

Causative-Victim Tracing for Integrative Criminal Policy on AI Deepfake Face and Voice Crimes in Indonesia

Muhammad Abdul Azis^{1*}, Pujiyono²

Faculty of Law, Universitas Diponegoro, Semarang
muhammadabdulazis@students.undip.ac.id

**Corresponding Author*

Article info

Received: 1 Jul 2026

Revised: 7 Aug 2026

Accepted: 10 Aug 2026

DOI: <https://doi.org/10.31599/krtha.v20i2.5666>

Abstract : *This study aims to analyze the weaknesses of Indonesia's criminal law policy in responding to facial and voice AI deepfakes, and to formulate Causative-Victim Tracing as an application of integralistic criminal law policy. The method used is normative juridical research with conceptual, statutory, case, and limited comparative approaches. The findings show that deepfake regulation remains partial because it is fragmented across the Personal Data Protection Law, the Electronic Information and Transactions Law, the Criminal Code, and the Law on Sexual Violence Crimes. These instruments can address certain acts, but they have not yet understood deepfake as a sequence of crime involving biometric data, AI technology, layered actors, platform distribution, digital evidence, and recurring harm to victims. This study offers Causative-Victim Tracing to connect the tracing of data sources, technology, actors, platforms, and evidentiary obstacles with the mapping of victims, forms of harm, protection, and recovery from the earliest stage.*

Keywords : *AI deepfake, Causative-Victim Tracing, integralistic criminal law, biometric identity, victim protection.*

Abstrak : Penelitian ini bertujuan menganalisis kelemahan kebijakan hukum pidana Indonesia dalam merespons AI deepfake wajah dan suara, serta merumuskan Causative-Victim Tracing sebagai penerapan kebijakan integralistik hukum pidana. Metode yang digunakan adalah yuridis normatif dengan pendekatan konseptual, perundang-undangan, kasus, dan komparatif terbatas. Hasil penelitian menunjukkan bahwa pengaturan deepfake masih parsial karena tersebar dalam UU Pelindungan Data Pribadi, UU ITE, KUHP, dan UU Tindak Pidana Kekerasan Seksual. Instrumen tersebut dapat menjangkau sebagian perbuatan, tetapi belum membaca deepfake sebagai rangkaian kejahatan yang melibatkan data biometrik, teknologi AI, aktor berlapis, distribusi platform, pembuktian digital, dan kerugian korban yang berulang. Penelitian ini menawarkan Causative-Victim Tracing untuk menghubungkan penelusuran sumber data, teknologi, aktor, platform, dan hambatan pembuktian dengan pemetaan korban, bentuk kerugian, perlindungan, dan pemulihan sejak tahap awal.



Kata kunci : AI deepfake, Causative-Victim Tracing, hukum pidana integralistik, identitas biometrik, perlindungan korban.

Introduction

The development of artificial intelligence (AI) deepfakes involving faces and voices shows a shift in digital crime from falsification of information toward the appropriation of human identity representation.¹ Faces and voices are not merely audiovisual data; they function as biometric markers attached to a person's identity. Their use through generative technology without consent can undermine reputation, dignity, personal security, and individual control over digital representation.² These characteristics mean that deepfakes cannot be adequately understood merely as hoaxes, manipulated content, or digital fraud because their effects also extend to the integrity of personal identity and public trust in audiovisual evidence.³

Indonesian law already has several instruments that can reach certain forms of deepfake. The Personal Data Protection Law regulates biometric data as specific personal data and prohibits the unlawful acquisition, use, disclosure, and falsification of personal data.⁴ The Electronic Information and Transactions Law prohibits the manipulation of electronic information so that it appears to be authentic data.⁵ The Criminal Code can be used when deepfake causes fraud, defamation, extortion, or other harm under general offenses.⁶ The Law on Sexual Violence Crimes can also reach sexually explicit deepfakes through provisions on electronic-based sexual violence.⁷ These legal entry points provide a basis for enforcement, although their application remains dependent on the distinct elements required under each legal regime.

The limits of these provisions become apparent in the deepfake case involving East Java Governor Khofifah Indar Parawansa. The perpetrators manipulated Khofifah's video using AI, uploaded it through TikTok, directed victims to WhatsApp, and offered cheap motorcycles priced at IDR 500,000. The police

¹ Felipe Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content," *International Review of Law, Computers and Technology* 39, no. 2 (2024): 1–30, <https://doi.org/10.1080/13600869.2024.2324540>.

² Riski Ananda Kusuma Putri. Muhammad Abdul Azis, Nur Rahman, "Between The Future Or Just Utopia: A Critical Analysis Of The Legal Personhood Of Artificial Intelligence On The Claim As A Patent Inventor," *Journal Critical Legal Review* 2, no. 1 (2025): 58–83; Angelica Vanessa Audrey Nasution, Suteki, and Anggita Doramia Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse," *International Journal for the Semiotics of Law* 38 (2025): 2489–2517, <https://doi.org/10.1007/s11196-025-10265-0>.

³ Kristof Meding and Christoph Sorge, "What Constitutes a Deep Fake? The Blurry Line between Legitimate Processing and Manipulation under the EU AI Act," in *Proceedings of the 2025 Symposium on Computer Science and Law*, 2025, 152–59, <https://doi.org/10.1145/3709025.3712218>.

⁴ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi", arts. 4, 65, 66..

⁵ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik", art. 35.

⁶ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana", arts. 433, 492..

⁷ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual", arts. 4, 14..

stated that there were approximately 100 victims from several provinces and that the perpetrators gained IDR 87,600,000 over three months.⁸ Article 492 of the Criminal Code may address the fraud that induced victims to transfer money,⁹ Article 35 of the Electronic Information and Transactions Law may reach the manipulated video that appeared authentic,¹⁰ and Articles 65 and 66 of the Personal Data Protection Law may apply to the unlawful use of her facial image.¹¹

Nevertheless, this construction separates Khofifah's identity into personal data, manipulated electronic information, and an instrument for obtaining financial gain. The appropriation of a public official's face to construct a synthetic identity is not yet positioned as an independent legal injury. The existing framework also does not specifically differentiate the liability of the video creator, uploader, communication administrator, and fund recipient according to each actor's contribution to the production and distribution chain.

A different limitation appears in the video of President Joko Widodo that circulated as if he were delivering a speech in Mandarin, even though the Ministry of Communication and Informatics stated that the content was a misleading AI-edited video.¹² Article 492 of the Criminal Code is difficult to apply because the video did not induce a transfer of property,¹³ while Article 433 requires an allegation of a particular matter that attacks a person's honor or reputation.¹⁴ A synthetic representation that falsely depicts a person delivering a speech may influence public perception without necessarily satisfying either element. Article 14 of the Law on Sexual Violence Crimes is also inapplicable because the content is not sexual.¹⁵

Article 35 of the Electronic Information and Transactions Law may still reach the act of manipulation, but its normative orientation concerns the authenticity of electronic information rather than the integrity of personal identity and individual control over the use of one's face and voice.¹⁶ Read together, the two cases show that the legal gap does not arise from a complete absence of enforcement provisions, but from the absence of a legal construction that

⁸ Fatichatun Nadhiroh, "Pelaku Penipuan Deepfake Khofifah Raup Untung Rp 87 Juta Selama 3 Bulan," *DetikNews*, July 1, 2025; Divisi Humas Polri, "Polisi Berhasil Menangkap Pelaku Sindikat Penipuan Modus Video Deepfake," *Tributanews*, July 1, 2025.

⁹ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana", art. 492.

¹⁰ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik", art. 35.

¹¹ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi", arts. 4, 65, 66.

¹² Kementerian Komunikasi dan Informatika, "Kominfo Pastikan Konten Presiden Pidato Bahasa Mandarin Disinformasi Menyesatkan," *InfoPublik*, July 1, 2023, <https://infopublik.id/kategori/nasional-sosial-budaya/790958/kominfo-pastikan-konten-presiden-pidato-bahasa-mandarin-disinformasi-menyestakan>.

¹³ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana", art. 492.

¹⁴ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana", art. 433.

¹⁵ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual", arts. 4, 14.

¹⁶ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik", art. 35.

comprehensively addresses non-consensual synthetic impersonation, biometric identity misuse, and layered actor liability.

The insufficiency of positive law is also evident in the absence of an integrated relationship between biometric-data protection, electronic-information authenticity, criminal responsibility, and victim recovery. Existing provisions operate through different protected objects and consequences, while deepfake crimes may unfold through biometric-data acquisition, AI synthesis, cross-platform distribution, private communication, receipt of benefits, and recurring harm. Romero-Moreno explains that deepfakes may produce identity, reputational, emotional, and financial harms.¹⁷ A response based only on the most readily visible consequence risks overlooking the overall structure of the offense and the victim's position.¹⁸

Previous studies in the last five years have discussed deepfake from several perspectives. Romero-Moreno found that deepfake can be used for voter manipulation, extortion, abusive sexual content, misinformation, and emotional and financial harm.¹⁹ Martin showed that the handling of deepfake abuse depends on reporting mechanisms, content removal, and platform responses.²⁰ Nasution, Suteki, and Lumbanraja found that victims of deepfake pornography in Indonesia face obstacles in fulfilling the right to be forgotten due to limited norms, delays in content removal, and weak recovery mechanisms.²¹ These studies have discussed human rights, online safety, and victim protection, but have not connected the causes of crime, actor structure, digital evidence, platform responsibility, and victim recovery within a single criminal law policy framework.

The need for a more integrated framework can be explained through integralistic criminal law policy. Integralistic criminal law policy combines penal measures, non-penal measures, and victim protection. Barda Nawawi Arief places criminal law policy within criminal policy and social policy, requiring crime prevention to connect penal measures, non-penal measures, and victim protection.²² This approach is relevant to deepfake crimes because their occurrence is shaped not only by the offender's intent, but also by the availability of facial and voice data in digital spaces, access to generative technologies, anonymous accounts, weak identity verification, limited

¹⁷ Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content."

¹⁸ Miotti and Wasil, "Combatting Deepfakes: Policies to Address National Security Threats and Rights Violations"; Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, 2023; Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana" (2023); Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.

¹⁹ Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content."

²⁰ Martin, "Online Safety Regulation of Deepfake Abuse: A Case Study on Australia's ESafety Commissioner."

²¹ Nasution, Suteki, and Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse."

²² Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru* (Jakarta: Kencana, 2017), p 6.

platform detection, and the absence of synthetic-content labeling. Tracing these factors enables criminal law policy to move beyond punishment toward identifying the vulnerable points that allow deepfakes to be produced, distributed, and exploited.²³

This direction must be complemented by a victimological approach that positions victims as subjects entitled to protection, recovery, and access to justice. In deepfake crimes, harm does not end when an offender is identified or punished. Content may continue to be downloaded, copied, re-uploaded, and reused, prolonging damage to identity, reputation, psychological wellbeing, and economic interests.²⁴ The legal response must therefore operate from the earliest stage through content removal, identity protection, reputational recovery, evidence preservation, and prevention of redistribution.²⁵ The relationship between tracing causal factors and mapping victims' needs provides the theoretical basis for a policy capable of reading deepfake as a sequence of crime rather than an isolated event ending with a particular offender or consequence.

On this theoretical basis, the research gap in previous studies lies in the absence of an analytical model that links the tracing of the causes of deepfake crimes with victim mapping within the framework of Indonesian criminal law.²⁶ Existing studies still place deepfake as harmful content, a rights violation, sexual abuse, or a normative gap, so they have not yet examined the sequence of acts from the acquisition of biometric data to victim recovery. The novelty of this article lies in the formulation of Causative-Victim Tracing as an application of integralistic criminal law policy, which combines causative tracing to examine data sources, technology, actors, platforms, and evidentiary obstacles with victim tracing to map victims, harm, protection, and recovery.

This study aims to analyze the fragmentation of Indonesia's criminal law policy in responding to facial and voice AI deepfake crimes and to formulate Causative-Victim Tracing as an integralistic criminal law policy framework for addressing such crimes. The analysis addresses two issues: the limitations of Indonesian criminal law in protecting biometric identity, attributing layered liability, authenticating synthetic content, and restoring victims; and the formulation of Causative-Victim Tracing to connect the tracing of causes, actors, technologies, platforms, evidentiary barriers, and victims' recovery needs from the earliest stage.

²³ Andrea Miotti and Akash Wasil, "Combatting Deepfakes: Policies to Address National Security Threats and Rights Violations," *ArXiv*, 2024, <https://doi.org/10.48550/arXiv.2402.09581>.

²⁴ Chesney and Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security."

²⁵ N Martin, "Online Safety Regulation of Deepfake Abuse: A Case Study on Australia's ESafety Commissioner," *Griffith Law Review* 34, no. 1 (2025): 23–46, <https://doi.org/10.1080/10383441.2025.2504791>.

²⁶ Nasution, Suteki, and Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse"; Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content."

Methods

This study uses a normative legal method with conceptual, statutory, case, and limited comparative approaches. The conceptual approach is used to develop the formulation of Causative-Victim Tracing as an application of integralistic criminal law policy to facial and voice AI deepfake crimes. The statutory approach is used to examine the Personal Data Protection Law, the Electronic Information and Transactions Law, the Criminal Code, and the Law on Sexual Violence Crimes, while the case approach is used to analyze deepfake practices in Indonesia. The limited comparative approach is used to examine the direction of deepfake regulation in several other jurisdictions as a reflection on the weaknesses of Indonesian law.

The legal materials in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations related to personal data protection, electronic information, general criminal offenses, and electronic-based sexual violence. Secondary legal materials include books, journal articles, research findings, policy reports, and scholarly publications on deepfake, AI, biometric identity, criminal law policy, victimology, digital evidence, and platform responsibility. Tertiary legal materials are used to clarify technical terms related to deepfake, synthetic content, and generative technology.

Legal materials are collected through library research on laws and regulations, academic literature, reputable journal articles, and official sources concerning deepfake cases in Indonesia. The legal materials are analyzed qualitatively through systematic and conceptual interpretation. Systematic interpretation is used to examine the relationship among fragmented norms, while conceptual interpretation is used to formulate Causative-Victim Tracing as a framework that connects the causa of crime, victim mapping, and recovery needs. The results of the analysis are presented prescriptively to offer directions for reforming Indonesia's criminal law policy on facial and voice AI deepfake crimes.

Result And Discussion

The Fragmentation of Indonesia's Criminal Law Policy in Addressing AI Deepfake Crimes

AI deepfake crimes involving faces and voices indicate a shift in digital crime from data manipulation to the engineering of biometric identity. Through artificial intelligence, a person's face and voice can be synthesized in a way that makes it appear as though the victim is speaking, giving consent, promoting something, or carrying out a particular act.²⁷ This type of attack cannot be understood merely as disinformation, because its impact extends to the authenticity of identity, reputation, dignity, and the victim's sense of security in the digital sphere.²⁸ When synthetic content is used in political

²⁷ M Westerlund, "The Emergence of Deepfake Technology: A Review," *Technology Innovation Management Review* 9, no. 11 (2019): 40–52, <https://doi.org/10.22215/timreview/1282>.

²⁸ R Chesney and D K Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1753–1820, <https://doi.org/Chesney, Robert and Citron, Danielle Keats, Deep Fakes: A Looming>

communication, fraud, or the dissemination of information on social media, the issue becomes broader because public trust in audio-visual evidence is also disrupted.²⁹

This expanded conception of harm provides the basis for assessing Indonesia's fragmented legal response under the Personal Data Protection Law, the Electronic Information and Transactions Law, the Criminal Code, and the Law on Sexual Violence Crimes. The Personal Data Protection Law has indeed provided an initial legal basis because Article 4 paragraph (2) includes "biometric data" as a specific category of personal data, while Articles 65 and 66 prohibit the unlawful acquisition, disclosure, use, and falsification of personal data.³⁰

However, the adequacy of this protection cannot be assessed solely by classifying faces and voices as biometric data. AI deepfake creates a synthetic representation that can falsely attribute speech, conduct, consent, or endorsement to the data subject. The protected legal interest therefore extends beyond the confidentiality and lawful processing of biometric data to the integrity of personal identity and individual autonomy over whether, how, and for what purpose one's face or voice is digitally represented. Personal identity integrity refers to preserving the congruence between a person and the speech, conduct, consent, or endorsement digitally attributed to that person, while autonomy over digital representation concerns the individual's authority to determine whether, how, and for what purposes facial and vocal features may be used to generate synthetic content.³¹ Articles 4 paragraph (2), 65, and 66 of the Personal Data Protection Law may reach unlawful acquisition, disclosure, use, or falsification of biometric data, but they do not expressly construct non-consensual synthetic impersonation as an independent attack on those interests.³²

A similar limitation arises when deepfake is approached through the Electronic Information and Transactions Law and the Criminal Code. Article 35 of the Electronic Information and Transactions Law is relevant because it prohibits any person from intentionally and unlawfully manipulating, creating, altering, deleting, or destroying electronic information or electronic documents with the purpose of making them appear as authentic data.³³ This provision may be used to address content manipulation, but it remains

Challenge for Privacy, Democracy, and National Security (July 14, 2018). 107 California Law Review 1753 (2019), U of Texas Law, Public Law Research Paper No. 692, U of Maryland Legal Studies Research Paper No. 2018-21, Available at SSRN: <https://ssrn.com/abstract=3213954> or <http://dx.doi.org/10.2139/ssrn.3213954>.

²⁹ Cristian Vaccari and Andrew Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," *Social Media + Society* 6, no. 1 (2020): 1–13, <https://doi.org/10.1177/2056305120903408>.

³⁰ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi", arts. 4, 65, 66.

³¹ Mais Qandeel, "Facial Recognition Technology: Regulations, Rights and the Rule of Law," *Frontiers in Big Data* 7 (2024): 1354659, <https://doi.org/10.3389/fdata.2024.1354659>.

³² Ruben Tolosana et al., "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection," *Information Fusion* 64 (2020): 131–48, <https://doi.org/10.1016/j.inffus.2020.06.014>.

³³ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik", art. 35.

centered on the authenticity of electronic information rather than the appropriation of the victim's biometric identity.

Under the Criminal Code, deepfake may be connected to several general offenses, such as Article 492 on fraud, which emphasizes the use of a false name, false capacity, deceitful means, or a series of lies to induce another person to hand over property, provide a debt, acknowledge a debt, or release a claim.³⁴ If deepfake attacks reputation, Article 433 paragraph (1) on defamation may be used because it regulates acts that attack a person's honor or good name by accusing them of something with the intention that it becomes publicly known.³⁵ Nevertheless, fraud, extortion, forgery, and defamation still do not capture the core of deepfake as the creation of a false representation of a person through the synthesis of their face and voice.

The Law on Sexual Violence Crimes provides a more specific legal basis when deepfake is used to attack the victim's body and sexuality. Article 4 paragraph (1) letter i categorizes electronic-based sexual violence as one form of sexual violence crime, while Article 14 paragraph (1) regulates unlawful acts such as recording or capturing sexually explicit images without consent, transmitting sexually explicit electronic information against the recipient's will, and stalking or tracking through electronic systems for sexual purposes.³⁶ This provides a relevant entry point for electronically facilitated sexual harm. Its adequacy for synthetic sexual content remains uncertain, however, because the operative acts of recording, capturing, transmitting, stalking, and tracking do not expressly include generating a fabricated sexual representation through AI. The provision can address specified sexual conduct but does not extend to non-sexual impersonation or other facial and voice deepfakes.

Viewed through their respective protected interests, these provisions address different segments of deepfake harm. The Personal Data Protection Law protects the lawfulness of personal-data processing; Article 35 of the Electronic Information and Transactions Law protects the authenticity of electronic information; Articles 492 and 433 of the Criminal Code protect property and reputation; and Article 14 of the Law on Sexual Violence Crimes protects sexual autonomy against specified electronic conduct. Applied independently, none expressly recognizes unauthorized synthetic attribution as an attack on personal identity integrity and autonomy over digital representation. The gap therefore lies not merely in regulatory dispersion, but in a mismatch between the legal interests currently protected and the composite harm caused by AI-based biometric identity misuse.³⁷

Based on the fragmented regulation under the Electronic Information and Transactions Law, the Personal Data Protection Law, the Criminal Code, and the Law on Sexual Violence Crimes, the determination of deepfake offenses depends heavily on the construction adopted by law enforcement officials. A single incident may be interpreted as manipulation of electronic information,

³⁴ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana", art. 492.

³⁵ Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, art. 433.

³⁶ Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual", arts. 4, 14.

³⁷ Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content."

violation of personal data, fraud, defamation, extortion, or electronic-based sexual violence, depending on the most visible consequence.³⁸ This pattern risks reducing deepfake to merely false content or digital fraud, even though its main harm lies in attacks against the victim's identity and rights in the digital sphere.³⁹

This instability affects criminal liability, because the deepfake process may involve those who collect facial or voice data, users of AI applications, content creators, uploaders, account managers, communication administrators, beneficiaries, and distribution platforms. According to Tolosana, Romero-Tapiador, Fierrez, and Vera-Rodriguez, deepfake arises from layered visual manipulation processes, so an approach that focuses only on the creator or disseminator of the content is insufficient to understand the contribution of other actors who provide the means, expand the reach, or gain benefits from the manipulation of the victim's identity.⁴⁰

This multi-actor pattern can be seen in the deepfake fraud case involving the impersonation of East Java Governor Khofifah Indar Parawansa. The perpetrators did not merely create AI-based videos, but also uploaded the content through TikTok, directed potential victims to WhatsApp, and offered cheap motorcycles priced at IDR 500,000 as if they were part of a public official's program. The police stated that there were three perpetrators with different roles and approximately 100 victims from several provinces.⁴¹ These facts show that deepfake operates through a combination of identity engineering, platform distribution, private communication, and economic gain. If the case is understood merely as ordinary fraud, the dimension of biometric identity impersonation and the layered roles within the digital ecosystem will not be seen comprehensively.

Apart from economic fraud, deepfake may also function as an instrument for manipulating public perception. This can be seen in the video of President Joko Widodo that circulated as if he were delivering a speech in Mandarin. The Ministry of Communication and Informatics stated that the video was identical to Jokowi's speech recording at a USINDO event in 2015, but had been edited using AI technology so that it displayed a narrative that did not correspond to the original event.⁴² This case shows that deepfake is not always aimed at directly obtaining money, but may also create false impressions,

³⁸ Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, art. 35; Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, arts. 4, 65, 66; Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, arts. 433, 492; Republic of Indonesia, Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, arts. 4, 14.

³⁹ Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content."

⁴⁰ Tolosana et al., "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection."

⁴¹ Praditya Fauzi Rahman, "3 Pelaku Penipuan Deepfake Khofifah Ditangkap, Korban 100 Orang," *DetikNews*, July 1, 2025, <https://news.detik.com/berita/d-7892188/3-pelaku-penipuan-deepfake-khofifah-ditangkap-korban-100-orang>.

⁴² Kementerian Komunikasi dan Informatika, "Kominfo Pastikan Konten Presiden Pidato Bahasa Mandarin Disinformasi Menyesatkan."

disrupt public trust, and blur the boundary between authentic recordings and manipulated digital representations.⁴³

These two cases show that the issue of deepfake does not end with the identification of perpetrators, but also extends to evidentiary matters and platform governance. Audio-visual evidence can no longer be assessed merely based on its appearance, because videos or voice recordings that seem convincing still need to be verified through metadata, provenance data, audit trails, file modification history, and digital forensic examination. Meding and Sorge show that the boundary between original content, legitimate edited content, and deepfake becomes increasingly blurred as editing technologies more closely resemble ordinary recording processes.⁴⁴ This condition creates two risks: false content may be accepted as authentic evidence, while authentic content may be denied as deepfake.

This series of weaknesses shows that deepfake needs to be understood as a legal issue that operates from the moment biometric data is obtained, processed through AI systems, formed into synthetic content, and then disseminated through digital platforms. To situate Indonesia's position, comparative references may be directed to three jurisdictions that have regulated deepfake at different points. The European Union regulates it through Regulation (EU) 2024/1689, or the EU AI Act, particularly Article 50, which places deepfake as part of transparency obligations concerning image, audio, or video content generated or manipulated by AI.⁴⁵

California regulates it through Assembly Bill No. 602 of 2019 concerning the use of digital or electronic technology in sexually explicit material without consent, as well as Senate Bill No. 942 of 2024, or the California AI Transparency Act, which regulates transparency obligations for generative system providers.⁴⁶ South Korea regulates it through the Act on Special Cases Concerning the Punishment of Sexual Crimes, particularly in the context of sexual deepfake, as well as the 2024 strengthening that expanded enforcement against the possession, storage, purchase, and viewing of sexual deepfake content.⁴⁷

⁴³ Vaccari and Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News."

⁴⁴ Meding and Sorge, "What Constitutes a Deep Fake? The Blurry Line between Legitimate Processing and Manipulation under the EU AI Act."

⁴⁵ European Union, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence" (2024), <https://artificialintelligenceact.eu/article/50/>.

⁴⁶ California State Legislature, "Senate Bill No. 942, California AI Transparency Act" (2024), https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942; California State Legislature, "Assembly Bill No. 602, Depiction of Individual Using Digital or Electronic Technology Sexually Explicit Material Cause of Action" (2019), https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

⁴⁷ Republic of Korea, "Act on Special Cases Concerning the Punishment of Sexual Crimes" (2026), https://elaw.klri.re.kr/eng_service/lawView.do?hseq=40947&lang=ENG; Hyunsu Yim, "South Korea to Criminalise Watching or Possessing Sexually Explicit Deepfakes," *Reuters*, July 1, 2024, <https://www.reuters.com/world/asia-pacific/south-korea-criminalise-watching-or-possessing-sexually-explicit-deepfakes-2024-09-26/>.

Table 1. Comparison of Deepfake Regulation in Indonesia, the European Union, California, and South Korea

Jurisdiction	Regulatory Instrument	Regulated Object	Regulatory Character
Indonesia	The Electronic Information and Transactions Law, the Personal Data Protection Law, the Criminal Code, and the Law on Sexual Violence Crimes.	Deepfake has not yet been regulated as a specific offense. The act is still connected to electronic information manipulation, misuse of personal data, fraud, defamation, extortion, or electronic-based sexual violence.	The regulation is fragmented and depends on the most visible consequence in each case.
European Union	Regulation (EU) 2024/1689, or the EU AI Act, particularly Article 50.	Image, audio, or video content generated or manipulated by AI, including deepfake.	Emphasizes transparency through disclosure obligations and the marking of synthetic content.
California	Assembly Bill No. 602 of 2019 and Senate Bill No. 942 of 2024, or the California AI Transparency Act.	AB 602 regulates the use of digital or electronic technology in sexually explicit material without consent, while SB 942 regulates the transparency of certain generative systems.	Connects protection against non-consensual sexual deepfake with transparency obligations for generative system providers.
South Korea	Act on Special Cases Concerning the Punishment of Sexual Crimes and the strengthening of criminalization against sexual deepfake in 2024.	Sexual deepfake, including the production, distribution, possession, storage, purchase, and viewing of synthetic sexual content.	Emphasizes criminal enforcement against the circulation chain of sexual deepfake.

The table above shows that Indonesia still places deepfake within a fragmented legal framework, while other jurisdictions have begun to regulate

it more specifically. The European Union emphasizes transparency of synthetic content, California regulates non-consensual sexual deepfake and the transparency of generative systems, while South Korea focuses on enforcement against the circulation chain of sexual deepfake. The comparison indicates that regulatory design can intervene at different stages of the deepfake chain: transparency at generation, consent-based protection at creation, and enforcement against circulation. Indonesia lacks equivalent coordination across these stages. Its principal weakness is therefore not simply the absence of a specific offense, but the absence of a framework aligning biometric identity protection, actor-specific liability, evidentiary duties, platform intervention, and victim remedies.

Accordingly, facial and voice deepfakes should be analyzed as a continuous sequence beginning with biometric-data acquisition, followed by AI synthesis, publication, amplification, and recurring harm. This sequencing allows legal responsibility to be assessed at each stage without collapsing the entire incident into its most visible consequence. It also provides the analytical basis for linking criminal enforcement with evidence preservation, platform action, and victim recovery.

The burden on victims also becomes heavier. Victims not only experience identity misuse, but also face the repeated circulation of content even when the perpetrators have not yet been identified. Victim protection cannot rely solely on criminal proceedings, but must also be accompanied by content removal, identity protection, reputational recovery, psychological support, and guarantees that the victim's biometric data will not be misused again.⁴⁸ For this reason, the next discussion needs to be directed toward a framework that is able to understand deepfake through a more comprehensive reading of the causative chain, criminogenic root causes, actors, technological medium, evidence, platform responsibility, and the victim's position.

Causative-Victim Tracing as an Integralistic Criminal Law Policy Framework for AI Deepfake Crimes

After the weaknesses of Indonesia's criminal law have been mapped, the next issue is no longer merely whether the available legal provisions can reach deepfake, but how criminal law policy should be formulated so that it can operate against a sequence of crime that moves from content creation to harm suffered by victims. Deepfake needs to be understood as the result of the intersection between biometric data, generative systems, digital distribution, and the victim's relational position. A response that relies only on enforcement against perpetrators therefore risks falling behind the speed at which content circulates.⁴⁹

In a study of law and technology, Romero-Moreno emphasizes that deepfake does not only create problems of harmful content, but also attacks privacy,

⁴⁸ D K Citron, "Sexual Privacy," *Yale Law Journal* 128, no. 7 (2019): 1870–1960; C McGlynn and E Rackley, "Image-Based Sexual Abuse," *Oxford Journal of Legal Studies* 37, no. 3 (2017): 534–61, <https://doi.org/10.1093/ojls/gqw033>.

⁴⁹ Tolosana et al., "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection."

reputation, identity, and victims' rights in the digital sphere.⁵⁰ For this reason, the formulation of criminal law policy needs to be directed toward two main tasks, namely tracing the criminogenic roots of the offense and ensuring victim protection from the earliest stage.

At this point, Causative-Victim Tracing can be formulated as the application of an integralistic criminal law policy to AI deepfake crimes involving faces and voices. The theoretical foundation of this framework rests on the concept of integralistic criminal law policy. Barda Nawawi Arief emphasizes that criminal law policy cannot be separated from criminal policy and social policy, so crime prevention needs to combine penal and non-penal measures.⁵¹ This policy formulation therefore consists of two interconnected elements, namely causative tracing and victim tracing.

Causative tracing is based on the criminal etiology approach, which understands crime as the result of interaction among social, technological, economic, and institutional factors, rather than merely as an individual act. In deepfake crimes, the cause does not only lie in the perpetrator's intent, but also in the supporting structure, such as the availability of faces and voices on social media, access to generative applications, weak digital identity verification, limited platform detection, the absence of synthetic content labeling, and the use of fake accounts.⁵² Tracing these factors enables criminal law policy to move from punishment toward the identification of vulnerable points in the production, distribution, and use of deepfake.

Victim tracing is based on victimology and victim-oriented criminal justice. This approach positions victims as subjects who have rights to protection, recovery, and access to justice, rather than merely as sources of information. Deepfake strengthens this need because the harm may continue through downloading, copying, re-uploading, or reusing the content even when the perpetrator has not yet been identified. The impacts may include reputational damage, psychological pressure, economic loss, harassment, threats, and the loss of control over digital identity.⁵³ For this reason, the legal response needs to operate from the earliest stage through content removal, reputational recovery, identity protection, and prevention of redistribution. The formulation of Causative-Victim Tracing can be illustrated as follows.

⁵⁰ Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content."

⁵¹ Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru* (Jakarta: Kencana, 2017), p 6.

⁵² Tolosana et al., "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection"; Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content."

⁵³ Chesney and Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security."

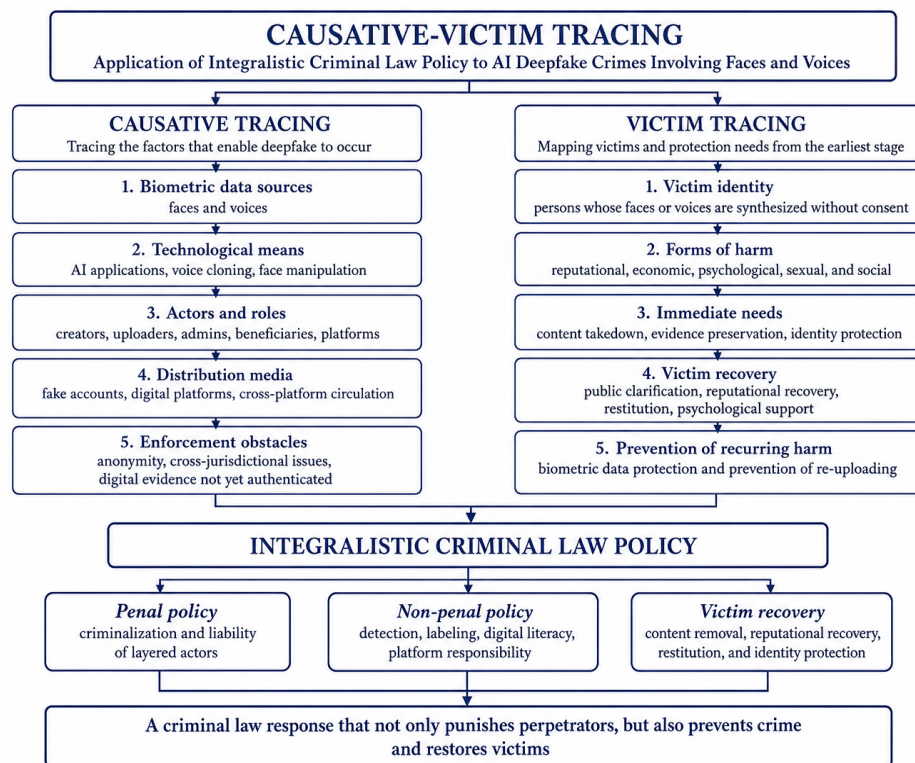


Figure 1. Scheme of Causative-Victim Tracing in Integralistic Criminal Law Policy on AI Deepfake Crimes Involving Faces and Voices

The scheme above shows that Causative-Victim Tracing operates through two parallel elements. Victim protection is not positioned as a subsequent consequence after the perpetrator has been identified, since in deepfake crimes, harm may arise from the moment content is produced, uploaded, copied, and consumed by the public.⁵⁴ Tracing the *causa* remains necessary to understand the origin of biometric data, the AI system used, the uploading account, the distribution medium, the beneficiary, and enforcement obstacles, because deepfake operates through a chain of production and distribution that is not always centered on a single perpetrator.⁵⁵ At the same time, the victim's position needs to be mapped immediately so that identity protection, content removal, evidence preservation, and reputational recovery can be carried out from the earliest stage.⁵⁶

On the side of causative tracing, attention is directed toward the points that enable deepfake to be created and disseminated. Tracing cannot stop at the video creator or content uploader, because the deepfake ecosystem may involve model providers, service providers, end users, distribution platforms, and parties who benefit from manipulative content.⁵⁷ In deepfake fraud cases, the content creator, communication administrator, transfer recipient, account

⁵⁴ Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content"; Arief, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*.

⁵⁵ Miotti and Wasil, "Combatting Deepfakes: Policies to Address National Security Threats and Rights Violations."

⁵⁶ Martin, "Online Safety Regulation of Deepfake Abuse: A Case Study on Australia's ESafety Commissioner."

⁵⁷ Miotti and Wasil, "Combatting Deepfakes: Policies to Address National Security Threats and Rights Violations."

owner, and uploader may be different parties. For this reason, criminal liability needs to be read in layers so that the law does not only reach surface-level perpetrators, but also parties who contribute to the production, distribution, and use of the content.⁵⁸

On the side of victim tracing, attention is directed toward the types of victims and the forms of harm they suffer. Facial and voice deepfakes may create identity victims, economic victims, reputational victims, and social victims when public trust in digital information is also disrupted.⁵⁹ This mapping is important because victims cannot be positioned merely as complainants or sources of information. As long as the content remains in circulation, harm may continue through downloads, re-uploads, comments, digital archives, or the reuse of biometric data.⁶⁰ The study by Umbach, Henry, Beard, and Berryessa shows that non-consensual synthetic intimate imagery produces impacts that are sexual, psychological, social, and relational.⁶¹ For this reason, recovery mechanisms need to include rapid takedown, identity protection, public clarification, psychological support, restitution, and prevention of redistribution.

This scheme also affirms the relationship between Causative-Victim Tracing and integralistic criminal law policy. Penal policy is needed to formulate prohibitions against the misuse of faces and voices through AI without consent, including liability for creators, disseminators, beneficiaries, account managers, and parties who knowingly facilitate dissemination.⁶² Non-penal policy is needed through digital literacy, early detection, synthetic content labeling, platform obligations, and cross-jurisdictional cooperation, because handling deepfake cannot rely solely on responses after content has circulated. Martin shows that complaint and takedown models in online safety regulation have limitations when dealing with deepfake content that spreads rapidly and requires effective platform responses.⁶³ Meanwhile, victim recovery is needed so that the legal process does not end only with punishment, but also restores victims from identity, reputational, economic, psychological, and social harm.⁶⁴

This formulation also preserves the boundary between lawful AI use and unlawful AI use. Visual or voice engineering for parody, education, research, art, or creative production with consent cannot be treated in the same way as deepfake used for fraud, extortion, sexual exploitation, reputational harm, or

⁵⁸ Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content."

⁵⁹ Vaccari and Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News."

⁶⁰ Martin, "Online Safety Regulation of Deepfake Abuse: A Case Study on Australia's ESafety Commissioner."

⁶¹ Rebecca Umbach et al., "Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries," *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, <https://doi.org/10.1145/3613904.3642382>.

⁶² Miotti and Wasil, "Combatting Deepfakes: Policies to Address National Security Threats and Rights Violations."

⁶³ Martin, "Online Safety Regulation of Deepfake Abuse: A Case Study on Australia's ESafety Commissioner."

⁶⁴ Umbach et al., "Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries."

manipulation of public perception.⁶⁵ Causative tracing helps assess how data is obtained, the purpose of use, the actors involved, and the context of dissemination. Victim tracing helps assess whether there is harm to the victim's identity, reputation, economic interests, psychological condition, sexuality, or dignity. Meding and Sorge show that the boundary between lawful content processing and deepfake manipulation may become blurred when editing technology increasingly resembles authentic recording.⁶⁶

Based on this scheme, Causative-Victim Tracing can be understood as both a realistic and normative framework. It is realistic because it adapts to the character of deepfake, which spreads rapidly, moves across platforms, and is difficult to authenticate.⁶⁷ Chandra et al. show that the performance of deepfake detectors that appears high on academic datasets may decline when tested on deepfakes circulating in real internet environments, so the legal response must not rest on the assumption that synthetic content is always easy to detect.⁶⁸ It is normative because this framework maintains the function of criminal law in responding to harmful conduct, while still taking prevention and victim recovery into account. Accordingly, criminal law policy on deepfake does not stop at the question of who the perpetrator is, but also traces how the crime is enabled, who contributes to it, how the content is proven, which platforms are involved, and what must be done so that victims do not continue to suffer harm.

Conclusion

This study finds that the main weakness of Indonesia's response to facial and voice AI deepfake crimes lies not in the absence of applicable legal provisions, but in the fragmentation of protected legal interests, liability, evidentiary mechanisms, platform responsibility, and victim protection. The Personal Data Protection Law, Electronic Information and Transactions Law, Criminal Code, and Law on Sexual Violence Crimes can address particular aspects of deepfake conduct, but none independently captures non-consensual synthetic impersonation as an attack on biometric identity, personal identity integrity, and individual autonomy over digital representation.

The original contribution of this study is the formulation of Causative-Victim Tracing as an integralistic criminal law policy framework that understands deepfake as a sequence of crime, from biometric data acquisition and AI-based synthesis to distribution, layered actor involvement, evidentiary barriers, and recurring victim harm. Theoretically, this framework connects criminal etiology with a victim-oriented approach, shifting criminal law analysis from merely identifying offenders toward examining how crimes are enabled, who

⁶⁵ Meding and Sorge, "What Constitutes a Deep Fake? The Blurry Line between Legitimate Processing and Manipulation under the EU AI Act."

⁶⁶ Meding and Sorge, "What Constitutes a Deep Fake? The Blurry Line between Legitimate Processing and Manipulation under the EU AI Act."

⁶⁷ Nuria Alina Chandra, "Deepfake-Eval-2024: A Multi-Modal In-the-Wild Benchmark of Deepfakes Circulated in 2024," *ArXiv*, 2025, <https://doi.org/10.48550/arXiv.2503.02857>.

⁶⁸ Chandra, "Deepfake-Eval-2024: A Multi-Modal In-the-Wild Benchmark of Deepfakes Circulated in 2024."

contributes to them, and how victims should be protected and restored from the earliest stage.

The legal policy implication is the need to recognize unauthorized synthetic impersonation as a form of biometric identity misuse, establish layered liability based on each actor's contribution, strengthen digital evidentiary standards through metadata, provenance information, audit trails, and forensic verification, and impose proportionate obligations on platforms for labeling, complaint handling, evidence preservation, content removal, and prevention of redistribution. Victim protection should also include identity protection, reputational recovery, psychological support, restitution, and safeguards against repeated misuse of biometric data. Causative-Victim Tracing therefore provides both a theoretical development of integralistic criminal law policy and a normative direction for restructuring Indonesia's response to AI deepfake crimes.

Recommendation

The recommendations of this study are directed toward the reform of Indonesia's criminal law policy so that it can recognize the misuse of faces and voices through AI as a form of biometric identity misuse. Future regulation needs to include the criminal liability of layered actors, not only content creators or disseminators, but also parties who gain benefits, manage accounts, facilitate distribution, or allow digital means to be used to expand harm to victims. Law enforcement officials also need to strengthen digital evidentiary standards through metadata, provenance data, audit trails, file modification history, and support from digital forensic experts.

Digital platforms need to be given clearer obligations to detect, label, receive reports, remove harmful content, preserve digital evidence, and prevent re-uploading. Victim protection must operate from the earliest stage through rapid takedown, identity protection, reputational recovery, psychological support, restitution, and guarantees that biometric data will not be misused again. Future research may develop Causative-Victim Tracing through concrete case studies, broader legal comparison, the formulation of investigative indicators, platform responsibility models, and rights-based victim recovery mechanisms.

References

- Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Kencana, 2017.
- California State Legislature. Assembly Bill No. 602, Depiction of Individual Using Digital or Electronic Technology Sexually Explicit Material Cause of Action (2019). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

- . Senate Bill No. 942, California AI Transparency Act (2024). https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942.
- Chandra, Nuria Alina. "Deepfake-Eval-2024: A Multi-Modal In-the-Wild Benchmark of Deepfakes Circulated in 2024." ArXiv, 2025. <https://doi.org/10.48550/arXiv.2503.02857>.
- Chesney, R, and D K Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." California Law Review 107, no. 6 (2019): 1753–1820. <https://doi.org/10.1215/00081143-1753>. Chesney, Robert and Citron, Danielle Keats, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security (July 14, 2018). 107 California Law Review 1753 (2019), U of Texas Law, Public Law Research Paper No. 692, U of Maryland Legal Studies Research Paper No. 2018-21, Available at SSRN: <https://ssrn.com/abstract=3213954> or <http://dx.doi.org/10.2139/ssrn.3213954>.
- Citron, D K. "Sexual Privacy." Yale Law Journal 128, no. 7 (2019): 1870–1960.
- Divisi Humas Polri. "Polisi Berhasil Menangkap Pelaku Sindikat Penipuan Modus Video Deepfake." Tribatanews, July 1, 2025.
- European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonized Rules on Artificial Intelligence (2024). <https://artificialintelligenceact.eu/article/50/>.
- Kementerian Komunikasi dan Informatika. "Kominfo Pastikan Konten Presiden Pidato Bahasa Mandarin Disinformasi Menyesatkan." InfoPublik, July 1, 2023. <https://infopublik.id/kategori/nasional-sosial-budaya/790958/kominfo-pastikan-konten-presiden-pidato-bahasa-mandarin-disinformasi-menyestakan>.
- Martin, N. "Online Safety Regulation of Deepfake Abuse: A Case Study on Australia's ESafety Commissioner." Griffith Law Review 34, no. 1 (2025): 23–46. <https://doi.org/10.1080/10383441.2025.2504791>.
- McGlynn, C, and E Rackley. "Image-Based Sexual Abuse." Oxford Journal of Legal Studies 37, no. 3 (2017): 534–61. <https://doi.org/10.1093/ojls/gqw033>.
- Meding, Kristof, and Christoph Sorge. "What Constitutes a Deep Fake? The Blurry Line between Legitimate Processing and Manipulation under the EU AI Act." In Proceedings of the 2025 Symposium on Computer Science and Law, 152–59, 2025. <https://doi.org/10.1145/3709025.3712218>.
- Miotti, Andrea, and Akash Wasil. "Combating Deepfakes: Policies to Address National Security Threats and Rights Violations." ArXiv, 2024. <https://doi.org/10.48550/arXiv.2402.09581>.
- Muhammad Abdul Azis, Nur Rahman, Riski Ananda Kusuma Putri. "Between The Future Or Just Utopia: A Critical Analysis Of The Legal Personhood Of Artificial Intelligence On The Claim As A Patent Inventor." Journal Critical Legal Review 2, no. 1 (2025): 58–83.
- Nadhiroh, Fatichatun. "Pelaku Penipuan Deepfake Khofifah Raup Untung Rp 87 Juta Selama 3 Bulan." DetikNews, July 1, 2025.

- Nasution, Angelica Vanessa Audrey, Suteki, and Anggita Doramia Lumbanraja. "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse." *International Journal for the Semiotics of Law* 38 (2025): 2489–2517. <https://doi.org/10.1007/s11196-025-10265-0>.
- Qandeel, Mais. "Facial Recognition Technology: Regulations, Rights and the Rule of Law." *Frontiers in Big Data* 7 (2024): 1354659. <https://doi.org/10.3389/fdata.2024.1354659>.
- Rahman, Praditya Fauzi. "3 Pelaku Penipuan Deepfake Khofifah Ditangkap, Korban 100 Orang." *DetikNews*, July 1, 2025. <https://news.detik.com/berita/d-7892188/3-pelaku-penipuan-deepfake-khofifah-ditangkap-korban-100-orang>.
- Republic of Indonesia. Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (2023).
- . Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (2023).
- . Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (2008).
- . Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (2022).
- . Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (2022).
- Republic of Korea. Act on Special Cases Concerning the Punishment of Sexual Crimes (2026). https://elaw.klri.re.kr/eng_service/lawView.do?hseq=40947&lang=ENG.
- Romero-Moreno, Felipe. "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content." *International Review of Law, Computers and Technology* 39, no. 2 (2024): 1–30. <https://doi.org/10.1080/13600869.2024.2324540>.
- Tolosana, Ruben, Sergio Romero-Tapiador, Julian Fierrez, and Ruben Vera-Rodriguez. "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection." *Information Fusion* 64 (2020): 131–48. <https://doi.org/10.1016/j.inffus.2020.06.014>.
- Umbach, Rebecca, Nicola Henry, Georgia F Beard, and Colleen M Berryessa. "Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries." *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024. <https://doi.org/10.1145/3613904.3642382>.
- Vaccari, Cristian, and Andrew Chadwick. "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media + Society* 6, no. 1 (2020): 1–13. <https://doi.org/10.1177/2056305120903408>.
- Westerlund, M. "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review* 9, no. 11 (2019): 40–52. <https://doi.org/10.22215/timreview/1282>.

Yim, Hyunsu. "South Korea to Criminalise Watching or Possessing Sexually Explicit Deepfakes." Reuters, July 1, 2024.
<https://www.reuters.com/world/asia-pacific/south-korea-criminalise-watching-or-possessing-sexually-explicit-deepfakes-2024-09-26/>