

CRIMINAL LIABILITY FOR THE MISUSE OF DEEPPFAKE VIDEOS IN THE CRIME OF DEFAMATION UNDER THE ELECTRONIC INFORMATION AND TRANSACTIONS LAW

Herson Djuanda¹
Universitas Mahendradatta

Erikson Sihotang²
Universitas Mahendradatta

Komang Edy Dharma Saputra³
Universitas Mahendradatta

Correspondence : Herson Djuanda (Hersondjuanda24@gmail.com)

ABSTRACT

The rapid advancement of artificial intelligence has produced deepfake technology capable of generating highly realistic audio-visual content that misrepresents a person's statements, conduct, or likeness. When such synthetic media is deliberately used to attack a person's honour or reputation, it raises pressing questions of criminal accountability under Indonesian positive law, particularly Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (UU ITE). This article examines how criminal liability for deepfake-based defamation is constructed under the UU ITE, focusing on the interaction between Article 27A (defamation), Article 35 (manipulation of electronic documents), Article 27 paragraph (1) (indecent content), and related provisions of the Personal Data Protection Law and the Penal Code. Using a normative juridical method combined with statutory, conceptual, and case-based approaches, this study finds that although the UU ITE does not expressly define the term "deepfake," its provisions on electronic document manipulation and defamation may be extended to cover deepfake-based attacks on reputation, provided that intent (*mens rea*), falsity of the content, and public disclosure can be proven. The study also identifies significant normative gaps: the absence of a specific statutory definition of synthetic or manipulated media, the difficulty of attributing authorship of AI-generated content, the complaint-based (*delik aduan*) character of Article 27A which limits standing to the individual victim, and jurisdictional obstacles when perpetrators or hosting platforms are located abroad. The article concludes that a coherent doctrine of criminal liability for deepfake-based defamation requires either an interpretive extension of existing norms through consistent judicial practice or a dedicated legislative amendment that explicitly defines synthetic and manipulated media within the electronic transactions legal framework.

Keywords: deepfake; criminal liability; defamation; Electronic Information and Transactions Law; artificial intelligence

INTRODUCTION

The convergence of artificial intelligence and digital media production has produced a new category of synthetic content known as "deepfake," a portmanteau of "deep learning" and "fake" that refers to audio-visual material generated or altered by machine-learning algorithms to depict a person saying or doing something that never actually occurred. What began as a niche academic curiosity in computer vision research has, within less than a decade, become a

widely accessible tool. Free and low-cost applications now allow ordinary users with no technical training to superimpose a person's face onto another body, synthesise a convincing voice from a short audio sample, and produce a video that is, to the untrained eye, indistinguishable from an authentic recording.

This technological accessibility carries a darker consequence when deepfake techniques are directed not at entertainment or satire but at deliberately damaging another person's honour and reputation. A fabricated video that appears to show a public official making corrupt statements, a businessperson admitting to fraud, or a private citizen engaged in conduct they never committed can spread across social media within minutes, reaching audiences long before any correction or denial can catch up. Because the harm caused by a defamatory deepfake is compounded by the apparent authenticity of moving image and sound, victims often face reputational injury that is more difficult to rebut than injury caused by written or spoken defamation alone.

Indonesia's principal instrument governing conduct in electronic systems is Law Number 11 of 2008 concerning Electronic Information and Transactions Law, as amended first by Law Number 19 of 2016 and, most recently, by Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (hereinafter "UU ITE"). The 2024 amendment relocated and reformulated the defamation provision that had previously been housed in Article 27 paragraph (3) into a new Article 27A, alongside a new Article 27B addressing threats of defamation and extortion. Separately, Article 35 of the UU ITE prohibits the manipulation, creation, alteration, deletion, or destruction of electronic information or electronic documents with the intent that such information or documents be regarded as authentic, an offence punishable under Article 51 paragraph (1) with imprisonment of up to twelve years and/or a fine of up to twelve billion rupiah. Neither Article 27A nor Article 35, however, was drafted with deepfake technology specifically in mind, and the UU ITE as a whole contains no definition of "deepfake," "synthetic media," or "AI-generated content."

This normative silence creates a doctrinal problem. When a perpetrator fabricates a video using AI face-swapping or voice-cloning technology and disseminates it with the intent of damaging another person's honour, prosecutors and courts must decide which provision, or combination of provisions, most accurately captures the wrongdoing: is the essence of the offence the act of manipulation itself (Article 35), the act of defaming through electronic means (Article 27A), the dissemination of indecent content where the deepfake is sexual in nature (Article 27 paragraph (1)), or some combination that requires layered charging (concurus)?

The absence of legislative clarity on this question risks inconsistent enforcement, under-inclusive protection of victims, or, conversely, an overly expansive application of existing norms that could chill legitimate satire, parody, and commentary.

Against this background, this article addresses the following research questions: first, how is criminal liability for the misuse of deepfake videos in the commission of defamation constructed within the existing framework of the UU ITE; and second, what normative and practical obstacles arise in applying that framework, and how might they be addressed. The discussion is confined to the criminal law dimension of deepfake-based defamation against natural persons and does not extend to civil remedies, corporate reputational harm, or the broader questions of platform liability, though these are referenced where relevant to contextualise the criminal law analysis.

METHOD

This study employs a normative (doctrinal) juridical method, which examines law as a system of norms concerning principles, rules, and doctrines that govern conduct, rather than as an empirical social phenomenon. The normative method is appropriate for this study because the central research problem is one of legal interpretation: determining how existing statutory provisions apply, or fail to apply, to a factual scenario (deepfake-based defamation) that was not explicitly contemplated at the time those provisions were drafted.

Three complementary approaches are used. First, the statutory approach (statute approach) is used to analyse the text of the relevant provisions of the UU ITE (Law Number 1 of 2024), the Personal Data Protection Law (Law Number 27 of 2022), the Penal Code (Wetboek van Strafrecht) and the new Penal Code (Law Number 1 of 2023), and their official explanatory notes. Second, the conceptual approach is used to clarify legal concepts that lack explicit statutory definition, particularly "deepfake," "electronic document manipulation," and "synthetic media," by reference to legal and technical literature. Third, a case approach is used to examine relevant judicial decisions and Constitutional Court rulings that have interpreted the elements of electronic defamation and electronic document manipulation, in order to understand how courts have historically applied these provisions and to extrapolate their likely application to deepfake-specific fact patterns.

Data for this study consist entirely of secondary legal data, gathered through library-based legal research (penelitian kepustakaan). Primary legal materials comprise the applicable statutes, their official elucidations (penjelasan), and published court and Constitutional Court decisions. Secondary legal materials comprise legal scholarship, journal articles, practitioner commentary, and academic theses addressing electronic defamation, electronic document

falsification, and deepfake technology. The collected materials are analysed qualitatively using legal-interpretive techniques, namely grammatical interpretation of statutory text, systematic interpretation across related provisions within and beyond the UU ITE, and teleological interpretation with reference to the legislative purpose of protecting individual honour and the integrity of electronic systems. The analysis proceeds by first isolating the constituent elements of each relevant offence, then testing whether those elements can, as a matter of legal reasoning, be satisfied by the technical process and product of deepfake video creation and dissemination, and finally identifying points at which the fit between norm and fact pattern becomes strained or indeterminate.

RESULT AND DISCUSSION

Mapping the Elements of Article 27A onto Deepfake Conduct

Article 27A of the amended UU ITE criminalises a person who "intentionally attacks the honour or good name of another person by accusing them of something, with the intent that the accusation be known to the public, in the form of Electronic Information and/or Electronic Documents transmitted through an Electronic System." Breaking this formulation into its constituent elements yields: (a) a subjective element of intent (*dengan sengaja*); (b) an objective act of attacking honour or good name; (c) a specific modality, namely accusing the victim of something (*menuduhkan suatu hal*); (d) a further subjective element that the accusation be intended for public knowledge; and (e) a technical element, that the conduct occurs in the form of electronic information or documents transmitted through an electronic system.

Applying this structure to a deepfake video used for defamatory purposes, element (e) is straightforwardly satisfied: a deepfake video is, by definition, an electronic document, and its dissemination via social media platforms, messaging applications, or streaming services constitutes transmission through an electronic system. Element (c) is likewise satisfied where the fabricated video depicts the victim making a statement or engaging in conduct that amounts to an accusation of wrongdoing, immorality, or incompetence; indeed, the audio-visual format arguably strengthens the accusatory force of the content relative to a written allegation, because the medium itself implies first-hand evidence of the victim's own words or actions.

Element (b), the attack on honour or good name, similarly poses little conceptual difficulty once falsity and reputational harm are established, since the explanatory note to Article 27A defines the attack broadly as conduct that demeans or damages a person's reputation or dignity. The greater analytical difficulty lies in elements (a) and (d), both of which concern the perpetrator's state of mind. Because deepfake production is a multi-step technical process, requiring the collection of source material, training or use of a generative model,

rendering of the synthetic output, and a separate act of dissemination, proving that the perpetrator acted with the specific intent to attack honour and to make the accusation known to the public requires evidence connecting each of these steps to a deliberate reputational purpose, as opposed to, for example, private experimentation, parody clearly labelled as such, or satire that a reasonable audience would not mistake for a genuine depiction. The line between punishable defamatory intent and protected expressive activity is therefore not resolved by the technology itself but by the totality of circumstances surrounding creation and distribution, including captions, context, audience reaction, and any disclaimer of fictional status.

Article 35 as a Falsification-Based Alternative

Where the defamatory intent behind a deepfake is difficult to establish, or where prosecutors prefer a charge less encumbered by the complaint-offence and subjective-intent requirements of Article 27A, Article 35 of the UU ITE offers an alternative or cumulative basis of liability directed at the act of falsification itself. Article 35 requires: (a) intent and unlawfulness; (b) an act of manipulation, creation, alteration, deletion, or destruction of electronic information or an electronic document; and (c) the purpose that the resulting information or document be regarded as authentic.

A deepfake video satisfies element (b) almost definitionally, since the entire technical process of generative face-swapping or voice cloning constitutes the "creation" or "manipulation" of an electronic document. Element (c), the purpose of being regarded as authentic, aligns closely with the core function of deepfake technology, which is specifically engineered to defeat a viewer's ability to distinguish synthetic from genuine content. Judicial decisions applying the predecessor provision (Article 35 of the 2016-amended UU ITE) to conventional document and account falsification confirm that courts are willing to treat the "appearance of authenticity" element as satisfied once the falsified material is shown to a third party who could reasonably be misled, a standard that transfers readily to deepfake fact patterns.

The comparative advantage of proceeding under Article 35 is twofold. First, it is not a complaint offence, meaning that prosecution is not contingent on the personal report of the defamed individual, which may matter where the victim is unable or unwilling to report, for instance due to intimidation, or where the primary societal harm (erosion of trust in digital evidence generally) extends beyond the individual victim. Second, its considerably heavier sanction, up to twelve years' imprisonment under Article 51 paragraph (1), better reflects the aggravated harm of AI-facilitated falsification compared with the two-year maximum attached

to conventional electronic defamation under Article 27A. The trade-off is that a charge grounded solely in Article 35 does not squarely capture the reputational harm suffered by the victim, since the falsification offence protects the integrity of electronic systems and evidentiary trust rather than personal honour as such. This suggests that, doctrinally, the most complete characterisation of deepfake-based defamation is a cumulative charge (*concursum realis* or, where the acts are inseparably connected, *concursum idealis*) combining Article 27A and Article 35, allowing a court to address both the falsification and the reputational injury within a single proceeding.

Indecent Deepfake Content and the Interface with Article 27 Paragraph (1)

A significant subset of malicious deepfake activity involves fabricating sexually explicit or indecent depictions of the victim, commonly referred to as non-consensual synthetic intimate imagery. In these cases, Article 27 paragraph (1) of the UU ITE, prohibiting the intentional and unlawful broadcasting, exhibition, distribution, transmission, or facilitation of access to electronic information or documents violating decency, provides an additional charge that may be brought alongside or instead of Article 27A, depending on whether the fabricated content also contains an accusatory statement capable of independently damaging reputation. Because indecent deepfake content inherently damages the depicted person's dignity even without an accompanying verbal accusation, Article 27 paragraph (1) fills a doctrinal gap that Article 27A, with its requirement of an accusation of "something," may not fully cover. Practitioner commentary consistently treats these two provisions as complementary rather than mutually exclusive, with the choice of charge, or combination of charges, depending on the specific content and manner of dissemination.

The Complaint-Offence Requirement and Its Practical Consequences for Deepfake Victims

The Constitutional Court's affirmation that Article 27A constitutes a *delik aduan*, prosecutable only upon the personal complaint of the victim or their duly appointed legal representative, carries particular significance in the deepfake context. Deepfake dissemination often occurs anonymously or pseudonymously across platforms, and victims may not immediately become aware that a fabricated video exists, particularly where it circulates within closed groups or foreign-hosted platforms before surfacing publicly. Because the statute of limitations and procedural clock for a complaint offence generally runs from the point the victim becomes aware of the offence and the identity of the offender, the delayed-discovery character of deepfake harm interacts awkwardly with the complaint-offence structure: a victim who only learns of a defamatory deepfake months after its creation, once it resurfaces or is

reported to them by a third party, may face practical uncertainty about whether their complaint remains timely, and in any event must undertake the complaint personally, which can be psychologically and practically burdensome given the intimate nature of much deepfake harm.

This structural limitation also means that corporations, government institutions, or collective entities that might be the ostensible target of a deepfake, for example a fabricated video purporting to show a corporate executive making defamatory statements about a company's own affairs, cannot rely on Article 27A in their own right, since the Constitutional Court has confined "other person" to natural persons. In such cases, liability, if it exists, must be reconstructed through the individual executive's personal complaint, through Article 35's falsification framework, or through civil remedies outside the criminal law altogether.

Attribution, Evidentiary, and Cross-Border Obstacles

Beyond the substantive elements of the offences discussed above, this study identifies three recurring practical obstacles to enforcing criminal liability for deepfake-based defamation. The first is attribution: because deepfake generation tools are widely distributed and often used through cloud-based or decentralised platforms, and because the resulting file can be re-uploaded, re-encoded, or stripped of metadata by intermediate distributors, establishing which specific person created the original synthetic content, as distinct from merely redistributing it, presents a significant evidentiary burden. Indonesian criminal procedure permits electronic evidence to be admitted under the UU ITE's evidentiary provisions, but digital forensic capacity to trace the provenance of AI-generated media, including model fingerprinting and metadata reconstruction, remains unevenly developed across Indonesian law enforcement institutions.

The second obstacle concerns the boundary between original creator and disseminator. Article 27A's language, focused on the act of attacking honour with intent for public disclosure, can in principle reach both the original fabricator and any subsequent person who redistributes the deepfake with the same defamatory intent, since the provision does not require that the disseminator be the original author of the content. This creates a broad potential pool of criminally liable parties, extending accountability to viral resharing, but simultaneously raises proportionality concerns where a casual resharer lacked full awareness that the content was fabricated, underscoring the continuing importance of proving subjective knowledge and intent at each link in the distribution chain rather than treating the technological ease of resharing as a substitute for *mens rea*.

The third obstacle is jurisdictional. Deepfake creation tools, hosting platforms, and even the perpetrators themselves may be located outside Indonesian territory, while the harmful effect is felt by a victim within Indonesia. Although the UU ITE contains an extraterritorial

jurisdiction clause allowing its application to acts committed outside Indonesia that produce legal consequences within the country, the practical capacity to secure evidence, compel platform cooperation, or extradite a foreign-based perpetrator remains constrained by the absence of comprehensive mutual legal assistance arrangements specific to AI-generated content, and by the differing legal treatment of deepfakes across jurisdictions.

Interface with the Personal Data Protection Law and the Forthcoming Penal Code

The analysis above concerns liability once a deepfake has been disseminated. An earlier point of intervention exists under the Personal Data Protection Law, since the unauthorised use of a victim's facial image or voice sample to train or prompt a generative model may itself constitute unlawful processing of personal data under Article 65 of the UU PDP, independent of whether the resulting content is ultimately used defamatorily. This provides a potentially valuable preventive charge, allowing intervention at the data-collection stage before reputational harm materialises, though its practical utility depends on victims or investigators becoming aware of the unauthorised data use before the defamatory content is disseminated, which is not always feasible.

Looking forward, the impending entry into force of the new Penal Code in 2026 will introduce a further layer of complexity. Because the new Penal Code's defamation provisions in Articles 433 and 441 will operate alongside the UU ITE's Article 27A, Indonesian courts and prosecutors will need to resolve whether the UU ITE continues to function as *lex specialis* for electronically committed defamation, consistent with its historical role since 2008, or whether the more recently enacted and more comprehensively drafted new Penal Code assumes that role for offences committed after its commencement. This study suggests that, absent an express repeal or harmonising amendment, the *lex specialis derogat legi generali* principle should continue to favour the UU ITE for electronically disseminated deepfake content, given that the UU ITE contains provisions, such as Article 35, specifically tailored to electronic document manipulation that the general Penal Code does not replicate in equivalent technical detail.

Toward a Coherent Liability Framework

Synthesising the foregoing analysis, this study proposes that criminal liability for deepfake-based defamation under current Indonesian law is best understood as a layered structure rather than a single offence. At its core lies Article 27A, protecting individual honour and good name, subject to the complaint-offence limitation and the requirement of proven defamatory intent. Article 35 supplies a falsification-based layer addressing the technical act of generating deceptive synthetic content, carrying substantially heavier sanctions and not requiring victim complaint. Article 27 paragraph (1) supplies a decency-based layer where the

content is sexual or indecent in nature. The Personal Data Protection Law supplies a preventive, data-processing-based layer addressing unauthorised use of the victim's likeness at the point of content creation. Taken together, these provisions offer meaningful, if imperfect, coverage of deepfake-based defamation, but the analysis reveals that none of them was designed with the specific evidentiary and technical features of generative AI in mind, and prosecutors and courts are consequently required to stretch general concepts of manipulation, authenticity, and intent to accommodate a technology whose defining characteristic is the erosion of the very distinction between authentic and fabricated media that these provisions presuppose. This gap supports the case for a targeted legislative clarification, whether through an explanatory regulation, a Supreme Court circular guiding uniform charging practice, or a further statutory amendment, that expressly addresses synthetic and AI-manipulated media within the electronic transactions legal framework, including clearer rules on the liability of original creators versus disseminators, the treatment of labelled satire and parody, and coordinated procedures between the UU ITE, the UU PDP, and the forthcoming new Penal Code.

Platform Intermediary Position and Notice-and-Takedown Practice

Although this article's focus is the criminal liability of the individual who creates or disseminates a defamatory deepfake, no analysis of enforcement in practice is complete without acknowledging the role of the electronic system provider through which the content is circulated. Indonesian regulation of electronic system providers, principally under Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and its implementing ministerial regulations, establishes a notice-and-takedown mechanism whereby a provider that receives a valid government or court order, or in some cases a substantiated report, is expected to restrict access to unlawful content, including content that violates the decency and defamation provisions of the UU ITE. Platform intermediaries are not, under the prevailing framework, treated as criminally liable for user-generated deepfake content absent their own intentional participation in its creation or dissemination, consistent with a conditional immunity model common in comparative internet law. This division of labour means that, in practice, rapid removal of a viral defamatory deepfake often depends more on administrative takedown procedures than on the pace of criminal investigation, and that criminal liability analysis of the kind undertaken in this article addresses accountability and punishment after the fact rather than the immediate mitigation of ongoing reputational harm. The two tracks are complementary: administrative takedown reduces

continuing exposure while criminal process establishes individual accountability, and effective victim protection in practice typically requires pursuing both simultaneously.

Balancing Enforcement with Freedom of Expression

A recurring concern in Indonesian public discourse concerning Article 27A and its predecessor Article 27 paragraph (3) is the risk that a broadly worded defamation offence functions as a "rubber article" (pasal karet) susceptible to strategic use against critics, journalists, and civil society actors rather than only against genuine bad-faith fabrication. This concern is not unique to deepfake cases, but it is arguably intensified where the underlying content is a synthetic video, because the same technology that enables malicious fabrication also enables legitimate satirical, artistic, and journalistic uses, such as clearly labelled parody of public figures or dramatized recreations used in investigative reporting. The Constitutional Court's clarification that criticism, oversight, and commentary directed at matters of public interest fall outside the scope of Article 27A provides an important interpretive safeguard, but its practical value for deepfake content depends on courts developing clear, technology-aware criteria for distinguishing labelled satire from content designed to deceive. This study suggests that relevant criteria should include whether the content carries an express and reasonably prominent disclaimer of its fictional or synthetic nature, whether the manner of presentation and distribution context would lead a reasonable viewer to believe the content depicts an actual event, and whether the creator took affirmative steps to represent the content as authentic, such as removing metadata or watermarks that would otherwise signal manipulation. Embedding such criteria into prosecutorial guidelines or judicial practice would help ensure that the criminal law reaches genuinely defamatory fabrication without chilling legitimate expressive use of an increasingly ubiquitous creative technology.

CONCLUSION

Criminal liability for the misuse of deepfake videos in the commission of defamation under Indonesian law is not governed by a single, purpose-built provision but emerges from the combined and sometimes overlapping application of several norms within the Electronic Information and Transactions Law, principally Article 27A on electronic defamation and Article 35 on the manipulation of electronic documents, supplemented where relevant by Article 27 paragraph (1) on indecent content and by the Personal Data Protection Law's prohibition on unlawful use of personal data. This study finds that the elements of these provisions can, through careful legal interpretation, be extended to cover the technical realities of deepfake production and dissemination: a deepfake video readily satisfies the technical

definitions of an electronic document and of manipulated or fabricated content, and its use to make a false accusation intended for public knowledge readily satisfies the objective elements of electronic defamation. The principal difficulties lie not in the objective elements but in proving subjective intent across a multi-actor, multi-step production and distribution chain, in the delik aduan structure of Article 27A which places the burden of initiating prosecution squarely on the individual victim, and in cross-border evidentiary and jurisdictional constraints that are amplified by the international and often anonymous character of deepfake technology and distribution.

These findings support two complementary recommendations. First, in the near term, law enforcement and judicial practice should adopt a consistent interpretive approach that treats Article 35 and Article 27A as cumulative rather than mutually exclusive charges in deepfake-based defamation cases, thereby capturing both the falsification harm and the reputational harm within a single prosecution, and should invest in digital forensic capacity specific to the detection and provenance-tracing of AI-generated media. Second, in the longer term, legislators should consider a targeted amendment or implementing regulation that explicitly defines synthetic and AI-manipulated media within the electronic transactions legal framework, clarifies the liability of original creators as distinct from subsequent disseminators, protects clearly labelled satire and parody from prosecution, and harmonises the relationship between the UU ITE, the Personal Data Protection Law, and the new Penal Code once the latter takes effect. Such measures would strengthen legal certainty for both prosecutors seeking to hold perpetrators accountable and for individuals seeking to understand the boundaries of lawful creative and expressive use of increasingly accessible generative AI technology.

REFERENCES

- Barda Nawawi Arief. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: Rajawali Pers.
- Grafonomi. "Pemalsuan Digital dalam UU ITE: Apa Sanksinya?" grafonomi.id.
- Hukumonline. "Perubahan Penting Soal Pencemaran Nama Baik di UU ITE Baru." hukumonline.com, 17 Januari 2024.
- IMM DIY. "Pasal 27A UU Nomor 1 Tahun 2024: Menggugat Kriminalisasi Pencemaran Nama Baik di Era Post Truth." immdiy.or.id.
- Jerkin: Journal of Election, Legal, and Constitutional Studies. "Penerapan Asas Lex Specialis dalam Kasus Penipuan Elektronik."
- Jurnal Lex Administratum. Kasenda, D. "Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial Ditinjau Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik." Vol. XII, No. 5.

- Jurnal Reformasi Hukum: Cogito Ergo Sum. "Penerapan UU ITE dalam Penegakan Hukum terhadap Manipulasi Dokumen Elektronik." Volume 7, Nomor 2, Juli 2024, hlm. 17-22.
- Jurnal Relasi Publik. Dima, Adrianus D. "Pertanggungjawaban Pidana Pencemaran Nama Baik." Vol. 2, No. 3, Agustus.
- Klaussa. "Analisis Hukum terhadap Deepfake untuk Konten Negatif." klaussa.com.
- LBH Pengayoman Universitas Katolik Parahyangan. "Kapan Memalsukan Tanda Tangan Bisa Dipidana?" lbhpengayoman.unpar.ac.id.
- Locus: Jurnal Konsep Ilmu Hukum. "Kajian Penerapan Pasal 27A Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik." Locus Journal of Academic Literature Review, 4(7), 546-552.
- Mahkamah Konstitusi Republik Indonesia. "MK Mempertegas Pemaknaan Unsur-Unsur Pencemaran Nama Baik dalam UU ITE." Siaran Pers Mahkamah Konstitusi, mkri.id.
- Moeljatno. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.
- Munir. "Kajian Pasal 27A Undang-Undang Nomor 1 Tahun 2024." Jurnal Hukum, No. 2.
- Recidive: Jurnal Hukum Pidana. "Tinjauan Yuridis terhadap Tindak Pidana Manipulasi Dokumen Elektronik." Universitas Sebelas Maret, kajian atas Putusan Nomor 155/Pid.Sus/2018/PN Cbn.
- Republik Indonesia. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842).
- Republik Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905).
- Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).
- Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).
- Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).
- SIP Law Firm. "Penegakan Hukum Pidana atas Konten Deepfake." siplawfirm.id.
- SIP Law Firm. "Pertanggungjawaban Pidana Korporasi terhadap Pemalsuan Dokumen Elektronik." siplawfirm.id.
- Soekanto, Soerjono, dan Sri Mamudji. Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: Rajawali Pers.
- Soesilo, R. Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal. Bogor: Politeia.
- UNES Journal of Swara Justisia. "Tinjauan Yuridis Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial." Volume 7, Issue 3, Oktober 2023.

Wardata, Aulia. Pencemaran Nama Baik oleh Deepfake Artificial Intelligence sebagai Tindak Pidana Berdasarkan KUHP dan Undang-Undang Informasi dan Transaksi Elektronik. Skripsi/Repositori Digital, Universitas Lambung Mangkurat, 2024.

Wetboek van Strafrecht (Kitab Undang-Undang Hukum Pidana), Staatsblad 1915 Nomor 732, sebagaimana berlaku sebagai hukum positif di Indonesia.