harm concerns the unauthorized exploitation of personal identity rather than the unauthorized use of a protected work. Legal systems that fail to distinguish between these categories risk reducing human identity to a mere economic asset detached from dignity-based protections (Jurcys, Kozuka, & Fenwick, 2026; Olasiyan & Olasiyan, 2026).

The Indonesian legal framework contains several normative foundations capable of supporting personality-rights protection despite the absence of an explicit statutory regime dedicated to personality rights. Article 28G paragraph (1) of the Constitution of the Republic of Indonesia guarantees protection of personal dignity, honor, and security. Article 1365 of the Indonesian Civil Code establishes liability for unlawful acts causing damage to another person. Deepfake-generated impersonation can be interpreted as a form of unlawful interference with legally protected personality interests because it distorts the individual's public identity and social reputation. Teleological interpretation of constitutional and civil law principles suggests that protection of human dignity necessarily encompasses protection against synthetic identity appropriation (Putri, 2025; Kusnadi & Putri, 2025).

Commercial exploitation of deepfake-generated identities presents a particularly significant challenge for contemporary legal doctrine. Artificial intelligence systems can reproduce the likeness, voice, and behavioral characteristics of public figures for advertising, marketing, and entertainment purposes without authorization. The resulting practices implicate the doctrine of publicity rights, which seeks to protect the economic value associated with personal identity.

Existing Indonesian regulations provide limited guidance concerning the legal status of AI-generated identity replicas used for commercial gain. Normative analysis indicates that unauthorized commercial deployment of synthetic identities constitutes a violation of both economic interests and dignity-based personality rights (Putri, 2025; Jurcys, Kozuka, & Fenwick, 2026). The doctrinal relationship between personality rights and synthetic identity replication may be mapped through the following normative framework.

Table 2. Normative Classification of Personality Rights Violations Arising from Deepfake-Based Identity Replication

Personality Interest	Legal Basis	Nature of Deepfake Interference	Juridical Consequence
Name	Civil Personality Doctrine	False Attribution	Identity Misrepresentation
Image and Likeness	Constitutional Dignity Protection	Unauthorized Replication	Personality Rights Violation
Voice	Personal Identity Interest	Voice Cloning	Identity Appropriation
Reputation	Tort and Defamation Principles	Fabricated Conduct	Reputational Harm
Commercial Identity	Publicity Rights Doctrine	Unauthorized Exploitation	Economic and Moral Injury

The table demonstrates that deepfake technologies simultaneously affect multiple dimensions of legally protected personality interests. Traditional legal classifications often address these interests separately despite their interconnected nature within synthetic media environments. Deepfake replication produces cumulative harms that transcend conventional doctrinal boundaries. A unified personality-rights framework offers greater normative coherence when assessing these multidimensional injuries.

Deepfake pornography provides one of the clearest examples of the inadequacy of fragmented legal responses. Victims frequently experience reputational degradation, emotional trauma, professional harm, and social exclusion despite having never participated in the depicted acts. The legal injury cannot be fully explained through privacy doctrines because the central harm involves the transformation of the victim's identity into an instrument of fabricated sexual representation. Article 4 and related provisions of Law Number 12 of 2022 concerning Sexual Violence Crimes provide important protections against image-based sexual abuse, yet synthetic pornography introduces new questions concerning the legal treatment of fabricated representations. Personality-rights doctrine supplies a complementary analytical framework by emphasizing the victim's entitlement to control the public manifestation of personal identity (Apriana & Nugroho, 2025; Pitaloka, 2025; Tobing & Yuli, 2026).

Recent scholarship concerning deepfake-enabled sextortion further illustrates the necessity of expanding personality-rights protections. Synthetic content may be used to coerce victims through threats of publication even when the material itself is entirely fabricated. The coercive power of such content derives from its perceived authenticity rather than its factual accuracy. Existing criminal-law approaches frequently focus upon extortion, harassment, or unlawful dissemination while underestimating the underlying violation of personal identity autonomy. A personality-rights perspective identifies the wrongful appropriation of identity as the foundational injury from which additional harms emerge (Chawki, Basu, & Choi, 2026; Rohmawati, Junaidi, & Khaerudin, 2024).

Theoretical developments concerning digital personhood further strengthen the argument for reconceptualizing personality rights within synthetic environments. Advances in generative artificial intelligence increasingly enable the creation of persistent digital replicas capable of simulating speech, behavior, and interpersonal interaction. Such developments blur the distinction between representation and substitution, creating uncertainty regarding the legal boundaries of personhood and identity ownership. Doctrinal analysis indicates that existing legal categories remain heavily influenced by analog assumptions concerning physical embodiment and direct human action. Synthetic identity systems require a revised conception of personality rights capable of protecting individuals against technologically mediated forms of identity fragmentation and replication (Boothe, 2022; Jurcys, Kozuka, & Fenwick, 2026; Kostenko, Onishchenko, & Zhuravlov, 2026).

Comparative examination of international regulatory discourse demonstrates a growing movement toward recognizing identity integrity as an autonomous legal interest deserving explicit protection. Emerging scholarship increasingly frames synthetic identity manipulation as a violation of

human dignity, autonomy, and legal personality rather than merely a technological misuse or privacy infringement. Personality-rights doctrine provides the conceptual bridge necessary to connect these normative concerns within a coherent legal framework. Legal protection against deepfake technology becomes substantially more effective when identity replication is treated as an independent juridical wrong rather than a derivative consequence of data misuse or reputational injury. This doctrinal reconstruction establishes the normative foundation for evaluating the evidentiary consequences of synthetic media and the resulting crisis of authenticity within contemporary legal systems.

Deepfake Technology and the Crisis of Digital Evidence: Reconstructing Authenticity, Admissibility, and Evidentiary Reliability

The rapid advancement of deepfake technology has generated a profound challenge to the foundational assumptions of evidentiary law because contemporary legal systems have historically relied upon the premise that audiovisual materials possess a presumptive connection to observable reality. Courts, administrative institutions, and law enforcement agencies increasingly depend upon digital evidence to establish facts, verify conduct, and determine legal responsibility across both civil and criminal proceedings. Deepfake systems undermine this evidentiary paradigm by enabling the production of highly convincing synthetic content that may be indistinguishable from authentic recordings through ordinary observation. The resulting phenomenon destabilizes traditional indicators of reliability and authenticity that have long supported judicial truth-finding processes. Legal scholarship consequently characterizes deepfakes not merely as technological risks but as catalysts of a broader crisis of legal authenticity within the digital age (Muhammad, 2025; Tekayadi, Efendi, & Rosikhu, 2026).

The admissibility of electronic evidence within Indonesian law is principally governed by Law Number 1 of 2024 concerning Amendments to the Electronic Information and Transactions Law, particularly Article 5 paragraph (1), which recognizes electronic information and electronic documents as valid legal evidence. Article 5 paragraph (3) further requires that electronic systems satisfy statutory requirements to ensure evidentiary validity. Deepfake-generated content complicates these provisions because technical compliance with electronic system requirements does not necessarily guarantee the authenticity of the resulting audiovisual material. Grammatical interpretation of the statutory language reveals an emphasis upon the legal status of electronic documents rather than the substantive reliability of their content. Teleological interpretation suggests that the legislative objective of facilitating digital evidence presupposes a reasonable degree of trust in the authenticity of electronically generated information, a presupposition increasingly challenged by synthetic media technologies (Tekayadi, Efendi, & Rosikhu, 2026; Muhammad, 2025).

Comparative legal developments demonstrate that concerns regarding evidentiary reliability have become central to contemporary debates surrounding artificial intelligence governance. Common law jurisdictions traditionally evaluate evidentiary authenticity through witness testimony, chain-of-custody requirements, and technical verification procedures. Deepfake technology reduces the effectiveness of these safeguards because fabricated content may be generated and disseminated without leaving easily identifiable traces of manipulation. The evidentiary challenge no longer concerns whether a document exists but whether the content accurately reflects an underlying event. Legal systems increasingly confront the possibility that digital evidence may satisfy procedural admissibility requirements while remaining substantively deceptive (Olasiyan & Olasiyan, 2026; Muhammad, 2025).

The doctrinal distinction between admissibility and probative value acquires heightened significance within deepfake-related disputes. Admissibility determines whether evidence may be presented before a court, whereas probative value concerns the weight assigned to that evidence during judicial evaluation. Deepfake-generated content creates a scenario in which formally admissible evidence may possess limited epistemic reliability.

Judicial institutions must consequently develop more sophisticated methodologies for assessing authenticity beyond traditional visual inspection and testimonial corroboration. Existing evidentiary doctrines require reinterpretation to accommodate the technological realities of synthetic media production (Mansoor, 2024; Shirish & Komal, 2024). The relationship between deepfake technology and evidentiary reliability may be illustrated through the following normative framework.

Table 3. Normative Framework for Assessing the Impact of Deepfake Technology on Digital Evidence and Evidentiary Reliability

Evidentiary Principle	Traditional Assumption	Deepfake Challenge	Required Legal Response
Authenticity	Content reflects actual events	Synthetic fabrication of events	Enhanced verification standards
Integrity	Evidence remains unaltered	Undetectable manipulation	Forensic authentication
Attribution	Content linked to identifiable actor	False identity replication	Multi-layer attribution analysis
Reliability	Visual credibility indicates truthfulness	Convincing synthetic realism	Technical and contextual assessment
Probative Value	Authentic appearance supports evidentiary weight	Appearance no longer guarantees authenticity	Revised judicial evaluation criteria

The table demonstrates that deepfake technologies affect multiple dimensions of evidentiary assessment simultaneously rather than challenging a single procedural requirement. Conventional doctrines were developed in environments where visual recordings generally possessed strong evidentiary credibility. Synthetic media significantly weakens this presumption. Normative adaptation becomes necessary to preserve the integrity of judicial fact-finding processes.

International legal discourse increasingly acknowledges that synthetic media threatens not only individual rights but also the institutional legitimacy of adjudication itself. Article 14 of the International Covenant on Civil and Political Rights guarantees the right to a fair trial, a principle that presupposes the availability of reliable evidence capable of supporting rational judicial decision-making. Deepfake-generated materials complicate this guarantee because fabricated evidence may distort factual determinations while remaining superficially persuasive. Judicial reliance upon unreliable digital evidence risks producing erroneous outcomes that undermine procedural justice. Evidentiary reform consequently becomes a matter of both technological regulation and human rights protection (Malik, Surbhi, & Roy, 2024; Muhammad, 2025).

The concept of digital authenticity requires substantial doctrinal reconstruction in response to these developments. Traditional evidentiary frameworks frequently associate authenticity with provenance, integrity, and identifiable authorship. Deepfake systems challenge each of these criteria by enabling realistic simulations that can obscure origins, disguise alterations, and fabricate attribution. Legal scholars increasingly argue that authenticity should be understood as a multidimensional concept incorporating technical verification, contextual consistency, and forensic analysis rather than mere visual plausibility. Such an approach aligns with broader developments in digital law that emphasize the interaction between technological design and normative regulation (Kostenko, Onishchenko, & Zhuravlov, 2026; Olasiyan & Olasiyan, 2026).

Criminal law presents particularly acute concerns regarding synthetic evidence because prosecutorial decisions frequently depend upon audiovisual documentation. Article 184 of the Indonesian Criminal Procedure Code recognizes several categories of evidence, while subsequent developments in electronic evidence law have expanded the role of digital materials within criminal proceedings. Deepfake-generated recordings may be deployed to fabricate confessions, construct false narratives, or undermine genuine evidence through claims of manipulation. The resulting phenomenon, often described as the “liar’s dividend,” enables wrongdoers to deny authentic recordings by invoking the possibility of deepfake fabrication. Evidentiary uncertainty consequently affects both inculpatory and exculpatory dimensions of criminal adjudication (Tekayadi, Efendi, & Rosikhu, 2026; Basah, Wijaya, & Januardy, 2025).

Normative analysis of cybercrime regulation further indicates that evidentiary challenges cannot be separated from broader questions of accountability and criminalization. Deepfake technologies facilitate identity theft, synthetic fraud, reputational manipulation, child exploitation, and non-consensual sexual content dissemination through mechanisms that depend heavily upon deceptive audiovisual representations. Legal responses focused exclusively upon substantive criminal offenses

may prove insufficient if evidentiary systems remain vulnerable to sophisticated synthetic manipulation. Effective regulation requires simultaneous development of substantive norms governing prohibited conduct and procedural safeguards ensuring evidentiary reliability. Integrated approaches increasingly appear within contemporary discussions concerning cybercrime governance and digital justice (Nurkholisah et al., 2025; Darmawan, Junaidi, & Khaerudin, 2025; Chawki, Basu, & Choi, 2026).

The doctrinal reconstruction of evidentiary law in the era of deepfake technology requires movement beyond traditional assumptions that authenticity can be inferred from appearance, provenance, or formal admissibility alone. Contemporary legal systems must recognize that synthetic media has transformed authenticity from a presumed characteristic into a contested legal question requiring affirmative verification. Normative integration between evidentiary law, digital governance, privacy protection, and personality-rights doctrine offers a more coherent response to the challenges posed by algorithmically generated content. Judicial evaluation standards must increasingly incorporate technical expertise, forensic methodologies, and context-sensitive analysis to preserve the reliability of legal decision-making. The resulting framework supports a reconceptualized model of legal protection in which privacy, personality rights, and evidentiary integrity function as interconnected components of a comprehensive response to deepfake technology.

CONCLUSION

Deepfake technology has exposed fundamental inadequacies within conventional legal frameworks that continue to treat privacy, personality rights, and evidentiary integrity as separate juridical domains despite their increasingly interconnected nature within digital environments. Normative analysis demonstrates that privacy protection can no longer be confined to informational control because synthetic media enables harmful identity manipulation even in the absence of unauthorized data disclosure. Personality-rights doctrine provides a more robust conceptual basis for addressing the unauthorized replication, commercialization, and distortion of human identity, yet existing legal systems have not fully adapted these protections to the realities of artificial intelligence-generated representations. The evidentiary implications of deepfakes reveal an equally significant challenge, as traditional assumptions regarding authenticity, attribution, and reliability are increasingly incapable of ensuring accurate judicial fact-finding. Legal protection against deepfake-related harms requires a reconceptualized framework grounded in identity integrity, human dignity, and procedural reliability, in which privacy rights, personality rights, and digital evidence function as mutually reinforcing components of a coherent legal response. Such a framework contributes to the advancement of digital-era legal doctrine by aligning substantive rights protection with evolving technological realities and strengthening the normative foundations of justice in an age of synthetic media.

REFERENCES

Apriana, M., & Nugroho, A. (2025). Perlindungan Hukum bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelligence (AI) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual. *Journal of Social and Economics Research*, *7*(1), 57-75. https://doi.org/10.54783/jser.v7i1.796.

Basah, D. A. Y., Wijaya, A., & Januardy, I. (2025). Kriminalisasi pelanggaran protokol digital: tinjauan hukum pidana terhadap penyebaran deepfake di media sosial. *Innovative: Journal of Social Science Research*, *5*(4), 386-398. https://doi.org/10.31004/innovative.v5i4.20258.

Boothe, A. (2022). The death and life of Jang Nayeon: a case for personality rights in the digital layers of reality. *International Journal of Law and Information Technology*, *30*(4), 398-422. https://doi.org/10.1093/ijlit/eaad005.

Chawki, M., Basu, S., & Choi, K. S. (2026). Deepfake Sextortion in England, Wales and Northern Ireland: A Doctrinal and Regulatory Analysis. *Laws*, *15*(1), 11. https://doi.org/10.3390/laws15010011.

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artifical Intelegence Di Indonesia. *Jurnal Penelitian Serambi Hukum*, *18*(01), 42-54. https://doi.org/10.59582/sh.v18i01.1257.

Fernandez, H. (2025). Face Card Declined: The Deepfake Threat to Biometric Security in Financial Systems. *Washington and Lee Law Review Online*, *83*(1), 38.

Huang, W., Arora, P., & Zarzycka, M. (2026). Geographies of Hope: Rethinking Deepfake Harms and Gender AI Safety in the Global South. *Media and Communication*, *14*. https://doi.org/10.17645/mac.10969.

Jurcys, P., Kozuka, S., & Fenwick, M. (2026). A Private Law Framework for Personal AI Replicas: A Comprehensive Analysis of Legal Issues. *Available at SSRN 6500358*. https://dx.doi.org/10.2139/ssrn.6500358.

Kostenko, O., Onishchenko, N., & Zhuravlov, D. (2026). Technical And Legal Definitions As A Basis Of Modern Digital Law And Digital Jurisdiction: A Model Algorithm Of AI Design Technical And Legal Norms. *Metaverse Science, Society and Law*, *2*(2). https://doi.org/10.69635/mssl.2026.2.2.41.

Kusnadi, S. A., & Putri, D. W. S. (2025). Perlindungan hak privasi dalam penyalahgunaan teknologi deepfake di Indonesia. *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional*, *14*(2).

Lodhi, A. R. K., Sajjad, A., Akbar, K., Uddin, D. S. S., Jabeen, D. R., & Lashari, A. H. (2024). Artificial Intelligence, Cyber Law, And Data Protection: Legal Challenges And Regulatory Responses In The Digital Age. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *31*(S2), 84-97. https://doi.org/10.5281/zenodo.20258787.

Malik, S., Surbhi, A., & Roy, D. (2024, October). Blurring boundaries between truth and illusion: analysis of human rights and regulatory concerns arising from abuse of deepfake technology. In *AIP Conference Proceedings* (Vol. 3220, No. 1, p. 050016). AIP Publishing LLC. https://doi.org/10.1063/5.0234995.

Mansoor, S. I. U. (2024). Legal implications of deepfake technology: In the context of manipulation, privacy, and identity theft. *Central University of Kashmir Law Review*, *4*, 65-92. https://doi.org/10.66498/CUKLR.4.2024.65-92.

Meliana, Y. (2025). Urgensi formulasi perlindungan hukum dan kepastian pidana terhadap pengaturan tindak pidana deepfake dalam sistem hukum pidana nasional. *Jurnal Hukum Lex Generalis*, *6*(7). https://doi.org/10.56370/jhlg.v6i7.1087.

Muhammad, O. (2025). AI-Generated Deepfakes and the Crisis of Legal Authenticity: Reconstructing Evidentiary Standards in the Digital Age. *Sarhad Journal of Legal Studies*, *1*(1), 01-15.

Nurkholisah, S., Rismana, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia. *Jurnal USM Law Review*, *8*(3), 2421-2445. https://doi.org/10.26623/julr.v8i3.13060.

Nurmiati, E., & Rizqi, F. N. (2026). Tinjauan etika profesi teknologi informasi terhadap deepfake harassment di media sosial: Systematic literature review. *Jurnal Ilmiah Multidisipin*, *4*(4), 368-376. https://doi.org/10.60126/jim.v4i4.1563.

Olasiyan, T., & Olasiyan, A. (2026). Regulating Synthetic Identity: Deepfakes, Voice-Cloning and the Future of AI Law. *Voice-Cloning and the Future of AI Law (April 26, 2026)*. https://dx.doi.org/10.2139/ssrn.6660880.

Pitaloka, C. A. G. (2025). Penyalahgunaan Teknologi Deepfake untuk Konten Pornografi Non-Konsesual di Indonesia. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, *2*(2), 74-81. https://doi.org/10.62383/humif.v2i2.1475.

Putri, B. W. Y. (2025). Perlindungan Hukum Hak Publisitas Terhadap Eksploitasi Teknologi Deepfake Ai Dalam Konteks Komersial Menurut Hukum Positif Di Indonesia. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *12*(9), 3968-3978. https://doi.org/10.31604/jips.v12i9.2025.3968-3894.

Rohmawati, I., Junaidi, A., & Khaerudin, A. (2024). Urgensi regulasi penyalahgunaan deepfake sebagai perlindungan hukum korban kekerasan berbasis gender online (KBGO). *Innovative: Journal Of Social Science Research*, *4*(6), 1779-1794. https://doi.org/10.31004/innovative.v4i6.16559.

Salsabilla, A. (2026). Perlindungan Hukum terhadap Korban Perekaman Tidak Sah dan Penyebaran Konten Pribadi di Platform Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(3), 3769-3781. https://doi.org/10.61104/alz.v4i3.5941.

Shirish, A., & Komal, S. (2024). A socio-legal inquiry on deepfakes. *California Western International Law Journal*, *54*(2), 6.

Singh, A. (2024). Development of Personality Rights and Data Privacy Regulation of Deepfakes. *Available at SSRN 5348028*. https://dx.doi.org/10.2139/ssrn.5348028.

.

Tekayadi, S. K., Efendi, S., & Rosikhu, M. (2026). Konstruksi Hukum Pidana Terhadap Kejahatan Deepfake Dalam Perspektif Manipulasi Bukti Digital. *Justice Voice*, *5*(1), 47-59. https://doi.org/10.37893/jv.v5i1.1367.

Tobing, R. N. A., & Yuli, Y. (2026). Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media. *Eduvest-Journal of Universal Studies*, *6*(2), 1302-1314. https://doi.org/10.59188/eduvest.v6i2.52738.