Law Development Journal
SINTA 2 Degree No. 0228/DTS/C3/DT.05.00/2026
ISSN: 2747-2604
Volume 8 No. 3, 2026

Legal Liability of Digital Platforms for Disseminating Deepfake Content that Violates Victims' Privacy and Reputation Rights

Yanto Irianto [1)], Semuel Haning [2)], Rudi Afianto [3)], Hadi Supriyanto [4)], Vegitya Ramadhani Putri [5)]

[1)] Universitas Nahdatul Ulama Cirebon, E-mail: yantoirianto755@gmail.com
[2)] Universitas Persatuan Guru 1945 NTT, E-mail: semuel94891@gmail.com
[3)] Universitas padjadjaran Bandung, E-mail: Rudiafia81@gmail.com
[4)] Universitas Muhammadiyah Buton, E-mail: hadisupriyanto@umbuton.ac.id
[5)] Universitas Sriwijaya, E-mail: vegityaramadhani@fh.unsri.ac.id

Abstract: *Indonesian digital platforms cannot yet be held clearly liable for spreading deepfake content that violates victims' privacy and reputation, because platform duties are scattered across several regulations and no deepfake-specific norm exists. Using library research with statutory, conceptual, and comparative approaches, this article analyses the legal basis, forms, and limits of platform liability as electronic system operators (PSE). It finds that the Electronic Information and Transactions Law (Law 1/2024), the Personal Data Protection Law (Law 27/2022), Government Regulation 71/2019, and Ministerial Regulation 5/2020 give a basis for platform duties, chiefly takedown and the operation of reliable and secure systems, but sanctions remain mostly administrative. Civil liability under Article 1365 of the Civil Code and corporate criminal liability still depend on proving negligence without a defined duty of care. Comparison with the United States (TAKE IT DOWN Act), the European Union (DSA and AI Act), and South Korea points toward rules that combine fixed takedown deadlines, transparency duties, and enforceable sanctions. The article recommends deepfake-specific platform duties: notice-and-action with clear deadlines, labelling of synthetic content, re-upload prevention, and victim remedies.*

Keywords: *Deepfake; Digital; Electronic; Privacy; Reputation.*

1. Introduction

Deepfakes are artificial intelligence-based synthetic media that mimic a person's face, voice, or movements so that they appear authentic. Chesney and Citron (2019) place it as a threat to privacy, democracy, and national security, because high realism makes it difficult for victims to prove that the content is fake. For individual victims, the disadvantages are concrete: their faces are attached to sexual content, or speech they have never spoken is made as if they are real. Citron (2019) calls this pattern a violation of *sexual privacy*, which is the deprivation of a person's control over their body and intimate image.

In Indonesia, the spread of deepfakes takes place almost entirely through social media platforms and short video services. Content creators are often anonymous or outside the jurisdiction, whereas platforms are known parties, are legal entities, have technical control over distribution, and profit from users' attention. The legal debate therefore shifts from "who is the creator" to "what are the platform's obligations". The case of the image maker feature on AI Grok on platform X in early 2026 shows that shift: (Indonesia, 1945)reported that its ability to manipulate photos into fake pornographic content was considered an offence and put the platform at risk of being blocked by Komdigi.

Indonesia's positive law does not yet have a norm that explicitly mentions deepfakes. (KUHPerdata, n.d.) concluded that the ITE Law, PP 71/2019, and the PDP Law can be used as a basis for assessing platform obligations through systematic interpretation, but have not yet established the liability of platforms that neglect to prevent the spread of deepfakes. The criminal provisions in the ITE Law target more perpetrators, not system operators. The Presidential Regulation on the ethics of artificial intelligence prepared by Komdigi has also not yet been issued; (Indonesia, 2024) is still reporting it awaiting the President's signature.

In the meantime some jurisdictions are already moving. The United States requires platforms to degrade nonconsensual intimate images, including AI-generated ones, within 48 hours of the lawful notification (Indonesia, 2022). The European Union imposes deepfake transparency obligations in Article 50 of the AI Act from 2 August 2026 (Indonesia, 2022) This gap makes the study of platform responsibilities in Indonesia urgent and worth comparing.

B. Problem Formulation

1. How is Indonesia's positive legal arrangement on the obligations and accountability of digital platforms against the spread of deepfake content that violates the privacy and reputation rights of victims?

2. What are the forms and limits of the platform's legal liability (administrative, civil, and criminal) as well as the weaknesses of existing norms?

3. How can the experience of the United States, the European Union, and South Korea serve as a reference for strengthening the regulation in Indonesia?

C. Objectives and Contributions

This article aims to map the legal basis of platform liability, assess the adequacy of sanctions and victim recovery mechanisms, and formulate a more decisive regulatory direction. The contribution is to an integrated reading of the ITE Law, the PDP Law, the National Criminal Code, and implementing regulations from the perspective of platform responsibility, while most previous studies focused on criminal responsibility of perpetrators.

2. Research Methods

This research is a normative legal research that uses the library *research method*, which

is the tracing and processing of data from written materials without collecting field data(Indonesia, 2022). All data comes from documents, not from interviews or surveys.

A. Approach

The research uses three approaches(Indonesia, 2023):

1. A legislative approach, to examine the norms that govern PSE obligations, personal data protection, and criminal related to electronic content.

2. Conceptual approach, to explain the concept of deepfakes, the right to privacy, the right to reputation, and *intermediary liability*.

3. The comparative approach, against the United States, the European Union, and South Korea, was chosen because each represents a different model of platform regulation.

B. Legal Materials and Collection Techniques

Material type	Contents	How to obtain
First	1945 Constitution; Law 1/2024 (second amendment to the ITE Law); Law 27/2022 (PDP); Law 12/2022 (TPKS); Law 1/2023 (Criminal Code) and Law 1/2026; PP 71/2019; Permenkominfo 5/2020 jo. 10/2021; Civil Code; TAKE IT DOWN Act 2025; DSA; AI Act (Regulation 2024/1689)	Search for regulations in official databases and authority websites, and then match them with legal reviews
Seconds	Journal articles, preprints, theses, and theses on deepfakes and PSE liability; legal opinions and reviews	Online searches with keywords "deepfake", "platform liability", "PSE", and "intermediary liability"
Tertiary	Legal news, official ministry broadcasts, regulatory guidance (FTC), and law firm summaries	Search online for the latest developments until October 28, 2026

Data collection follows the stages of literature research: compiling a bibliography of work, reading, and taking notes (Indonesia, 2019)

C. Analysis and Limitations

The material is analyzed qualitatively prescriptively with systematic and grammatical interpretation: the norm is placed in a broader legal system, and then it is tested whether the norm can accommodate the problem of deepfakes. Limitations of the research: (1) there is no court ruling that specifically decides the platform's responsibility for deepfakes in the material that has been successfully collected; (2) some secondary sources in the form of preprints or theses that have not gone through peer review; (3) regulations that are still in process, such as the Presidential Regulation on artificial intelligence, are only discussed based on news; and (4) the article number and provisions need to be re-verified in the official database (JDIH) before the manuscript is submitted to the journal.

Law Development Journal
SINTA 2 Degree No. 0228/DTS/C3/DT.05.00/2026
ISSN: 2747-2604
Volume 8 No. 3, 2026

3. Results and Discussion

A. Conceptual Framework

1. Privacy and reputation as rights violated by deepfakes. The modern idea of privacy originated from Warren and Brandeis' (1890) formulation of the *right to be left alone*. Deepfakes shift the problem: content no longer reveals true personal facts, but produces false "facts" that use the victim's biometric identity. The violations are multi-layered. The use of faces or voices without consent violates privacy and personal data, while its dissemination in public spaces damages honor and reputation. In Indonesian law, these two interests are based on Article 28G paragraph (1) of the 1945 Constitution, which guarantees personal protection, honor, and dignity. (Indonesia, 2021)noted that the impact of deepfakes on victims includes damage to the image in society and loss of a sense of security, not just material losses.

2. Three models of intermediary liability.

The platform governance literature (Indonesia, 2024)distinguishes three approaches to *intermediary liability*:

Models	Principle	Consequences for deepfake victims
Broad immunity	The platform is not responsible for third-party content	Victims can only sue the often anonymous creator
Conditional exemption (*safe harbour*)	The platform is free of liability during the content downgrade after being notified	There is a recovery path, but it depends on the speed and clarity of the procedure
Active responsibility (*duty of care*)	Platforms must prevent and assess risks, not just react	The strongest protection, with the risk of expression restriction and the burden of moderation costs

(United States, 2025) states that platforms generally take refuge behind the *safe harbor* principle with a *notice and take down mechanism*, but the responsibility becomes heavier when platforms provide generative AI tools that can directly generate illegal content. There are three arguments: platforms act as technology facilitators, are bound by the principle of prudence according to PP 71/2019, and can be sued as providers of products that cause losses. The difference between platforms that only *host* content and platforms that *provide* deepfake tools are used in this article as a differentiator between the level of liability(European Union, 2022).

B. Indonesia's Positive Legal Foundations

There is not a single article that mentions deepfakes. The obligations of the platform must be assembled from several regulations, as seen below.

Conditions	Tree contents	Relevance to the platform
Article 28G paragraph (1) of the 1945 Constitution	Right to personal protection, honour and dignity	The constitutional basis of the obligation of the state and the system to protect victims

Article 15 of the ITE Law	PSE organizes an electronic system that is reliable, safe, and responsible for the operation of the system	General liability basis; liability may be excluded if the fault is on the user's side or compelling circumstances
Article 26 paragraph (1) of the ITE Law	The use of information about personal data through electronic media requires the consent of the person concerned	The basis of the victim's right to stop the use of his image
Article 27 paragraph (1) jo. Article 45 paragraph (1) of the ITE Law	Prohibition of disseminating content that violates morality; criminal penalty of up to 6 years and/or a fine of IDR 1 billion (SIP Law Firm)	Making sexual deepfakes prohibited information that platforms must take down
Article 27A jo. Article 45 paragraph (4) of the ITE Law	Attack on honor or good name through electronic information (Nidal & Multazam, 2026)	The basis of deepfakes that damage reputation
Article 40 paragraph (2a), Article 40A paragraph (2)–(3), and Article 43 letter i of the ITE Law	The government prevents the dissemination of unlawful content and can order the PSE to cut off access; the PSE is obliged to carry out the order (Business, 2025; NU Online)	Obligation to take down content after a government order
PP 71/2019	PSEs are required to be registered, maintain a reliable and secure system, and provide a mechanism for the deletion of information upon request (Hukumonline, 2024)	Administrative basis and governance obligations
Permenkominfo 5/2020 jo. 10/2021	Private PSEs are prohibited from containing prohibited information (Article 9) and must cut off access: 1x24 hours after official request, 4 hours for urgent matters (IDX Channel); administrative fines if they are negligent (SmartLegal)	The only explicit content removal deadline in Indonesian law
Law 27/2022 (PDP)	Biometrics are specific personal data (Article 4 paragraph 2 letter b); criminal forgery of personal data up to 6 years and/or IDR 6 billion (Hukumonline, 2022)	The victim's face and voice are protected; the platform as a data controller is bound by the rights of the data subject and administrative sanctions
Law 12/2022 (TPKS) Article 14	Electronic-based sexual violence, including the dissemination of sexual content without consent	Criminal basis and recovery of victims of sexual deepfakes (Qothrunnada, 2025)
Law 1/2023 (KUHP) jo. Law 1/2026	Effective from 2 January 2026 (Hukumonline; Bundle, 2026); Recognizing corporations as criminal subjects	Opening corporate criminal channels for platforms, with strict evidentiary requirements

The table shows two patterns. First, criminals target perpetrators (creators and dissepers), while platforms only face administrative obligations: cutting off access, maintaining a reliable system, and complying with the rights of data subjects. Second, the obligation to take down content is *reactive*. It depends on official requests or government orders, and there is no obligation to detect, tag, or prevent deepfake reuploads(European Union, 2024). Nidal and Multazam (2026) came to a similar conclusion: the provisions of the ITE Law focus more on perpetrators and have not yet strictly regulated the platform's preventive obligations.

C. Form and Limit of Platform Liability

1. Administrative liability. This is the form that is most ready to be implemented. Platforms that do not cut off access to content are prohibited from being subject to administrative fines, and their implementation is directed through the Moderation Compliance System based on the Decree of the Minister of Communication and Informatics 522/2024; the fine becomes non-tax state revenue (Ariwibowo et al., 2026). On the other hand, Permenkominfo 5/2020 opens the possibility of PSEs being exempted from responsibility for prohibited content if they manage information and reporting systems and meet the moderation requirements. (Chesney & Citron, 2019)criticized the formulation of "can be liberated" because it does not provide certainty for the platform. Thus, Indonesia actually already has an initial form *safe harbour* conditional, but the terms are vague. The PDP Law adds administrative sanctions for platforms as controllers of personal data, including termination of data processing and deletion, as well as administrative fines.

At the same time, civil society organizations such as (Citron, 2019)and SAFEnet consider that categories of information are banned, especially those that "disturb society", are too flexible and risk limiting freedom of expression. Strengthening platforms' obligations on deepfakes should therefore limit themselves to content that clearly violates the rights of victims, rather than expanding categories that have been criticized.

2. Civil liability. The civil route is based on unlawful acts (Article 1365 of the Civil Code), which requires acts, unlawful nature, faults, losses, and causal relationships. (Gorwa et al., 2020)concluded that the article can be applied progressively to deepfake creators and spreaders, and that platforms can be held liable if they neglect to carry out supervision and moderation, with the ITE Law and the PDP Law serving as special provisions. Article 38 of the ITE Law provides a basis for lawsuits against electronic system operators who cause losses, and the PDP Law gives data subjects the right to sue and receive compensation for their data processing violations (Article 12).

Constructively, the negligence of the platform can be distinguished according to its role:

Platform roles	The birthplace of error	Evidence the victim needs
Hosting user content	Continue to display content after receiving a valid notification, or exceeding the deadline of Permenkominfo 5/2020	Proof of reporting, time of receipt, and content that remains live
Algorithmically distributing	Recommend or strengthen the reach of content that has already been reported	Reach data; often only powered by the platform
Setting up a deepfake maker tool	Not installing reasonable filters for foreseeable abuse	Proof of features and ease of abuse

The main difficulty lies in proof. Victims rarely have access to the platform's internal data, while a reasonable standard of prudence has not been formulated in any regulation. Without that standard, judges would have to assess themselves on a case-by-case basis. In the material compiled by this study, no verdict was found that decided the platform's civil liability for deepfakes.

3. Criminal liability. The National Criminal Code recognizes corporations as criminal

subjects, so in theory legal entity platforms can be held accountable. However, relevant provisions, such as Article 27 paragraph (1) and Article 27A of the ITE Law, require intentionality. Platforms that merely accommodate difficult content are considered to have the intention of spreading deepfakes. Ignorance after receiving a clear notification can be considered a form of intentionality, but this construction has not been tested. Corporate crime is therefore more appropriately positioned as the last resort (*ultimum remedium*), while the main burden remains on administrative sanctions and civil lawsuits.

D. Weaknesses of Existing Norms

4. **There is no definition of deepfake or synthetic content.** This void is noted by ("Analisis Tanggung Gugat", 2025), ("Analisis Pertanggungjawaban Perdata", 2025), and (Nidal & Multazam, 2026). Without definition, platforms can argue that there is no special obligation.

5. **The PDP Law does not clearly reach synthetic images.** Perpetrators can create deepfakes from public photos without hacking any data, making it difficult to meet the element of "unlawful acquisition of personal data" (Hafiduddin, 2026)Teleological interpretations that view faces and voices as biometrics used without a legitimate basis can close some of this gap, but there is no certainty yet.

6. **Content degradation is reactive and relies on the government.** If the platform does not take down its own content, the public must submit an application to the Minister (Qothrunnada, 2025). The victim has no direct rights to the deadlines that bind the platform, and there is no obligation to delete identical copies.

7. **There is no labeling or detection obligation.** Platform policies are very diverse: TikTok and YouTube require the disclosure of AI content under certain conditions, while SnackVideo does not yet have a specific deepfake policy argues that the rule vacuum actually benefits platforms because they do not need to invest in detection systems.

8. **Complementary regulations have not yet been issued.** The Presidential Regulation on the ethics of artificial intelligence which will contain the roles and responsibilities of the parties is still waiting for ratification(Abidin, 2025).

E. Comparison with Other Jurisdictions

Aspects	United States	European Union	South Korea
Instruments	TAKE IT DOWN Act, signed May 19, 2025	The Digital Services Act (DSA) and Article 50 of the AI Act (Regulation 2024/1689)	Revision of the digital sexual crimes law (September 2024) and the Basic AI Act (2026)

Platform obligations	Providing a notification mechanism and degrading nonconsensual intimate images, including AI-made, within 48 hours and attempting to remove identical copies (FTC, 2026)	DSA: mechanism *notice-and-action* and the systemic risk assessment of the platform is very large (Resemble AI). AI Act: providers mark synthetic outputs in a machine-readable manner, and the party spreading the deepfakes is obliged to disclose it (Didi, 2026)	Criminalization of the creation, dissemination, possession, and viewing of sexual deepfakes (Abidin, 2025)
Enforcement and sanctions	FTC; civil fines of up to US$53,088 per violation (FTC, 2026)	DSA: fines of up to 6% of global turnover; AI Act: up to 15 million euros or 3% of turnover	Prison sentence for perpetrators, up to 7 years for makers and spreaders (Abidin, 2025)
Platform protection	Immunity for platforms that delete in good faith even if the content is later deemed legitimate (Latham & Watkins)	Conditional liability exemption in DSA	Not found in the assembled material
Noted weaknesses	Only intimate content; no proactive detection obligation (The Conversation/Yahoo); no civil lawsuit against the platform (C.A. Goldberg)	The AI Act's liability falls on the tools and disclosures, not on the victim's losses (Didi, 2026); the obligation to mark machines for systems already in circulation is postponed until December 2, 2026 (GDPRLocal)	Criticized by human rights activists and industry players for having the potential to suppress innovation (Abidin, 2025)

There are four lessons. First, a definite deadline. The United States chose 48 hours; Indonesia already has 24 hours and 4 hours, but only through an order or plea to the government, not the victim's right to the platform. Second, protection for good-faith removal. Without this protection, platforms tend to delay removal until there is an official order. Third, transparency obligations at the tool level, such as tagging and disclosure in the AI Act, complement downstream approaches that only degrade content. Fourth, there are limits to avoid: the scope is too narrow, there is no right of claim for the victim, and there are no attempts to prevent reuploads.

F. Proposed Arrangement Direction

Based on these findings, platform obligations should be tiered according to roles and scale, so as not to burden small services with obligations that only large platforms can fulfill.

Level	Subject	Core obligations
1	All PSEs that host user content	Easy reporting channels for victims; reduction in 24 hours, and 4 hours for sexual or clearly degrading content; removal of identical copies; notification of decisions and objection lines
2	Large platforms and platforms with algorithmic distribution	Periodic risk assessments; labeling of synthetic content; reasonable efforts to prevent re-uploading of content that has already been taken down; moderation transparency reports
3	Generative AI tool provider	Security since design that prevents the creation of intimate content from photos of real people without consent; machine-readable output tagging

Three complementary elements should be added to the level:

1. Clear exclusion of liability. Platforms that meet their level obligations are not burdened with civil liability for user content, and good-faith deletions are protected. This clarity replaces the phrase "can be exempted" in Permenkominfo 5/2020.

2. Safeguarding freedom of expression. Liability is limited to content that impersonates real identities without consent and violates privacy or reputation; satire and clearly marked works remain protected (compare Section 50 of the AI Act which relaxes forms of disclosure for artistic and satirical works).

3. Victim recovery. The right to sue for compensation, restitution, and assistance, so that the victim does not bear the burden of psychosocial recovery alone, which Qothrunnada (2025) noted as a weakness of the current protection.

The form of the instrument can be gradual. In the short term, the improvement of Permenkominfo 5/2020 and the provisions in the Presidential Regulation on the ethics of artificial intelligence can contain deadlines and labeling obligations. In the medium term, obligations that carry sanctions and the right to sue should be regulated in law, in accordance with the principle that the restriction of rights and the imposition of sanctions require a legal basis.

4. Conclusion

Regulation. Indonesian law has not explicitly regulated deepfakes, but platform obligations can be assembled from the ITE Law (Law 1/2024), the PDP Law, PP 71/2019, Permenkominfo 5/2020, the TPKS Law, and the National Criminal Code. These obligations are centered on the implementation of a reliable and secure system and the termination of access to content is prohibited, and is reactive. Form and limits of liability. Administrative liability is best prepared, with deadlines of 1x24 hours and 4 hours and administrative fines. Civil liability on the basis of Article 1365 of the Civil Code and Article 38 of the ITE Law are available, but depend on proving negligence without a formulated standard of prudence. Corporate criminal liability is hampered by the requirement of intentionality. The main weaknesses are the absence of a definition of synthetic content, the unclear scope of the PDP Law on synthetic images, the absence of direct victims' rights to the platform, and the absence of labeling or re-upload prevention obligations. Comparison. The United States, the European Union, and South Korea chose different instruments, but both affirmed a reduction deadline, transparency obligations, or real sanctions. Their experience also showed risks to avoid: narrow scope, no prevention of reuploads, and no victim redress route.

5. References

Jurnals:

Abidin, M I. “Deepfake Menyebar Cepat, Hukum Bergerak Lambat.” *Hukumonline*, 2025. https://www.hukumonline.com/berita/a/deepfake-menyebar-cepat--hukum-bergerak-lambat-lt68f065103ad53.

"Analisis Pertanggungjawaban Perdata Terhadap Penyalahgunaan Teknologi Artificial Intelligence (Deepfake)." *Rewang Rencang: Jurnal Hukum Lex Generalis* 6, no. 12 (2025). https://www.ojs.rewangrencang.com/index.php/JHLG/article/download/2019/996/9094.

"Analisis Tanggung Gugat Dalam Kasus Deepfake Yang Dihasilkan AI Generatif Berdasarkan KUHPerdata Terkait Kerugian Yang Ditimbulkan." *Jurnal Pustaka Nusantara Multidisiplin (JPNM)* 3, no. 2 (2025). https://repository.unmuhjember.ac.id/30297/.

Ariwibowo, T, Ismaidar, and A Rahman M.S. "Analisis Hukum Pidana Terhadap Penyebaran Deepfake Berbasis Artificial Intelligence (AI) Dalam Perspektif Pembaruan Hukum Pidana Di Indonesia." *Yustisi* 13, no. 2 (2026). https://ejournal.uika-bogor.ac.id/index.php/YUSTISI/article/download/23887/8616/114567.

Chesney, R, and D K Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107 (2019): 1753.

Citron, D K. "Sexual Privacy." *Yale Law Journal* 128 (2019): 1870.

Gorwa, R, R Binns, and C Katzenbach. "Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance." *Big Data & Society* 7, no. 1 (2020). https://doi.org/10.1177/2053951719897945.

Hafiduddin, M. "Hukum Siber Di Era Digital: Rekonstruksi Penanggulangan Kejahatan Deepfake Dalam Perspektif Hukum." *SEIKAT* 5, no. 4 (2026). https://doi.org/10.55681/seikat.v5i4.3370.

Regulations:

Indonesia. Law of the Republic of Indonesia Number 12 of 2022 concerning Sexual Violence Crimes (2022).

Decree of the Minister of Communication and Informatics Number 522 of 2024 concerning Implementation Guidelines for Non-Tax State Revenue (PNBP) Derived from Administrative Fines (2024).

"Civil Code (Burgerlijk Wetboek)," n.d.

Nidal, G. A., and M. T. Multazam. "Legal Liability of Digital Platforms Regarding the Dissemination of Deepfake Content on Short-Video-Based Social Media in Indonesia (Preprint)." Universitas Muhammadiyah Sidoarjo, 2026. https://archive.umsida.ac.id/index.php/archive/preprint/download/12376/89055/98701.

Regulation of the Minister of Communication and Informatics Number 5 of 2020 concerning Private-Sector Electronic System Providers, as amended by

Ministerial Regulation Number 10 of 2021 (2021). Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (2019).

Qothrunnada, A. F. "Criminal Law Protection for Victims of the Misuse of Artificial Intelligence 'Deepfake' Technology for Pornography: A Comparative Study Between Indonesia and China." UIN Sunan Ampel Surabaya, 2025. https://digilib.uinsa.ac.id/id/eprint/88098/.

Regulation (EU) 2022/2065 (Digital Services Act) (2022).

Regulation (EU) 2024/1689 (Artificial Intelligence Act) (2024).

TAKE IT DOWN Act (United States) (2025).

"The 1945 Constitution of the Republic of Indonesia," 1945.

Law Number 1 of 2023 concerning the Criminal Code, along with Law Number 1 of 2026 concerning criminal penalty adjustments (2023).

Law Number 11 of 2008 concerning Information and Electronic Transactions, as amended by Law Number 19 of 2016 and Law Number 1 of 2024 (2024).

Law Number 12 of 2022 concerning Sexual Violence Crimes (2022).

Law Number 27 of 2022 concerning Personal Data Protection (2022).