Perlindungan Hukum Korban *Deepfake* Sebagai Cyber-Fraud Dalam Hukum Pidana Indonesia

Dwi Setyo Pambudi[1], Yusuf Saefudin[2]
[12]Fakultas Hukum, Universitas Muhammadiyah Purwokerto
e-mail: [1]dwisetyo263@gmail.com, [2]yusuf.saefudin12@ump.ac.id

Abstrak

Penggunaan *deepfake* berbasis kecerdasan buatan telah berkembang menjadi sarana manipulasi identitas, penipuan, pemerasan, pornografi non-konsensual, dan disinformasi. Persoalan hukumnya tidak terletak pada ketiadaan hukum secara keseluruhan, melainkan pada keterbatasan pengaturan yang secara khusus mengidentifikasi *deepfake* sebagai modus tersendiri dan pada belum terpadunya mekanisme perlindungan korban. Penelitian ini bertujuan menganalisis konstruksi pertanggungjawaban pidana atas penggunaan *deepfake* sebagai sarana *cyber-fraud* dan merumuskan model perlindungan korban yang efektif dalam sistem hukum Indonesia. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, kasus, dan komparatif. Bahan hukum primer meliputi Undang-Undang Nomor 1 Tahun 2024 tentang ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 tentang KUHP sebagaimana disesuaikan dengan Undang-Undang Nomor 1 Tahun 2026, serta Undang-Undang Nomor 12 Tahun 2022 tentang TPKS. Analisis juga menggunakan perbandingan kewajiban transparansi *deepfake* dalam Uni Eropa dan tata kelola *deep synthesis* di Tiongkok. Hasil penelitian menunjukkan bahwa *deepfake* sebagai *cyber-fraud* dapat dikonstruksikan melalui delik penipuan apabila terpenuhi unsur tipu muslihat dan kerugian harta benda, melalui ketentuan manipulasi informasi elektronik, pelindungan data pribadi, serta delik lain sesuai muatan konten. Perlindungan korban harus dibangun melalui rantai perlindungan yang mencakup pencegahan, pelaporan cepat, preservasi bukti, penghentian penyebaran, penegakan hukum berbasis digital forensik, pemulihan reputasi dan privasi, serta restitusi atau ganti kerugian sesuai dasar hukumnya. Kebaruan penelitian terletak pada desain model perlindungan korban yang terintegrasi, bukan sekadar pada klaim adanya kekosongan hukum khusus *deepfake*.

***Kata kunci: deepfake, cyber-fraud*, UU ITE, UU PDP, perlindungan korban.**

Abstract

The use of artificial intelligence-based deepfakes has developed into a tool for identity manipulation, fraud, extortion, non-consensual pornography, and disinformation. The legal problem is not the total absence of applicable law, but the limited existence of provisions specifically addressing deepfakes and the lack of an integrated victim-protection mechanism. This study examines the construction of criminal liability for deepfake-based cyber-fraud and formulates an effective victim-protection model within the Indonesian legal system. It applies normative legal research using statutory, conceptual, case, and comparative approaches. Primary legal materials include Law Number 1 of 2024 on Electronic Information and Transactions, Law Number 27 of 2022 on Personal Data Protection, Law Number 1 of 2023 on the Criminal Code as adjusted by Law Number 1 of 2026, and Law Number 12 of 2022 on Sexual Violence Crimes. The study also compares the European Union transparency obligations for deepfakes with China's regulation of deep-synthesis services. The findings indicate that

deepfake-based cyber-fraud may be constructed through fraud provisions when deceit and property-loss elements are fulfilled, as well as through electronic information manipulation and personal-data offenses, depending on the content and conduct involved. Victim protection should operate through an integrated chain covering prevention, rapid reporting, evidence preservation, content restriction, digital-forensic investigation, restoration of privacy and reputation, and restitution or compensation where legally available. The novelty of this research lies in an integrated victim-protection model rather than a claim of a complete legal vacuum.

Keywords: deepfakes, cyber fraud, ITE Law, PDP Law, victim protection.

1. PENDAHULUAN

Perkembangan kecerdasan buatan telah memperluas kemampuan produksi dan manipulasi media digital pada tingkat yang semakin sulit dibedakan dari materi autentik. *Deepfake* merupakan salah satu bentuk media sintetis yang memungkinkan wajah, suara, gerak, atau kombinasi karakteristik seseorang ditempatkan ke dalam media lain secara meyakinkan. Literatur mengenai *AI crime* menempatkan *deepfake* sebagai bagian dari penyalahgunaan kecerdasan buatan yang dapat memperbesar kerentanan yang telah ada, termasuk penipuan, pemerasan, pornografi non-konsensual, pemalsuan, dan manipulasi informasi. Dalam perspektif hukum pidana, teknologi tersebut penting bukan karena teknologinya semata, melainkan karena fungsi teknisnya menjadi instrumen untuk melakukan perbuatan yang merugikan orang lain.[1]

Dalam konteks *cyber-fraud*, *deepfake* berfungsi terutama sebagai alat penipuan melalui penyamaran identitas dan penciptaan kesan keaslian. Pelaku dapat menggunakan wajah atau suara seseorang yang dikenal korban untuk memberikan perintah transfer dana, menawarkan hadiah palsu, meminta data sensitif, atau meyakinkan calon korban bahwa komunikasi tersebut berasal dari orang yang sebenarnya. Namun, tidak setiap *deepfake* merupakan *cyber-fraud*. *Deepfake* politik yang hanya bertujuan memengaruhi opini, misalnya, dapat lebih tepat dikaji sebagai disinformasi atau manipulasi informasi; *deepfake* yang menuduhkan perbuatan tertentu terhadap seseorang dapat berkaitan dengan pencemaran; sedangkan *deepfake* seksual dapat masuk ke rezim kekerasan seksual berbasis elektronik atau pornografi. Pembedaan ini penting agar konstruksi delik tidak dilakukan secara serampangan.[2]

Persoalan tersebut semakin penting karena hukum Indonesia saat ini telah memiliki sejumlah norma yang dapat digunakan, tetapi norma-norma tersebut tersebar dalam beberapa rezim hukum. Undang-Undang Nomor 1 Tahun 2024 masih memuat ketentuan mengenai informasi bohong yang merugikan konsumen dalam transaksi elektronik dan manipulasi Informasi Elektronik dan/atau Dokumen Elektronik agar seolah-olah autentik. Sementara itu, setelah mulai berlaku pada 2 Januari 2026, KUHP baru menyediakan konstruksi penipuan, pencemaran,

[1] Taís Fernanda Blauth, Oskar Josef Gstrein, and Andrej Zwitter, 2022, Artificial Intelligence Crime : An Overview of Malicious Use and Abuse of AI" 10, no. June, https://doi.org/10.1109/ACCESS.2022.3191790.

[2] Giuseppe Cascavilla and Damian A Tamburri, 2021, Cybercrime Threat Intelligence : A Systematic Multi-Vocal Literature Review," *Computers & Security* 105: 102258, https://doi.org/10.1016/j.cose.2021.102258.

penghinaan, persangkaan palsu, dan tindak pidana pornografi yang dapat menjadi dasar penindakan sesuai jenis *deepfake* yang digunakan. Karena itu, persoalan normatifnya lebih tepat dirumuskan sebagai keterbatasan atau kekosongan pengaturan khusus mengenai *deepfake*, bukan kekosongan hukum secara total.[3]

Kasus publik menunjukkan bahwa manipulasi berbasis identitas digital tidak selalu memiliki konstruksi hukum yang sama. Pada Oktober 2023, Kementerian Komunikasi dan Informatika melakukan klarifikasi atas video yang menampilkan Joko Widodo seolah-olah berpidato dalam bahasa Mandarin; materi tersebut dinyatakan sebagai hasil manipulasi dari video lama. Kasus tersebut lebih tepat ditempatkan sebagai ilustrasi disinformasi atau manipulasi informasi, bukan secara otomatis sebagai cyber-fraud, karena bahan yang tersedia tidak menunjukkan adanya unsur penyerahan harta benda oleh korban. Berbeda dengan itu, penipuan yang menggunakan nama dan identitas Baim Wong melalui akun atau nomor komunikasi palsu memang telah dilaporkan sebagai modus giveaway palsu. Namun, sumber publik yang dapat diverifikasi tidak cukup untuk menyatakan bahwa seluruh kasus tersebut merupakan *deepfake* berbasis AI. Oleh karena itu, penelitian ini memperlakukan kasus Baim Wong sebagai ilustrasi impersonation-based fraud, bukan sebagai bukti faktual bahwa suatu perkara tertentu telah terbukti menggunakan *deepfake*.[4]

Keterbatasan penelitian terdahulu terutama terlihat pada kecenderungan untuk berhenti pada pernyataan bahwa *deepfake* belum diatur secara khusus, tanpa menguraikan hubungan antara jenis perbuatan, unsur delik, pembuktian digital, dan kebutuhan pemulihan korban. Kajian mengenai kriminalisasi *deepfake*, pertanggungjawaban pidana, dan ancaman terhadap data pribadi telah berkembang; demikian pula kajian mengenai *cybercrime* dan perlindungan data pribadi di Indonesia. Namun, masih diperlukan penelitian yang secara sistematis memetakan konstruksi pertanggungjawaban pidana berdasarkan tipe *deepfake* sekaligus menyusun model perlindungan korban yang dapat dijalankan dari tahap pencegahan sampai pemulihan.[5]

Atas dasar itu, penelitian ini memusatkan kebaruan pada dua hal. Pertama, penelitian membedakan *deepfake* berdasarkan fungsi kriminalnya cyber-fraud, disinformasi, pencemaran, pornografi, dan pemerasan sehingga pasal yang digunakan tidak lagi bersifat "*one size fits all*". Kedua, penelitian membangun model perlindungan korban yang menggabungkan pelaporan cepat, preservasi alat bukti elektronik, penghentian penyebaran, penegakan hukum berbasis digital forensics, perlindungan data, pemulihan reputasi, dan restitusi atau ganti kerugian. Model tersebut kemudian dibandingkan dengan kecenderungan regulasi di Uni Eropa dan

[3] Republik Indonesia, Undang-Undang Nomor 1 Tahun 2024; Republik Indonesia, Undang-Undang Nomor 1 Tahun 2023; Republik Indonesia, Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana.

[4] Kementerian Komunikasi Dan Digital, n.d., https://www.komdigi.go.id/berita/berita-hoaks/detail/hoaks-video-kampanye-jokowi-amin-berbahaa-mandarin.

[5] Muhammad Nur Hidayat, 2025, Pertanggungjawaban Pidana Terhadap Penyalahgunaan *Deepfake* Sebagai Ancaman Keamanan Data Pribadi, *UNES Law Review* 7, no. 4 : 2036–48, https://doi.org/10.31933/unesrev.v7i4.2433.

Tiongkok yang telah menempatkan transparansi dan tanggung jawab penyedia layanan sebagai bagian penting dari tata kelola *deepfake*.[6]

Berdasarkan latar belakang tersebut, rumusan masalah penelitian ini adalah:

1. Bagaimana konstruksi pertanggungjawaban pidana terhadap penggunaan *deepfake* sebagai sarana *cyber-fraud* berdasarkan hukum pidana Indonesia?
2. Bagaimana model perlindungan hukum yang efektif bagi korban kejahatan *deepfake* dalam sistem hukum Indonesia?

2. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang berorientasi pada pengkajian norma hukum, asas, doktrin, dan keterkaitan antarrejimen hukum yang mengatur perbuatan *deepfake*. Pendekatan perundang-undangan (*statute approach*) digunakan untuk menelaah Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana sebagaimana disesuaikan dengan Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana, serta Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual. Pendekatan konseptual digunakan untuk menjelaskan *deepfake, cyber-fraud, victim protection, digital evidence, dan digital forensics*.[7]

Pendekatan kasus digunakan secara terbatas terhadap fakta publik mengenai video Joko Widodo berbahasa Mandarin dan penipuan yang mengatasnamakan Baim Wong. Kedua kasus tidak diposisikan sebagai bukti persidangan atau putusan pengadilan, melainkan sebagai bahan ilustratif untuk menguji kesesuaian unsur delik. Pendekatan komparatif diterapkan secara nyata dengan membandingkan model transparansi *deepfake* dalam *Regulation* (EU) 2024/1689 tentang *Artificial Intelligence Act*, khususnya *Article 50*, dengan *Provisions on the Administration of Deep Synthesis of Internet-Based Information Services* yang berlaku di Tiongkok sejak 10 Januari 2023.[8]

3. HASIL DAN PEMBAHASAN

3.1 Konstruksi Pertanggungjawaban Pidana Berdasarkan Hukum Indonesia

Deepfake tidak dapat dipersamakan dengan satu jenis tindak pidana. Secara teknologi, *deepfake* merupakan media sintetis atau media yang dimanipulasi dengan teknik pembelajaran mesin sehingga identitas atau tindakan seseorang dapat ditirukan. Secara yuridis, teknologi hanya merupakan sarana. Delik pidana ditentukan oleh tujuan, tindakan, akibat, dan hubungan kausal yang

[6] Rafi Satrya Arvitto, 2025, Implikasi Hukum *Deepfake* : Telaah Terhadap UU ITE Dan UU PDP (Legal Implications of *Deepfake* : A Review of the ITE Law and the PDP Law) 4, no. 2 : 73–82, https://doi.org/10.35912/jihham.v4i2.3937.

[7] Peter Mahmud Marzuki, 2005, *Penelitian Hukum*, Jakarta: Kencana Prenada Media 55.

[8] *Regulation - EU - 2024/1689 - EN - EUR-Lex*. (n.d.). 2026, Retrieved August 29, from https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng; *Provisions on the Administration of Deep Synthesis Internet Information Services*. (n.d.). 2026, Retrieved August 29, from https://www.chinalawtranslate.com/en/deep-synthesis

dapat dibuktikan. Kerangka analisis ini mencegah perluasan pasal secara berlebihan dan sekaligus memberikan kepastian bahwa penegakan hukum didasarkan pada unsur delik yang konkret.[9]

Dalam *cyber-fraud*, unsur sentralnya adalah adanya niat menguntungkan diri sendiri atau orang lain secara melawan hukum, penggunaan nama atau kedudukan palsu, tipu muslihat atau rangkaian kata bohong, serta adanya tindakan korban yang menyerahkan harta, memberikan utang, membuat pengakuan utang, atau menghapus piutang. *Deepfake* dapat menjadi bentuk tipu muslihat karena memberikan kesan otentik mengenai identitas komunikator. Dengan demikian, pada skenario suara palsu seorang atasan yang memerintahkan transfer dan korban benar-benar menyerahkan dana, konstruksi penipuan menjadi kuat. Sebaliknya, apabila *deepfake* hanya menghasilkan video palsu tanpa adanya perpindahan harta benda, Pasal 492 KUHP tidak serta-merta terpenuhi.[10]

Deepfake yang hanya menyesatkan publik juga harus dibedakan dari *cyber-fraud*. Kategori tersebut dapat berupa informasi manipulatif atau disinformasi yang memengaruhi opini tanpa tujuan langsung memperoleh harta benda. *Deepfake* yang menuduhkan suatu perbuatan yang merendahkan kehormatan dapat berkaitan dengan pencemaran menurut KUHP. *Deepfake* seksual dapat beririsan dengan pornografi dan, jika memenuhi unsur kekerasan seksual berbasis elektronik, dapat masuk ke UU TPKS. Pembedaan kategoris ini merupakan dasar untuk menentukan pasal yang tepat dan mencegah penggunaan satu norma untuk semua jenis *deepfake*.[11]

3.2.1 Undang-Undang ITE: Manipulasi Informasi Elektronik dan Penipuan Transaksi

Pasal 28 ayat (1) UU ITE perlu dibaca secara sempit sesuai rumusannya. Ketentuan tersebut tidak merupakan larangan umum atas semua berita palsu di internet, tetapi menargetkan distribusi dan/atau transmisi Informasi Elektronik atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiil bagi konsumen dalam Transaksi Elektronik. Oleh sebab itu, pasal ini relevan bagi *deepfake* yang digunakan untuk melakukan transaksi elektronik yang menimbulkan kerugian konsumen. Ia tidak tepat digunakan untuk setiap video *deepfake* yang sekadar merusak reputasi atau memengaruhi opini.[12]

Pasal 35 UU ITE mempunyai relevansi yang lebih langsung terhadap *deepfake* sebagai tindakan manipulasi digital karena mengatur manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar informasi atau dokumen tersebut dianggap seolah-olah autentik. Unsur yang harus dibuktikan bukan sekadar adanya video atau audio palsu, melainkan adanya tindakan yang disengaja

[9] Maria-Paz Sandoval et al., 2024, Threat of *Deepfake*s to the Criminal Justice System: A Systematic Review, *Crime Science* 13 : 41, https://doi.org/10.1186/s40163-024-00239-1.
[10] Sandoval et al.
[11] Taun Liswati, Anggi Lia, 2025, Analisis Yuridis Terhadap Pertanggungjawaban Pidana Pelaku Pelecehan Seksual Berbasis Al (*Deepfake* Pornografi) Di Media Sosial 2, no. 6 : 162–76, https://doi.org/10.62383/hukum.v2i6.742.
[12] undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, No. 190185.

dan tanpa hak atau melawan hukum serta tujuan membentuk kesan otentik. Dalam perkara *deepfake*, bukti forensik harus menghubungkan file yang diperiksa dengan tindakan manipulasi dan tujuan agar hasil manipulasi dipercaya sebagai asli.[13]

Pasal 36 UU ITE sebagai ketentuan umum kerugian. Untuk keadaan hukum setelah berlakunya KUHP baru pada 2 Januari 2026, rujukan tersebut tidak lagi dapat dipakai secara sembarangan karena beberapa ketentuan pidana UU ITE, termasuk Pasal 36 dan pasal tertentu mengenai muatan, diselaraskan atau dicabut melalui sistem transisi menuju KUHP. Karena itu, analisis artikel ini memusatkan UU ITE yang masih relevan untuk *deepfake* pada Pasal 28 ayat (1), Pasal 35, Pasal 26 ayat (3), serta ketentuan pembuktian elektronik, kemudian menghubungkannya dengan KUHP baru bila unsur deliknya terpenuhi.[14]

Terkait penghinaan, Pasal 27A UU ITE sebagai norma utama. Setelah KUHP baru berlaku, penggunaan Pasal 27A tidak boleh diposisikan sebagai norma pidana umum yang berdiri sendiri karena ketentuan tersebut dirancang dalam kerangka transisi menuju KUHP. Untuk perbuatan yang merupakan pencemaran atau penghinaan, rujukan substansinya bergeser ke KUHP baru, dengan Pasal 441 sebagai pemberatan apabila delik penghinaan tertentu dilakukan dengan sarana teknologi informasi. Pendekatan ini lebih konsisten dengan kebijakan harmonisasi antara UU ITE dan KUHP.[15]

3.2.2 Undang-Undang Pelindungan Data Pribadi: Wajah dan Suara sebagai Data Biometrik

UU PDP mengklasifikasikan data biometrik sebagai Data Pribadi yang bersifat spesifik. Karena wajah dan karakteristik suara dapat digunakan untuk mengidentifikasi seseorang, penggunaannya dalam pembuatan atau penyebaran *deepfake* harus dianalisis dengan kerangka pemrosesan Data Pribadi, bukan sekadar dianggap sebagai "gambar atau suara biasa". Penentuan pasal pidana tetap harus berangkat dari tindakan konkret terhadap data tersebut.[16]

Pasal 65 UU PDP membedakan tiga tindakan utama: memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya secara melawan hukum; mengungkapkan Data Pribadi yang bukan miliknya; dan menggunakan Data Pribadi yang bukan miliknya. Ketiga perbuatan tersebut memiliki objek dan unsur yang tidak identik. Pasal 66, selanjutnya, melarang pembuatan atau pemalsuan Data Pribadi dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain, dengan sanksi pidana pada Pasal 68. Karena itu, tidak setiap *deepfake* otomatis memenuhi Pasal 66. Penyidik harus membuktikan apakah terdapat pemalsuan Data Pribadi dalam arti yang dimaksud UU PDP dan apakah terdapat maksud keuntungan serta potensi kerugian yang menjadi bagian unsur deliknya.[17]

[13] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008.
[14] Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 20088 Tentang Informasi Dan Transaksi Elektronik.
[15] Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana, No. 16100 . Pasal 433-441
[16] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, No. 016999.
[17] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Pembedaan tersebut penting pada kasus *voice cloning* atau *face swapping*, apabila pelaku memperoleh, mengumpulkan, atau menggunakan data biometrik korban untuk menyusun identitas palsu, Pasal 65 jo. Pasal 67 dapat dianalisis. Apabila pelaku benar-benar membuat atau memalsukan Data Pribadi dengan motif keuntungan dan kerugian, Pasal 66 jo. Pasal 68 menjadi relevan. Dengan konstruksi demikian, artikel tidak lagi menyamakan semua penggunaan wajah dan suara dengan satu pasal PDP.[18]

3.2.3 KUHP Baru Setelah 2 Januari 2026

KUHP berdasarkan Undang-Undang Nomor 1 Tahun 2023 mulai berlaku pada 2 Januari 2026 dan dalam perkembangan berikutnya ketentuan pidananya disesuaikan melalui Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana. Konsekuensinya, analisis *deepfake* dalam artikel ini harus ditempatkan pada hukum positif yang telah berlaku, bukan lagi sekadar sebagai hukum yang akan berlaku. Harmonisasi tersebut juga menjelaskan mengapa beberapa delik yang dahulu terdapat dalam UU ITE sekarang harus dibaca bersama atau digantikan oleh ketentuan KUHP baru.[19]

Pasal 492 KUHP mengatur tindak pidana penipuan dengan unsur maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, memakai nama atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata bohong, dan menggerakkan orang supaya menyerahkan barang, memberi utang, membuat pengakuan utang, atau menghapus piutang. *Deepfake* sangat mungkin menjadi sarana memenuhi unsur tipu muslihat atau kedudukan palsu. Akan tetapi, unsur akibat berupa tindakan korban terhadap harta benda tetap harus dibuktikan. Ini yang membedakan *cyber-fraud* dari sekadar *deepfake* yang hanya menipu persepsi tanpa transaksi.[20]

Untuk *deepfake* yang menyerang kehormatan atau nama baik, Pasal 433 sampai dengan Pasal 439 dapat digunakan sesuai bentuk perbuatan. Pasal 433 mencakup pencemaran, termasuk pencemaran tertulis melalui tulisan atau gambar yang disiarkan, dipertunjukkan, atau ditempelkan di tempat umum. Pasal 434 berkaitan dengan fitnah. Pasal 436 mengatur penghinaan ringan. Apabila perbuatan tersebut dilakukan dengan sarana teknologi informasi, Pasal 441 menaikkan pidana sampai sepertiga untuk delik penghinaan yang termasuk dalam cakupannya. Dengan demikian, *deepfake* yang menggambarkan seseorang secara palsu sambil menuduhkan perbuatan yang merusak reputasinya tidak cukup dianalisis sebagai "pemalsuan video"; struktur delik pencemaran dan pemberatannya harus diuji.[21]

Untuk *deepfake* pornografi, Pasal 407 KUHP sebagaimana berlaku setelah penyesuaian pidana tahun 2026. Ketentuan tersebut tidak berarti bahwa semua *deepfake* seksual otomatis merupakan tindak pidana yang sama. Penilaian harus

[18] Hidayat, *Pertanggungjawaban Pidana Terhadap Penyalahgunaan Deepfake Sebagai Ancaman Keamanan Data Pribadi*.
[19] Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana.
[20] Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana.
[21] Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana.

memperhatikan tindakan produksi, pembuatan, reproduksi, distribusi, atau penyiaran konten pornografi dan pengecualian yang diatur dalam pasal. Apabila materi *deepfake* mengandung kekerasan seksual berbasis elektronik dan memenuhi unsur UU TPKS, rezim TPKS dapat diterapkan secara khusus.[22]

Konstruksi tersebut memperlihatkan bahwa masalah Indonesia bukan ketiadaan dasar pemidanaan, tetapi keterbatasan pengaturan yang secara eksplisit mengatur *synthetic impersonation* atau *deepfake* sebagai modus yang mempunyai karakteristik khusus. Aparat tetap memiliki beberapa jalur pemidanaan, tetapi harus memilih pasal berdasarkan objek, tujuan, akibat, dan bukti. Ketiadaan delik khusus menyebabkan penegakan hukum sangat bergantung pada kecermatan kualifikasi dan kemampuan pembuktian digital.[23]

3.2.4 UU TPKS dan Batas Penerapannya

UU Nomor 12 Tahun 2022 tentang TPKS relevan apabila *deepfake* mengandung kekerasan seksual berbasis elektronik atau tindak pidana kekerasan seksual lain yang memenuhi unsur undang-undang. Pasal 14 mengatur Kekerasan Seksual Berbasis Elektronik, sementara Pasal 15 memberikan pemberatan ketika tindak pidana tertentu dilakukan dengan sarana elektronik. Karena itu, UU TPKS tidak dapat digunakan sebagai "payung" untuk semua *deepfake*. Rezim ini harus dibatasi pada jenis perbuatan yang memang mempunyai unsur seksual sebagaimana ditentukan undang-undang.[24]

Kelebihan pendekatan TPKS terletak pada orientasinya pada korban. Hak korban mencakup penanganan, perlindungan, dan pemulihan; mekanisme restitusi dan skema kompensasi negara juga telah dibentuk dalam kerangka TPKS. Namun, kompensasi negara bukan hak otomatis setiap korban *deepfake*. Ia berlaku dalam konteks dan mekanisme yang ditentukan UU TPKS serta peraturan pelaksananya. Oleh karena itu, artikel ini membedakan restitusi dari pelaku, ganti kerugian berdasarkan jalur perdata, dan kompensasi negara dalam rezim khusus TPKS.[25]

3.2.5 Perbandingan Regulasi Uni Eropa dan Tiongkok

Uni Eropa melalui *Regulation (EU) 2024/1689 (Artificial Intelligence Act)* menempatkan transparansi sebagai instrumen pencegahan. Article 50 mewajibkan penyedia sistem AI yang menghasilkan audio, gambar, video, atau teks sintetis untuk memastikan keluaran dapat ditandai dalam format yang dapat dibaca mesin dan dapat dideteksi sebagai dibuat atau dimanipulasi secara artifisial. Untuk *deepfake*, pihak yang menyebarkan atau menggunakan konten juga diwajibkan mengungkapkan bahwa konten tersebut telah dibuat atau dimanipulasi secara artifisial. Per 2 Agustus 2026, kewajiban transparansi tersebut mulai diterapkan.

[22] Hairul Saleh Satrul and Nur Hafizal Hasanah, 2026, Reconstruction of Criminal Liability for *Deepfake* Misuse in Defamatory Defenses in Indonesia, *Rechtsvinding*, https://doi.org/10.59525/rechtsvinding.1541.
[23] Agus Nugroho and An An, 2023, Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries, *Security Journal* 36, no. 4 : 651–70, https://doi.org/10.1057/s41284-022-00357-y.
[24] Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual, N.D.
[25] Liswati, Anggi Lia, Analisis Yuridis Terhadap Pertanggungjawaban Pidana Pelaku Pelecehan Seksual Berbasis Al (*Deepfake* Pornografi) Di Media Sosial.

Model ini menunjukkan bahwa perlindungan tidak hanya diberikan setelah korban jatuh, tetapi juga melalui kewajiban *ex ante* pada penyedia dan pengguna AI.[26]

Tiongkok menerapkan *Provisions on the Administration of Deep Synthesis of Internet-Based Information Services* yang berlaku sejak 10 Januari 2023. Regulasi tersebut membebankan kewajiban pada penyedia layanan *deep synthesis*, termasuk mekanisme verifikasi identitas, pengelolaan dan pelabelan konten sintetis, pengamanan data, serta kewajiban pengawasan dan kerja sama dengan otoritas. Pendekatan Tiongkok menempatkan penyedia layanan sebagai bagian dari arsitektur pencegahan, bukan hanya sebagai platform pasif setelah konten beredar.[27]

Dari kedua rezim tersebut, terdapat dua pelajaran yang relevan bagi Indonesia. Pertama, pencegahan harus dimulai dari transparansi asal-usul konten melalui label atau penanda teknis. Kedua, penyedia layanan perlu mempunyai kewajiban yang lebih jelas mengenai identifikasi, preservasi data, respons terhadap pengaduan, dan pengurangan penyebaran. Indonesia dapat mengadopsi prinsip tersebut tanpa harus menyalin model sanksinya secara utuh. Hal tersebut sejalan dengan kebutuhan memperkuat perlindungan korban dan mengurangi beban pembuktian pada tahap awal.[28]

Korban *deepfake* tidak hanya mengalami kerugian ekonomi. Mereka dapat kehilangan reputasi, privasi, keamanan psikologis, pekerjaan, dan rasa percaya terhadap lingkungan sosial. Oleh sebab itu, perlindungan korban harus dipahami sebagai proses yang berlangsung sejak sebelum tindak pidana terjadi, pada saat konten pertama muncul, selama proses penyidikan, dan setelah perkara selesai. Model yang hanya menyediakan akses untuk melapor setelah konten viral tidak cukup untuk karakter *deepfake* yang persebarannya cepat dan sulit ditarik kembali.[29]

Tahap pertama adalah pencegahan. Pemerintah dan penyedia layanan perlu meningkatkan literasi digital mengenai impersonation, penggunaan verifikasi dua faktor, autentikasi identitas untuk komunikasi berisiko tinggi, serta pelabelan konten sintetis. Pada level kelembagaan, perusahaan dan instansi yang rentan terhadap penipuan "atas nama atasan" perlu mempunyai prosedur *callback* atau verifikasi ganda sebelum transaksi. Pencegahan tersebut mengurangi ketergantungan pada penegakan hukum setelah kerugian terjadi.[30]

Tahap kedua adalah pelaporan awal dan preservasi bukti. Korban sebaiknya menyimpan file asli, tautan, URL, nama akun, nomor telepon, e-mail,

[26] Athalia Pranata Putri S Meliala and Indah Sri Utari, 2026, Policy on the Formulation of Artificial Intelligence Accountability for the Creation and Dissemination of *Deepfake* Videos from a Criminal Law Perspective in Indonesia, *Law Research Review Quarterly* 12, no. 2 : 953–81, https://doi.org/10.15294/lrrq.v12i2.44714.

[27] Chiquita Thefirstly Noerman and Aji Lukman Ibrahim, 2024, *Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara*, 7, no. 2 : 1–4.

[28] Yuliannova Lestari and M Misbahul Mujib, 2022, Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study), *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 11, no. 2 : 203–34, https://doi.org/10.14421/sh.v11i2.2729.

[29] Sandoval et al., *Threat of Deepfakes to the Criminal Justice System: A Systematic Review*.

[30] Iqbal Kamalludin Ayon Diniyanto, 2021, Menyelamatkan Korban Dari Jerat UU ITE: Studi Kasus Baiq Nuril Maknun Dan Relevansinya Bagi Penguatan Peran Pemerintah Melindungi Pelapor Tindak Asusila, 10, no. 1 (2021): 1–18, https://doi.org/10.14421/sh.v10i1.2341.

rekaman percakapan, waktu kejadian, bukti pembayaran, serta konteks komunikasi. File asli sebaiknya tidak hanya disimpan dalam bentuk tangkapan layar. Sistem pelaporan yang baik harus membantu korban mengunggah bukti dan mencatat waktu penerimaan laporan sehingga data dapat segera diamankan sebelum dihapus atau dipindahkan oleh pelaku.[31]

Tahap ketiga adalah penghentian penyebaran. Mekanisme pelaporan kepada platform perlu berjalan paralel dengan proses hukum. Untuk penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan, Pasal 26 ayat (3) UU ITE mengaitkannya dengan permintaan orang yang bersangkutan berdasarkan penetapan pengadilan. Karena itu, artikel tidak lagi menyatakan bahwa Pasal 26 ayat (3) otomatis menjadi mekanisme *takedown*. Secara praktis korban dapat memanfaatkan mekanisme pelaporan platform, sedangkan penghapusan berdasarkan undang-undang harus mengikuti dasar dan prosedur yang tersedia.[32]

Tahap keempat adalah penegakan hukum dan *digital forensics*. Penyidik perlu memeriksa keaslian audio atau video, metadata, artefak kompresi, sumber file, perangkat yang digunakan, akun dan log aktivitas, serta aliran transaksi. Prinsip *chain of custody* harus dipenuhi agar bukti yang dikumpulkan tetap dapat ditelusuri dari saat ditemukan sampai disajikan di persidangan. Tantangan utama bukan hanya mendeteksi bahwa konten palsu, tetapi menghubungkan pembuatan atau penyebaran konten tersebut dengan pelaku tertentu.[33]

Tahap kelima adalah perlindungan privasi dan pemulihan reputasi. Korban berhak meminta perlindungan terhadap data pribadi dan melakukan langkah untuk membatasi pemrosesan yang tidak sah sesuai kerangka UU PDP. Pada kasus yang menyerang reputasi, pemulihan tidak cukup hanya dengan menghapus video. Diperlukan strategi koreksi informasi, klarifikasi publik yang proporsional, dan dokumentasi yang menunjukkan bahwa konten telah dinyatakan palsu atau dimanipulasi. Pendekatan ini penting karena kerugian reputasi dapat bertahan setelah konten asli dihapus.[34]

Tahap keenam adalah pemulihan kerugian. Restitusi kepada korban harus dibedakan dari ganti kerugian perdata dan dari kompensasi negara yang hanya tersedia dalam rezim tertentu. Kerugian materiil dapat mencakup uang yang hilang, biaya pemulihan, atau pendapatan yang hilang. Kerugian nonmateriil dapat berkaitan dengan kerusakan reputasi dan penderitaan psikologis, sepanjang dasar gugatan atau rezim hukum yang digunakan memperbolehkannya. Pada *deepfake* seksual yang memenuhi UU TPKS, perlindungan korban dapat diperkuat melalui

[31] Olivia Anggie Johar Muhammad Safei, Sandra Dewi, 2025, Implementasi Pada Alat Bukti Jejak Digital Dalam Penegakan Hukum Tindak Pidana Penipuan Online 8, no. 2 : 501–19.
[32] Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2oo8 Tentang Informasi Dan Transaksi Elektronik.
[33] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, 2020, Comprehensive Review of Cybercrime Detection Techniques, in IEEE Access, vol. 8, pp. 137293-137311, doi: 10.1109/ACCESS.2020.3011259.
[34] Lestari and Mujib, *Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study).*

mekanisme restitusi, bantuan psikologis, dan pemulihan yang tersedia dalam rezim tersebut.[35]

Tahap ketujuh adalah pencegahan berulang. Platform, aparat, dan lembaga keuangan harus mempunyai mekanisme berbagi indikator penyalahgunaan, pemblokiran akun pelaku yang telah teridentifikasi sesuai hukum dan kebijakan platform, serta pembatasan pola transaksi berisiko. Prinsipnya bukan membuat daftar hitam tanpa dasar hukum, tetapi memperkuat koordinasi agar pelaku tidak dengan mudah memindahkan modus yang sama ke platform atau identitas baru.[36] *Deepfake* mengubah cara aparat menilai bukti digital. Video tidak lagi dapat diperlakukan sebagai representasi otomatis dari kejadian yang sebenarnya. Sistem peradilan perlu menilai sumber file, rantai penguasaan, konsistensi metadata, perangkat pembuat, pola kompresi, jejak pengeditan, serta kesesuaian dengan bukti digital lain. Kajian sistematis mengenai ancaman *deepfake* terhadap sistem peradilan menunjukkan bahwa masalah utama meliputi erosi kepercayaan terhadap bukti audio-visual, kesulitan atribusi pelaku, dan potensi pemalsuan bukti itu sendiri.[37]

Pada tahap forensik, minimal terdapat empat pertanyaan yang perlu dijawab. Pertama, apakah konten merupakan hasil manipulasi? Kedua, teknik manipulasi apa yang digunakan? Ketiga, dari perangkat atau akun mana konten berasal dan bagaimana rantai penyebarannya? Keempat, apakah terdapat hubungan antara akun atau perangkat tersebut dengan orang yang diduga sebagai pelaku? Jawaban atas pertanyaan pertama tidak otomatis menjawab tiga pertanyaan berikutnya. Karena itu, "deteksi *deepfake*" bukan sinonim dengan "pembuktian pelaku".[38]

Keterangan ahli menjadi penting ketika autentikasi tidak dapat dilakukan hanya dengan pemeriksaan sederhana. Namun, ahli tidak boleh menggantikan fungsi hakim dalam menentukan kesalahan. Ahli memberikan penjelasan teknis mengenai karakteristik file, proses pembentukan atau manipulasi, dan konsistensi bukti; sedangkan penilaian keseluruhan mengenai terpenuhinya unsur tindak pidana tetap menjadi kewenangan penegak hukum dan pengadilan.[39]

Selain masalah teknologi, penegak hukum menghadapi keterbatasan kapasitas, koordinasi antarinstansi, dan pengelolaan bukti digital. Studi mengenai penyidikan kejahatan siber di Indonesia dan penelitian tentang tantangan polisi *cybercrime* menunjukkan bahwa keterbatasan sumber daya dan koordinasi dapat mengurangi efektivitas investigasi. Karena itu, model perlindungan korban harus

[35] Liswati, Anggi Lia, *Analisis Yuridis Terhadap Pertanggungjawaban Pidana Pelaku Pelecehan Seksual Berbasis Al (Deepfake Pornografi) Di Media Sosial.*

[36] Lukman Khakim and Nabila Nur Fadlilah, 2024, *The Yogyakarta Police Overcoming Online Fraud Crimes* 33, no. 2 : 124–36, https://doi.org/10.33369/jsh.33.2.124-136.

[37] Sandoval et al., *Threat of Deepfakes to the Criminal Justice System: A Systematic Review*.

[38] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, 2020, *Comprehensive Review of Cybercrime Detection Techniques*, in IEEE Access, vol. 8, pp. 137293-137311, doi: 10.1109/ACCESS.2020.3011259.

[39] Stefano De Paoli et al., 2020, *A Qualitative Exploratory Study of the Knowledge , Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists* 15, no. 2 : 1429–45, https://doi.org/10.1093/police/paaa027.

memasukkan penguatan kapasitas *digital forensics* sebagai bagian dari kebijakan hukum, bukan sekadar perangkat tambahan.[40]

Kasus video yang menampilkan Joko Widodo seolah-olah berpidato dalam bahasa Mandarin menunjukkan kemampuan *deepfake* atau manipulasi digital untuk membentuk persepsi publik. Sumber pemerintah pada saat itu mengidentifikasi materi tersebut sebagai video yang dimanipulasi dari video lama. Secara yuridis, kasus tersebut tidak otomatis dapat digolongkan sebagai *cyber-fraud* karena tidak terdapat bukti dalam sumber yang digunakan bahwa seseorang telah digerakkan untuk menyerahkan harta benda. Nilai analitis kasus tersebut justru berada pada risiko disinformasi, kerusakan reputasi, dan gangguan terhadap kepercayaan publik. Kesimpulan tersebut sekaligus mengoreksi draf awal yang menggeneralisasi setiap *deepfake* sebagai *cyber-fraud*.[41]

Kasus penipuan yang mencatut nama Baim Wong berbeda. Berbagai laporan menunjukkan adanya akun atau nomor komunikasi palsu yang menjanjikan *giveaway* dan meminta korban mentransfer uang. Namun, sumber yang dapat diverifikasi lebih kuat untuk membuktikan adanya *impersonation-based scam* daripada penggunaan teknologi *deepfake* tertentu. Karena itu, penelitian ini tidak menggunakan kasus Baim Wong sebagai bukti bahwa *deepfake* telah terbukti digunakan dalam perkara tersebut. Kasus tersebut digunakan untuk menunjukkan bagaimana *synthetic impersonation* dapat beroperasi dalam ekosistem *cyber-fraud* dan mengapa verifikasi sumber identitas menjadi penting.[42]

Dari kedua ilustrasi tersebut, tampak bahwa perlindungan korban dan konstruksi pertanggungjawaban harus bergantung pada fakta. Konten yang memanipulasi tokoh publik tanpa transaksi finansial tidak boleh dipaksakan menjadi penipuan. Sebaliknya, ketika identitas palsu digunakan untuk menggerakkan korban menyerahkan uang, unsur penipuan perlu menjadi titik awal analisis. Pendekatan faktual seperti ini membuat penelitian lebih konsisten dengan asas legalitas dan kepastian hukum.[43]

Kebaruan penelitian ini tidak ditempatkan pada klaim bahwa hukum Indonesia sama sekali tidak mampu menangani *deepfake*. Justru, penelitian menunjukkan bahwa sejumlah norma telah tersedia, tetapi tersebar dan berbeda cakupan. Keterbatasan utama berada pada tidak adanya delik khusus yang dirancang untuk *synthetic impersonation*, belum seragamnya standar pembuktian digital, dan belum terintegrasinya perlindungan korban dengan tata kelola platform. Temuan ini sejalan dengan literatur yang menunjukkan bahwa hukum

[40] Muhammad Rizqy Romadhony, 2019, *Mekanisme Penyidikan Tindak Pidana Manipulasi Data Transaksi Grab Di Polres Lamongan* 8, no. 1, https://doi.org/10.14421/sh.v8i1.2047.

[41] Kementerian Komunikasi dan Digital. (n.d.). Retrieved August 29, 2026, from https://www.komdigi.go.id/berita/berita-hoaks/detail/hoaks-video-kampanye-jokowi-amin-berbahaa-mandarin. Accesed 29-08-2026

[42] *Jala Hoaks Jakarta*. (n.d.). Retrieved August 29, 2026, from https://jalahoaks.jakarta.go.id/detail/HOAKS-Pengumuman-Pemenang-Giveway-Baim-Wong. Accesed 29-08-2026

[43] Hidayat, *Pertanggungjawaban Pidana Terhadap Penyalahgunaan Deepfake Sebagai Ancaman Keamanan Data Pribadi.*

cybercrime sering tertinggal dari perkembangan teknologi dan bahwa *deepfake* menciptakan *blind spots* pada proses investigasi dan peradilan.[44]

Implikasi kebijakan pertama adalah kebutuhan harmonisasi antara hukum pidana materiil, hukum acara, dan regulasi platform digital. Implikasi kedua adalah perlunya standar teknis nasional untuk *digital evidence deepfake*, termasuk prosedur akuisisi, hash, preservasi, *chain of custody*, dan kompetensi ahli. Implikasi ketiga adalah penguatan kewajiban transparansi dan pelabelan konten AI, dengan mempertimbangkan pengalaman Uni Eropa. Implikasi keempat adalah kewajiban tanggap insiden bagi penyedia layanan deep synthesis dan mekanisme aduan yang mudah diakses, dengan mengambil pelajaran dari model Tiongkok.[45]

Arah pembaruan hukum yang ideal bukan semata-mata menambahkan kata "*deepfake*" ke dalam undang-undang. Pembentuk undang-undang perlu mengatur definisi, bentuk perbuatan, unsur kesalahan, hubungan dengan delik umum, tanggung jawab penyedia atau pihak yang mendistribusikan, standar bukti, perlindungan korban, dan mekanisme penghapusan konten. Dengan demikian, regulasi baru tidak menciptakan duplikasi antara UU ITE, KUHP, UU PDP, dan UU TPKS, tetapi justru membangun sistem yang saling melengkapi.[46]

3.2 Integrasi Perlindungan Korban dalam Sistem Hukum Pidana Indonesia

Pembahasan mengenai perlindungan korban *deepfake* perlu ditempatkan dalam kerangka sistem hukum yang tidak hanya berorientasi pada pemidanaan pelaku. Perlindungan korban harus dipahami sebagai rangkaian tindakan sejak sebelum laporan diterima sampai setelah proses peradilan selesai. Dalam konteks *deepfake*, pendekatan tersebut penting karena kerugian dapat berlangsung secara simultan: korban dapat kehilangan uang, mengalami penyalahgunaan identitas, menghadapi penyebaran konten yang merusak reputasi, dan mengalami kesulitan mengendalikan salinan konten yang telah beredar. Oleh karena itu, efektivitas perlindungan tidak dapat hanya diukur dari berhasil atau tidaknya pelaku dihukum, tetapi juga dari kemampuan sistem untuk menghentikan penyebaran, mempertahankan bukti, membatasi kerugian, dan memulihkan kedudukan korban.[47]

Jalur pidana tetap menjadi instrumen utama ketika *deepfake* digunakan dengan maksud memperoleh keuntungan secara melawan hukum, menimbulkan kerugian, atau memenuhi unsur delik lain. Namun, jalur pidana memiliki waktu proses yang relatif lebih panjang dibandingkan kebutuhan korban untuk segera menghentikan konten. Karena itu, jalur pidana perlu berjalan beriringan dengan mekanisme administratif dan teknis. Pada tahap awal, korban perlu memperoleh saluran pelaporan yang dapat menerima URL, akun, tangkapan layar, metadata, dan dokumen transaksi. Setelah itu, aparat atau pihak yang berwenang dapat

[44] Arvitto, *Implikasi Hukum Deepfake : Telaah Terhadap UU ITE Dan UU PDP (Legal Implications Of Deepfake : A Review Of The ITE Law And The PDP Law)*.
[45] Reza Dipta Prayitna Milka Kumala, Tuti Handayani, Muhammad Rizki, 2026, Civil and Criminal Liability of *Deepfake* AI Platform Providers in Violations of the Right to Reputation, *International Journal of Sustainable Law* 3, no. 1, https://doi.org/10.71131/0rqvry57.
[46] Meliala and Utari, *Policy on the Formulation of Artificial Intelligence Accountability for the Creation and Dissemination of Deepfake Videos from a Criminal Law Perspective in Indonesia.*
[47] Novianti, L. 2024. Metodologi penelitian hukum di era digital. *Gerechtikeit: Jurnal Riset Peradaban Hukum*, *1*(2), 55-59

melakukan preservasi bukti dan meminta penyedia platform mempertahankan data yang relevan dengan penyelidikan. Pola ini mencegah keadaan ketika konten telah dihapus oleh pengguna, tetapi salinan atau jejak digital yang penting untuk pembuktian juga ikut hilang.[48]

Jalur perdata mempunyai fungsi yang berbeda. Ketika korban mengalami kerugian materiil atau immateriil, gugatan ganti rugi dapat digunakan sebagai instrumen pemulihan sepanjang unsur perbuatan melawan hukum dapat dibuktikan. Jalur ini menjadi penting pada kasus yang tidak sepenuhnya dapat diselesaikan melalui pemidanaan, misalnya ketika kerugian korban timbul dari penggunaan identitas, reputasi, atau materi digital secara tidak sah. Pemulihan reputasi juga dapat membutuhkan tindakan yang lebih spesifik daripada sekadar putusan pidana, seperti pernyataan klarifikasi, penghentian pemuatan ulang, atau penghapusan materi yang terus dipublikasikan. Karena itu, penelitian ini menempatkan ganti rugi sebagai bagian dari tahap pemulihan, bukan sebagai pengganti pertanggungjawaban pidana.[49]

Sementara itu, jalur administratif dan mekanisme platform memiliki fungsi preventif dan remedial. Dalam praktik digital, kecepatan menjadi faktor penting karena dampak reputasional dan ekonomi dapat bertambah secara eksponensial ketika suatu konten memperoleh distribusi luas. Mekanisme pengaduan konten harus dapat membedakan antara konten yang sekadar salah informasi dan konten yang menggunakan identitas orang lain untuk memperoleh keuntungan. Pada kasus *deepfake* yang menyerang individu tertentu, platform seharusnya memiliki mekanisme prioritas untuk penyalahgunaan identitas, peniruan suara atau wajah, dan konten intim non-konsensual. Dengan demikian, model perlindungan korban tidak bergantung pada satu lembaga saja, tetapi merupakan sistem respons yang saling terhubung antara korban, platform, aparat penegak hukum, dan pengendali atau prosesor data.[50]

Pengamanan bukti merupakan tahapan yang menentukan kualitas proses hukum terhadap *deepfake*. Bukti awal yang dimiliki korban sering kali berupa video atau audio yang diterima melalui media sosial, pesan instan, atau platform berbagi konten. Bukti tersebut harus diperlakukan dengan hati-hati karena file dapat mengalami kompresi, perubahan format, penghilangan metadata, atau perubahan waktu unggah ketika dipindahkan dari satu perangkat ke perangkat lain. Karena itu, korban sebaiknya menyimpan file dalam bentuk asli apabila tersedia, mencatat tautan dan waktu akses, menyimpan tangkapan layar, serta tidak melakukan penyuntingan terhadap file asli. Tindakan sederhana tersebut dapat memperkuat kemampuan penyidik dan ahli untuk menilai autentisitas dan kronologi konten.[51]

---

[48] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.;Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2oo8 Tentang Informasi Dan Transaksi Elektronik.

[49] Republik Indonesia, Kitab Undang-Undang Hukum Perdata, Pasal 1365

[50] *Regulation - EU - 2024/1689 - EN - EUR-Lex*. (n.d.). Retrieved August 29, 2026, from https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.; *Provisions on the Administration of Deep Synthesis Internet Information Services*. (n.d.). Retrieved August 29, 2026, from https://www.chinalawtranslate.com/en/deep-synthesis/. Accesed 29-08-2026

[51] Paoli et al., A Qualitative Exploratory Study of the Knowledge , Forensic , and Legal Challenges from the Perspective of Police Cybercrime Specialists

Dari perspektif *digital forensics*, pemeriksaan *deepfake* sekurang-kurangnya mencakup verifikasi sumber file, analisis metadata, pemeriksaan jejak kompresi, perbandingan suara atau wajah, serta analisis konteks komunikasi yang menyertai file tersebut. Pemeriksa perlu menjawab apakah konten merupakan rekaman asli, hasil manipulasi, atau hasil *re-encoding* yang dapat menjelaskan perubahan teknis tertentu. Pemeriksaan tidak boleh hanya mengandalkan satu indikator karena perangkat lunak generatif terus berubah dan konten yang telah diedit berulang kali dapat kehilangan tanda-tanda manipulasi yang mudah dikenali. Oleh karena itu, kombinasi pemeriksaan teknis, keterangan ahli, bukti komunikasi, dan konteks transaksi lebih dapat dipertanggungjawabkan daripada hanya mengandalkan aplikasi pendeteksi *deepfake*.[52]

Konsep *chain of custody* juga perlu dipertegas. Setiap perpindahan barang bukti digital harus dicatat, termasuk siapa yang menerima, media penyimpanan yang digunakan, waktu penerimaan, metode penyalinan, serta nilai hash apabila pemeriksaan forensik dilakukan. Tujuannya bukan sekadar administratif, tetapi untuk menunjukkan bahwa bukti yang diajukan di persidangan merupakan bukti yang sama dengan yang diperoleh pada tahap awal. Aspek ini semakin penting karena lawan pembuktian dapat mempermasalahkan apakah suatu file telah diubah setelah diperoleh. Dengan dokumentasi yang baik, pemeriksaan ahli dapat diposisikan sebagai bagian dari proses pembuktian yang transparan dan dapat diuji.[53]

Pertanggungjawaban pidana pelaku dan perlindungan korban merupakan dua sisi yang saling berkaitan tetapi tidak identik. Pertanggungjawaban pidana terutama diarahkan untuk membuktikan bahwa pelaku memenuhi unsur delik dan dapat dimintai pertanggungjawaban. Sebaliknya, perlindungan korban berfokus pada kebutuhan korban agar kerugiannya berhenti, bukti tetap tersedia, privasi terjaga, dan proses pemulihan dapat berlangsung. Karena *deepfake* sering melibatkan beberapa aktor dan layanan digital, satu perkara dapat mengandung perbuatan yang berbeda: pembuat konten, pihak yang menyebarkan, pihak yang menggunakan konten untuk menipu, dan pihak yang memperoleh keuntungan. Analisis yang hanya mencari satu pelaku utama berisiko mengabaikan struktur perbuatan yang sebenarnya terjadi.[54]

Dalam konteks *cyber-fraud*, pihak yang menggunakan *deepfake* untuk meyakinkan korban agar mengirimkan uang memiliki konstruksi berbeda dari pihak yang membuat video *deepfake* untuk menjatuhkan reputasi seseorang. Keduanya dapat memiliki hubungan faktual, tetapi tidak otomatis memiliki unsur delik yang sama. Karena itu, penelitian normatif perlu menggunakan pendekatan berbasis perbuatan: pertama menentukan tujuan penggunaan *deepfake*, kedua mengidentifikasi tindakan yang dilakukan, ketiga menguji

[52] M Caldwell et al., 2020, AI - Enabled Future Crime, *Crime Science*, 1–13, https://doi.org/10.1186/s40163-020-00123-8.
[53] Paoli et al., A Qualitative Exploratory Study of the Knowledge , Forensic , and Legal Challenges from the Perspective of Police Cybercrime Specialists.
[54] Blauth, Gstrein, and Zwitter, *Artificial Intelligence Crime : An Overview of Malicious Use and Abuse of AI*.

akibat atau kerugian yang timbul, dan keempat menentukan norma yang paling tepat. Pendekatan ini mencegah penggunaan pasal secara berlebihan hanya karena suatu perbuatan terjadi melalui media elektronik.[55]

Model perlindungan yang telah dirumuskan dalam penelitian ini memiliki keunggulan karena menempatkan korban sebagai pusat respons hukum. Namun, efektivitasnya bergantung pada koordinasi kelembagaan. Tahap pencegahan memerlukan keterlibatan pemerintah dan platform; tahap pelaporan memerlukan prosedur yang sederhana; tahap preservasi bukti memerlukan kapasitas teknis; tahap penegakan hukum membutuhkan penyidik dan ahli; sedangkan tahap pemulihan memerlukan akses korban terhadap restitusi, ganti kerugian, perlindungan data, dan pendampingan. Apabila salah satu mata rantai tersebut tidak berfungsi, korban dapat tetap mengalami kerugian meskipun tersedia dasar hukum untuk menindak pelaku. Dengan demikian, efektivitas harus diukur melalui keseluruhan siklus perlindungan dan bukan hanya keberadaan norma pidana.[56]

Kelemahan lain terdapat pada perbedaan kecepatan antara teknologi dan proses hukum. Pembuatan *deepfake* dapat dilakukan dalam waktu singkat, sedangkan verifikasi, penyidikan, dan proses peradilan membutuhkan tahapan yang lebih panjang. Pelaku juga dapat menggunakan akun sementara, layanan lintas yurisdiksi, atau sarana pembayaran digital yang mempersulit atribusi. Oleh karena itu, ukuran efektivitas perlindungan korban harus mencakup kemampuan sistem untuk merespons secara cepat sekaligus tetap menjaga standar pembuktian. Kecepatan tidak boleh mengorbankan validitas barang bukti, sedangkan kehati-hatian tidak boleh menjadi alasan untuk membiarkan konten merugikan korban terus menyebar.[57]

Pengalaman Uni Eropa dan Tiongkok menunjukkan bahwa penguatan perlindungan korban dapat dilakukan melalui kewajiban transparansi dan tata kelola penyedia layanan, tidak hanya melalui pemberatan pidana. Pembelajaran tersebut relevan bagi Indonesia dalam merancang kewajiban penandaan atau pengungkapan konten sintetis, prosedur respons cepat terhadap penyalahgunaan identitas, dan mekanisme audit atau pencatatan tertentu untuk layanan generatif.[58]

Pembaruan hukum yang dibutuhkan bukan semata-mata penciptaan delik baru, tetapi juga penyusunan mekanisme perlindungan yang dapat bekerja sejak laporan pertama diterima. Norma baru, apabila dibentuk, idealnya memberikan definisi yang cukup jelas mengenai *synthetic* media atau *deepfake*, mengatur keadaan yang meningkatkan risiko pidana seperti penggunaan identitas orang lain untuk memperoleh keuntungan, serta membedakan konten berisiko tinggi dari penggunaan yang sah untuk seni, pendidikan, penelitian, atau satire. Pendekatan demikian dapat mengurangi dua risiko sekaligus, yaitu *overcriminalization* terhadap penggunaan

[55] Nugroho and An, Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries.
[56] Shereen Khan et al., 2025, A Systematic Literature Review on Cybercrime Legislation,, 1–19.
[57] Khan et al.
[58] European Union, Regulation (EU) 2024/1689; *Cyberspace Administration of China et al., Provisions on the Administration of Deep Synthesis.*

teknologi yang sah dan under-protection terhadap korban penyalahgunaan teknologi.[59]

Dari sisi perlindungan korban, pembaruan juga perlu mengatur hak atas informasi, mekanisme penghapusan atau pembatasan distribusi, preservasi data untuk kepentingan penegakan hukum, dan akses terhadap pemulihan. Korban seharusnya tidak dibebani seluruh tanggung jawab untuk mengidentifikasi pelaku atau mencari bukti teknis yang kompleks. Negara yang menyediakan platform perlu menyediakan prosedur yang memungkinkan korban menyerahkan informasi awal secara sederhana, kemudian proses autentikasi dan analisis teknis dilakukan oleh pihak yang memiliki kompetensi. Pengaturan tersebut akan membuat prinsip perlindungan korban lebih operasional dan mengurangi kesenjangan antara norma hukum dan realitas teknologi.[60]

Dengan demikian, hasil penelitian menunjukkan bahwa penguatan hukum *deepfake* harus dibangun melalui tiga lapisan. Lapisan pertama adalah hukum pidana materiil untuk memastikan terdapat kualifikasi perbuatan dan pertanggungjawaban yang tepat. Lapisan kedua adalah mekanisme prosedural dan pembuktian digital untuk memastikan penegakan hukum dapat dilakukan secara sah dan dapat diuji. Lapisan ketiga adalah sistem pemulihan korban yang mencakup penghentian penyebaran, perlindungan data dan identitas, pemulihan reputasi, serta kompensasi atau restitusi sesuai rezim hukum yang berlaku. Ketiga lapisan tersebut harus berjalan secara terintegrasi agar kehadiran hukum tidak berhenti pada kemampuan menghukum pelaku, melainkan benar-benar menghasilkan perlindungan yang efektif bagi korban.[61]

Konstruksi hukum yang telah diuraikan menunjukkan bahwa penanganan *deepfake* membutuhkan perubahan cara kerja penegakan hukum. Aparat tidak cukup menunggu laporan yang telah lengkap, karena korban sering kali tidak mempunyai kemampuan untuk mengidentifikasi teknik manipulasi atau menemukan pelaku. Pada tahap awal, aparat perlu membangun pola penerimaan laporan yang mampu mengubah informasi teknis sederhana menjadi bahan penyelidikan. URL, nama akun, waktu unggah, bentuk permintaan pembayaran, nomor rekening atau dompet digital, serta komunikasi yang menyertai konten dapat menjadi titik awal untuk membangun hubungan antara konten dan pelaku. Pendekatan ini sekaligus memperkuat posisi korban karena laporan tidak dipersyaratkan sudah memiliki pembuktian forensik yang lengkap sejak awal.[62]

Koordinasi antarlembaga juga menjadi faktor menentukan. Perkara *deepfake* yang berkaitan dengan kerugian finansial dapat memerlukan

[59] Noerman and Ibrahim, Kriminalisasi *Deepfake* Di Indonesia Sebagai Bentuk Pelindungan Negara.

[60] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.";"Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2oo8 Tentang Informasi Dan Transaksi Elektronik.

[61] Hidayat, Pertanggungjawaban Pidana Terhadap Penyalahgunaan *Deepfake* Sebagai Ancaman Keamanan Data Pribadi.

[62] *Polri dan Kementerian Komdigi Dukung Posbankum dalam Meningkatkan Literasi Hukum Digital*. (n.d.). Retrieved August 30, 2026, from https://bphn.go.id/berita-utama/polri-dan-kementerian-komdigi-dukung-posbankum-dalam-meningkatkan-literasi-hukum-digital. Accesed 29-08-2026

keterlibatan aparat penegak hukum, penyelenggara sistem elektronik, lembaga sektor keuangan, dan pengawas pelindungan data. Ketika konten digunakan untuk penipuan melalui identitas tokoh publik, penanganannya dapat memerlukan verifikasi fakta sekaligus penelusuran aliran transaksi. Sedangkan ketika *deepfake* mengandung materi seksual nonkonsensual, kebutuhan perlindungan korban menjadi lebih mendesak dan harus memperhatikan kerahasiaan identitas serta pemulihan korban. Diferensiasi tersebut menunjukkan bahwa kebijakan penegakan tidak boleh bersifat seragam untuk semua *deepfake*, melainkan harus mengikuti tujuan, objek, korban, dan akibat dari perbuatannya.[63]

Orientasi pada korban mensyaratkan agar proses hukum tidak menambah kerugian baru. Korban *deepfake* dapat mengalami tekanan karena harus mengulang kronologi, menyerahkan materi sensitif, atau berhadapan dengan pertanyaan yang menyentuh kehidupan privat. Oleh karena itu, prosedur penerimaan laporan dan pemeriksaan harus memperhatikan kebutuhan kerahasiaan dan meminimalkan penyebaran ulang materi yang menjadi alat serangan. Dalam kasus yang mengandung materi intim atau informasi pribadi, salinan untuk kepentingan penyidikan seharusnya dikelola secara terbatas dan hanya digunakan oleh pihak yang memiliki kewenangan. Perlindungan ini berkaitan langsung dengan prinsip pelindungan data dan hak korban atas rasa aman selama proses hukum berlangsung.[64]

Pemulihan reputasi juga harus dipahami sebagai proses, bukan hasil sekali jadi. Konten digital dapat disalin, diunggah kembali, diberi judul baru, atau dipotong sehingga membentuk konteks yang berbeda. Karena itu, pemulihan memerlukan kombinasi tindakan hukum, teknis, dan komunikasi publik. Tindakan hukum memberikan dasar untuk meminta pertanggungjawaban, tindakan teknis menurunkan akses terhadap konten yang merugikan, sedangkan komunikasi publik yang akurat membantu mengurangi dampak informasi palsu. Pada korban yang memiliki posisi publik, klarifikasi yang cepat dapat menjadi bagian dari mitigasi kerugian, tetapi tidak boleh menghilangkan tanggung jawab platform dan pelaku untuk menghentikan penyebaran.[65]

Selanjutnya, pemulihan kerugian perlu dibedakan antara kerugian yang dapat dihitung secara langsung dan kerugian yang bersifat non-ekonomis. Kerugian finansial dalam *cyber-fraud* relatif lebih mudah ditelusuri melalui bukti transaksi, rekening, atau pembayaran digital. Sebaliknya, kerugian terhadap reputasi, privasi, dan kondisi psikologis memerlukan pendekatan pembuktian yang berbeda. Karena penelitian ini menggunakan metode normatif, penilaian bukan dilakukan melalui

[63] Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana.

[64] Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2oo8 Tentang Informasi Dan Transaksi Elektronik.

[65] Bergerak Bersama Membangun Ruang Siber Aman: Belajar dari Pencegahan dan Penanganan Kekerasan Siber di Mancanegara. (n.d.). Retrieved August 30, 2026, from https://komnasperempuan.go.id/pengembangan-pengetahuan-detail/bergerak-bersama-membangun-ruang-siber-aman-belajar-dari-pencegahan-dan-penanganan-kekerasan-siber-di-mancanegara. Accesed 29-08-2026

pengukuran empiris terhadap korban, tetapi dengan melihat apakah sistem hukum menyediakan instrumen yang memadai untuk mengakui dan memulihkan kedua jenis kerugian tersebut. Hasil analisis menunjukkan perlunya integrasi antara pertanggungjawaban pidana, mekanisme ganti rugi, dan perlindungan korban agar kerugian tidak berhenti sebagai konsekuensi yang harus ditanggung korban sendiri.[66]

4. PENUTUP

4.1 Kesimpulan

1) Konstruksi pertanggungjawaban pidana terhadap penggunaan *deepfake* sebagai sarana *cyber-fraud* dalam hukum Indonesia pada prinsipnya telah mempunyai dasar normatif, tetapi bersifat fragmentaris. *Deepfake* yang digunakan untuk menggerakkan korban menyerahkan harta benda dapat dikonstruksikan sebagai penipuan berdasarkan Pasal 492 KUHP apabila unsur nama atau kedudukan palsu, tipu muslihat atau rangkaian kata bohong, maksud memperoleh keuntungan secara melawan hukum, dan tindakan korban terhadap harta benda terpenuhi. Pasal 35 UU ITE relevan terhadap manipulasi Informasi Elektronik dan/atau Dokumen Elektronik agar dianggap seolah-olah autentik, sedangkan UU PDP dapat diterapkan apabila penggunaan wajah, suara, atau data lain memenuhi unsur memperoleh, mengungkapkan, menggunakan, atau memalsukan Data Pribadi secara melawan hukum. Untuk *deepfake* yang memuat pencemaran, penghinaan, pornografi, atau kekerasan seksual berbasis elektronik, pasal yang digunakan harus dipilih sesuai muatan dan unsur deliknya. Dengan demikian, persoalan hukum bukan kekosongan total, melainkan kekosongan pengaturan khusus mengenai *synthetic impersonation* dan keterbatasan konsistensi penerapannya.
2) Model perlindungan korban yang efektif harus bersifat bertahap dan terintegrasi: pencegahan melalui literasi dan autentikasi; pelaporan cepat dan preservasi bukti; penghentian penyebaran melalui mekanisme platform dan prosedur penghapusan yang sah; penyidikan dengan *digital forensics dan chain of custody*; perlindungan data dan identitas korban; pemulihan reputasi dan psikologis; serta restitusi atau ganti kerugian sesuai dasar hukum yang tersedia. UU TPKS memberikan kerangka perlindungan yang kuat hanya untuk perkara yang memenuhi unsur kekerasan seksual berbasis elektronik, bukan untuk seluruh *deepfake*. Pengalaman Uni Eropa dan Tiongkok menunjukkan bahwa kewajiban pelabelan, penandaan teknis, verifikasi identitas, pengelolaan keamanan, dan kewajiban penyedia layanan dapat memperkuat perlindungan korban sejak tahap pencegahan. Oleh sebab itu, pembaruan hukum Indonesia perlu mengintegrasikan aspek pidana, pembuktian digital, tata kelola platform, dan pemulihan korban.

4.2 Saran

1. Pembentuk undang-undang perlu mempertimbangkan pengaturan khusus mengenai *deepfake* atau *synthetic impersonation* yang memuat definisi, bentuk

[66] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. ;Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual.

perbuatan, unsur kesalahan, hubungan dengan delik umum, kewajiban platform, tata kelola bukti digital, dan hak korban.

2. Penegak hukum perlu mengembangkan pedoman pemeriksaan bukti *deepfake* dan memperkuat kapasitas *digital forensics*, termasuk mekanisme kerja sama dengan penyelenggara sistem elektronik dan lembaga keuangan untuk preservasi log dan pelacakan transaksi serta pemerintah dan platform perlu memperkuat mekanisme pelaporan cepat, transparansi identitas konten, dan edukasi publik agar korban dapat melakukan verifikasi serta mengambil langkah protektif sebelum kerugian meluas.

DAFTAR PUSTAKA

Arvitto, Rafi Satrya. 2025, *Implikasi Hukum Deepfake* : Telaah Terhadap UU ITE Dan UU PDP (Legal Implications of *Deepfake* : A Review of the ITE Law and the PDP Law)" 4, no. 2. https://doi.org/10.35912/jihham.v4i2.3937.

Ayon Diniyanto, Iqbal Kamalludin. 2021, Menyelamatkan Korban Dari Jerat UU ITE: Studi Kasus Baiq Nuril Maknun Dan Relevansinya Bagi Penguatan Peran Pemerintah Melindungi Pelapor Tindak Asusila 10, no. 1. https://doi.org/10.14421/sh.v10i1.2341.

Blauth, Taís Fernanda, Oskar Josef Gstrein, and Andrej Zwitter. 2022, *Artificial Intelligence Crime : An Overview of Malicious Use and Abuse of AI* 10, no. June. https://doi.org/10.1109/ACCESS.2022.3191790.

Caldwell, M, J T A Andrews, T Tanay, and L D Griffin. 2020, AI - Enabled Future Crime. *Crime Science*. https://doi.org/10.1186/s40163-020-00123-8.

Cascavilla, Giuseppe, and Damian A Tamburri. 2021, Cybercrime Threat Intelligence : A Systematic Multi-Vocal Literature Review. *Computers & Security* 105: 102258. https://doi.org/10.1016/j.cose.2021.102258.

Hidayat, Muhammad Nur. 2025, Pertanggungjawaban Pidana Terhadap Penyalahgunaan *Deepfake* Sebagai Ancaman Keamanan Data Pribadi." *UNES Law Review* 7, no. 4 : 2036–48. https://doi.org/10.31933/unesrev.v7i4.2433.

Khakim, Lukman, and Nabila Nur Fadlilah. 2024, The Yogyakarta Police Overcoming Online Fraud Crimes 33, no. 2. https://doi.org/10.33369/jsh.33.2.124-136.

Khan, Shereen, Tajneen Saleh, Magiswary Dorasamy, Olivia Tan, Swee Leng, Rossanne Gale Vergara, and Nasreen Khan. 2025, *A Systematic Literature Review on Cybercrime Legislation.*

Kitab Undang-Undang Hukum Perdata

Lestari, Yuliannova, and M Misbahul Mujib. 2022, Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study). *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 11, no. 2 : 203–34. https://doi.org/10.14421/sh.v11i2.2729.

Liswati, Anggi Lia, Taun. 2025, *Analisis Yuridis Terhadap Pertanggungjawaban Pidana Pelaku Pelecehan Seksual Berbasis Al (Deepfake Pornografi) Di Media Sosial 2*, no. 6. https://doi.org/10.62383/hukum.v2i6.742.

Mahmud Marzuki, Peter. 2005, *Penelitian Hukum*. Jakarta: Kencana Prenada Media.

Marzuki, Peter Mahmud. 2017, *Penelitian Hukum*. Kencana.

Meliala, Athalia Pranata Putri S, and Indah Sri Utari. 2026, Policy on the Formulation of Artificial Intelligence Accountability for the Creation and Dissemination of

Deepfake Videos from a Criminal Law Perspective in Indonesia. *Law Research Review Quarterly* 12, no. 2. https://doi.org/10.15294/lrrq.v12i2.44714.

Milka Kumala, Tuti Handayani, Muhammad Rizki, Reza Dipta Prayitna. 2026, Civil and Criminal Liability of *Deepfake* AI Platform Providers in Violations of the Right to Reputation. *International Journal of Sustainable Law* 3, no. 1. https://doi.org/10.71131/0rqvry57.

Muhammad Safei, Sandra Dewi, Olivia Anggie Johar. 2025, *Implementasi Pada Alat Bukti Jejak Digital Dalam Penegakan Hukum Tindak Pidana Penipuan Online* 8, no. 2.

Noerman, Chiquita Thefirstly, and Aji Lukman Ibrahim. 2024, Kriminalisasi *Deepfake* Di Indonesia Sebagai Bentuk Pelindungan Negara 7, no. 2 : 1–4.

Nugroho, Agus, and An An. 2023, Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries. *Security Journal* 36, no. 4 : 651–70. https://doi.org/10.1057/s41284-022-00357-y.

Paoli, Stefano De, Jason Johnstone, Natalie Coull, Ian Ferguson, Georgina Sinclair, Patrick Tomkins, Maureen Brown, and Rebecca Martin. 2020, A Qualitative Exploratory Study of the Knowledge , Forensic , and Legal Challenges from the Perspective of Police Cybercrime Specialists 15, no. 2. https://doi.org/10.1093/police/paaa027.

Romadhony, Muhammad Rizqy. 2019, *Mekanisme Penyidikan Tindak Pidana Manipulasi Data Transaksi Grab Di Polres Lamongan* 8, no. 1. https://doi.org/10.14421/sh.v8i1.2047.

Sandoval, Maria-Paz, Maria de Almeida Vau, John Solaas, and Luano Rodrigues. 2024, Threat of *Deepfake*s to the Criminal Justice System: A Systematic Review. *Crime Science* 13. https://doi.org/10.1186/s40163-024-00239-1.

Satrul, Hairul Saleh, and Nur Hafizal Hasanah. 2026, Reconstruction of Criminal Liability for *Deepfake* Misuse in Defamatory Defenses in Indonesia. *Rechtsvinding*. https://doi.org/10.59525/rechtsvinding.1541.

https://bphn.go.id/berita-utama/polri-dan-kementerian-komdigi-dukung-posbankum-dalam-meningkatkan-literasi-hukum-digital.

https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

https://jalahoaks.jakarta.go.id/detail/HOAKS-Pengumuman-Pemenang-Giveway-Baim-Wong.

https://komnasperempuan.go.id/pengembangan-pengetahuan-detail/bergerak-bersama-membangun-ruang-siber-aman-belajar-dari-pencegahan-dan-penanganan-kekerasan-siber-di-mancanegara.

https://www.chinalawtranslate.com/en/deep-synthesis/

Kementerian Komunikasi Dan Digital, n.d. https://www.komdigi.go.id/berita/berita-hoaks/detail/hoaks-video-kampanye-jokowi-amin-berbahaa-mandarin.

Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual, N.D.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana, No. 16100.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2oo8 Tentang Informasi Dan Transaksi Elektronik, No. 190185.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, No. 016999.