Law Studies and Justice Journal (LAJU)
Vol 3 (3) 2026 : 688-696

THE EFFECTIVENESS OF LAW ENFORCEMENT AGAINST ARTIFICIAL INTELLIGENCE-BASED FRAUD CRIMES IN INDONESIA

EFEKTIVITAS PENEGAKAN HUKUM TERHADAP TINDAK PIDANA PENIPUAN BERBASIS ARTIFICIAL INTELLIGENCE DI INDONESIA

Chrysna Andrew Saputra, Selvia Intan Sari, Aufa Raissa Farrell, Lulu Aoudita

Mahasiswa Fakultas Hukum, Universitas Pamulang
*krisnapak675@gmail.com, selvia.intansari.sh@gmail.com, aufaraissafarrell06@gmail.com, Auoditalulu304@gmail.com

**Corresponding Author*

ABSTRACT

Generative artificial intelligence, particularly voice and face deepfakes, has changed how fraud is committed by making impersonation cheap and highly convincing. This article assesses the effectiveness of law enforcement against AI-based fraud in Indonesia using a normative juridical method supported by secondary performance data. It applies Soekanto's five factors of law enforcement and Friedman's legal system framework. The findings indicate that AI-based fraud is not yet a distinct offence but can be reached through Article 492 of the 2023 Penal Code (in force since 2 January 2026), Articles 28(1) and 35 of the Electronic Information and Transactions Law, and the Personal Data Protection Law. The central problem is therefore legal uncertainty in classification and the absence of aggravation, not a total regulatory vacuum. Repressive enforcement is moderately effective in detected cases, whereas preventive and restorative effectiveness remains low: as of 14 January 2026 only about 4.7 percent of reported losses had been blocked, and by 30 September 2026 about 25.5 percent of blocked funds had been returned to victims. The article recommends legal certainty reforms, faster cross-institutional intervention, stronger digital forensics, platform accountability, and public literacy.
Keywords: law enforcement; fraud; artificial intelligence; deepfake; cybercrime

ABSTRAK

Perkembangan kecerdasan artifisial (artificial intelligence/AI) generatif, khususnya teknologi deepfake suara dan wajah, mengubah cara pelaku menjalankan penipuan: kepercayaan korban kini dapat dipalsukan secara meyakinkan dengan biaya rendah. Artikel ini menilai efektivitas penegakan hukum terhadap tindak pidana penipuan berbasis AI di Indonesia dengan metode yuridis normatif yang dilengkapi data sekunder kinerja penanganan penipuan digital. Analisis memakai teori faktor-faktor penegakan hukum Soerjono Soekanto dan kerangka sistem hukum Lawrence M. Friedman. Hasil kajian menunjukkan tiga hal. Pertama, penipuan berbasis AI belum diatur sebagai delik tersendiri, tetapi dapat dijangkau melalui Pasal 492 UU No. 1 Tahun 2023 (KUHP Nasional, berlaku sejak 2 Januari 2026), Pasal 28 ayat (1) dan Pasal 35 UU ITE, serta UU Perlindungan Data Pribadi, sehingga masalah utamanya bukan kekosongan total, melainkan ketidakpastian kualifikasi dan ketiadaan pemberatan. Kedua, efektivitas represif tergolong sedang pada kasus yang terungkap, tetapi efektivitas preventif dan restoratif masih rendah: per 14 Januari 2026 dana yang berhasil diblokir hanya sekitar 4,7 persen dari kerugian yang dilaporkan ke Indonesia Anti-Scam Centre, dan per 30 September 2026 hanya sekitar 25,5 persen dana terblokir yang telah dikembalikan. Ketiga, penguatan perlu bertumpu pada kepastian norma, kecepatan intervensi lintas lembaga, kapasitas forensik digital, tanggung jawab platform, dan literasi masyarakat.
Kata kunci: penegakan hukum; penipuan; kecerdasan artifisial; deepfake; kejahatan siber

1. PENDAHULUAN

Penipuan selalu bertumpu pada satu unsur: kepercayaan korban terhadap identitas dan pernyataan pelaku. Kecerdasan artifisial generatif melemahkan fondasi itu. Wajah, suara, dan gaya bicara seorang pejabat atau anggota keluarga kini dapat ditiru melalui *deepfake* sehingga korban sulit membedakan yang asli dari yang palsu. Di Indonesia, dampaknya tampak pada dua tingkat. Pada tingkat kasus, Direktorat Tindak Pidana Siber Bareskrim Polri pada Januari 2025 mengungkap

LAJU,3 (3) 2026 : 688-696, https://journal.ppipbr.com/index.php/laju | DOI: https://doi.org/10.62207/2apv9j94
Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.

penipuan yang memakai video *deepfake* wajah dan suara pejabat negara untuk menjanjikan bantuan dana, dengan penyidik mengidentifikasi sebelas korban dan hasil laboratorium forensik menyatakan materi tersebut seluruhnya palsu (Liputan6, 2025a, 2025b). Pada tingkat sistem, Indonesia Anti-Scam Centre (IASC) milik Otoritas Jasa Keuangan (OJK) mencatat 702.342 laporan penipuan transaksi keuangan sejak beroperasi pada 22 November 2024 hingga 30 September 2026 (GARTONnews, 2026).

Pada saat yang sama, kerangka hukum Indonesia sedang berganti. KUHP Nasional (UU No. 1 Tahun 2023) dan KUHAP baru (UU No. 20 Tahun 2025) mulai berlaku pada 2 Januari 2026, diikuti UU No. 1 Tahun 2026 tentang Penyesuaian Pidana (Mahkamah Agung RI, 2026). Di sisi tata kelola AI, dua rancangan Peraturan Presiden, yakni peta jalan AI nasional dan etika AI, menurut keterangan Kementerian Komunikasi dan Digital pada 30 Oktober 2026 masih berada pada tahap penandatanganan (CNBC Indonesia, 2026). Artinya, aparat menegakkan hukum atas kejahatan teknologi baru dengan instrumen pidana yang juga baru dan dengan payung tata kelola AI yang belum final.

Sebagian kajian terdahulu masih berpijak pada Pasal 378 KUHP lama dan UU ITE ketika membahas penipuan *deepfake*, misalnya kajian tentang pertanggungjawaban platform dalam kasus penipuan berkedok ritual uang gaib (Jurnal Progres, 2025). Kajian lain menyoroti ketiadaan definisi teknis *deepfake* dan persoalan asas kepastian hukum (*lex certa*) berdasarkan telaah lima belas putusan pengadilan periode 2023–2025 (Jurnal USM Law Review, 2025). Artikel ini melengkapi literatur tersebut dengan menilai efektivitas, bukan hanya kecukupan norma, dalam rezim hukum pidana yang baru berlaku, dan dengan memadukan analisis normatif dengan data kinerja penanganan penipuan digital.

1.2 Rumusan Masalah

1. Bagaimana kualifikasi yuridis dan dasar pemidanaan tindak pidana penipuan berbasis AI dalam hukum positif Indonesia?
2. Seberapa efektif penegakan hukum terhadap penipuan berbasis AI jika dinilai berdasarkan faktor hukum, penegak hukum, sarana, masyarakat, dan budaya?
3. Langkah penguatan apa yang perlu ditempuh agar penegakan hukum lebih efektif?

2. METODE PENELITIAN

Penelitian ini berjenis yuridis normatif (Marzuki, 2017) dengan tiga pendekatan: pendekatan perundang-undangan, pendekatan kasus, dan pendekatan konseptual. Bahan hukum primer meliputi UU No. 1 Tahun 2023 tentang KUHP, UU No. 1 Tahun 2024 (perubahan kedua UU ITE), UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, UU No. 20 Tahun 2025 tentang KUHAP, dan UU No. 1 Tahun 2026 tentang Penyesuaian Pidana. Bahan hukum sekunder berupa artikel jurnal nasional, siaran pers resmi OJK, dan keterangan resmi aparat penegak hukum. Data kuantitatif berasal dari publikasi OJK dan dikutip melalui pemberitaan yang memuat pernyataan resmi pimpinan OJK, kemudian dihitung ulang secara sederhana untuk memperoleh rasio indikatif.

Analisis bersifat kualitatif deskriptif-preskriptif dengan kerangka teori faktor-faktor yang mempengaruhi penegakan hukum (Soekanto, 2008), yaitu faktor hukum, penegak hukum, sarana atau fasilitas, masyarakat, dan kebudayaan, serta kerangka sistem hukum Friedman (1975) yang membedakan struktur, substansi, dan budaya hukum. Efektivitas dinilai melalui lima indikator: kepastian norma, penindakan terhadap pelaku, kecepatan intervensi, pemulihan kerugian korban, dan pencegahan.

Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.

Penelitian memiliki batasan yang perlu dinyatakan. Pertama, data diakses sampai 1 November 2026. Kedua, publikasi IASC yang ditelaah tidak memilah laporan berdasarkan penggunaan AI, sehingga angka nasional mencerminkan penipuan digital secara umum dan dipakai sebagai gambaran kapasitas sistem, bukan sebagai angka penipuan AI semata. Ketiga, kasus dianalisis dari keterangan resmi dan pemberitaan, bukan dari berkas putusan.

3. HASIL DAN PEMBAHASAN

3.1 Kualifikasi Yuridis Penipuan Berbasis AI

Hukum pidana Indonesia tidak menyebut AI atau *deepfake* sebagai unsur delik penipuan. Karena itu, penipuan berbasis AI lebih tepat dipahami sebagai penipuan konvensional yang dilakukan dengan sarana baru. Pasal 492 UU No. 1 Tahun 2023, pengganti Pasal 378 KUHP lama, mengatur penipuan dengan ancaman pidana penjara paling lama empat tahun atau denda paling banyak kategori V, yaitu Rp500 juta. Rumusan deliknya memuat sarana berupa nama palsu atau kedudukan palsu, tipu muslihat, dan rangkaian kata bohong untuk menggerakkan orang menyerahkan sesuatu. *Deepfake* yang meniru identitas pejabat termasuk dalam cakupan nama palsu dan kedudukan palsu, sedangkan video atau suara hasil rekayasa dapat dipandang sebagai tipu muslihat. Pada titik ini norma yang ada pada dasarnya sudah mampu menjangkau perbuatan tersebut.

Tabel 1 memetakan perbuatan yang lazim muncul dalam penipuan berbasis AI dengan norma yang dapat dikenakan.

Tabel 1. Pemetaan perbuatan dan norma yang dapat dikenakan

Perbuatan	Norma yang dapat dikenakan	Ancaman pidana
Meniru wajah atau suara pejabat atau orang dikenal untuk membujuk korban menyerahkan uang	Pasal 492 UU No. 1 Tahun 2023	Penjara maksimal 4 tahun atau denda kategori V (Rp500 juta)
Menyebarkan informasi bohong atau menyesatkan yang merugikan konsumen dalam transaksi elektronik	Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE (UU No. 1 Tahun 2024)	Penjara maksimal 6 tahun dan/atau denda maksimal Rp1 miliar; terbatas pada korban berstatus konsumen
Merekayasa informasi elektronik agar tampak seolah-olah data otentik	Pasal 35 jo. Pasal 51 ayat (1) UU ITE	Penjara maksimal 12 tahun dan/atau denda maksimal Rp12 miliar
Memakai foto, suara, atau data pribadi orang lain tanpa hak	Pasal 65 ayat (3) jo. Pasal 67 ayat (3) UU No. 27 Tahun 2022 (UU PDP)	Penjara maksimal 5 tahun dan/atau denda maksimal Rp5 miliar
Menyamarkan atau mengalirkan hasil penipuan	UU No. 8 Tahun 2010 tentang TPPU	Membuka jalur pelacakan dan perampasan aset

Sumber: Data Diolah, 2026

Praktik penyidikan memang memadukan norma-norma tersebut. Kajian atas kasus penipuan *deepfake* berkedok ritual uang gaib menyimpulkan bahwa pelaku dapat dijerat dengan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE dan Pasal 378 KUHP (Jurnal Progres, 2025), dan setelah 2 Januari 2026 padanan Pasal 378 adalah Pasal 492 KUHP Nasional.

Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.

Namun, tiga persoalan kualifikasi tampak dari pemetaan ini. Pertama, Pasal 28 ayat (1) UU ITE mensyaratkan kerugian materiel bagi konsumen dalam transaksi elektronik (Hukumonline, n.d.). Penipuan dengan modus bantuan dana atau hadiah yang dibawakan oleh wajah pejabat palsu tidak selalu berstatus transaksi perdagangan, sehingga penerapannya bisa diperdebatkan. Kedua, tidak ada pemberatan pidana ketika AI dipakai untuk memperbesar daya tipu dan jangkauan korban, padahal sifat berbahaya perbuatan itu lebih tinggi daripada penipuan biasa. Ketiga, studi atas putusan 2023–2025 menemukan bahwa pengaturan yang ada masih reaktif dan belum memuat definisi teknis *deepfake* sehingga sulit memenuhi asas *lex certa* (Jurnal USM Law Review, 2025). Penulis menilai ketiga persoalan ini, bukan ketiadaan norma sama sekali, yang menjadi sumber ketidakpastian pada tahap penyidikan dan penuntutan.

Dari sisi pembuktian, informasi dan dokumen elektronik diakui sebagai alat bukti dalam UU ITE. Mahkamah Konstitusi dalam Putusan No. 20/PUU-XIV/2016 tanggal 7 September 2016 menafsirkan bahwa informasi dan dokumen elektronik sebagai alat bukti harus diperoleh dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lain yang ditetapkan undang-undang (Prahassacitta, 2016). Karena itu, cara perolehan dan pemeriksaan laboratorium forensik digital menjadi penentu, sebagaimana tampak pada kasus Januari 2025 ketika hasil laboratorium forensik menyatakan seluruh materi video palsu hasil *deepfake* (Liputan6, 2025b).

3.2 Penilaian Efektivitas Berdasarkan Lima Faktor Penegakan Hukum

a. Faktor Hukum

Dari sisi keberadaan norma, aparat tidak menghadapi kekosongan hukum yang menghalangi penindakan. Akan tetapi, kualitas norma belum memadai: tidak ada definisi deepfake, tidak ada pemberatan, dan tidak ada kewajiban pelabelan konten sintetis. Gagasan kewajiban label pada produk yang dihasilkan AI memang termuat dalam rancangan Perpres Etika AI, tetapi rancangan itu belum ditandatangani per akhir Oktober 2026 (CNBC Indonesia, 2026). Sebagai pembanding, Uni Eropa melalui Regulation (EU) 2024/1689 mendefinisikan deep fake pada Pasal 3 angka 60 dan mewajibkan pihak yang menggunakan sistem AI untuk menghasilkan atau memanipulasi konten tersebut mengungkapkan sifat buatannya (Pasal 50 ayat (4)) (European Parliament & Council of the European Union, 2024). Pembaruan hukum pidana nasional dan UU Penyesuaian Pidana menyelaraskan sistem pidana, termasuk pemidanaan korporasi (Mahkamah Agung RI, 2026), tetapi belum menjawab kekhususan sarana AI.

b. Faktor Penegak Hukum

Kapasitas penindakan terbukti ada. Dittipidsiber Bareskrim Polri mengungkap kasus deepfake yang mencatut Presiden dan sejumlah pejabat, menangkap tersangka di Lampung Tengah, lalu melimpahkan tersangka dan barang bukti ke kejaksaan. Di tingkat daerah, Polda Jawa Timur mengungkap kasus deepfake yang mencatut nama Gubernur Jawa Timur melalui media sosial dan menangkap tiga tersangka di Pangandaran (Antara, 2025). Pada kasus lain, tersangka berinisial JS disebut memperoleh keuntungan Rp65 juta dari penipuan berkedok bantuan pendanaan yang memakai wajah pejabat (Antara Foto, 2025).

Meski demikian, pola kasus yang terungkap tampak berpusat pada konten yang mencatut tokoh publik dan terdeteksi lewat patroli siber, sehingga menurut penulis ada risiko bahwa penipuan AI yang menyasar korban perorangan melalui panggilan suara atau video pribadi lebih sulit terdeteksi. Hal ini merupakan inferensi analitis, bukan temuan empiris. Kajian akademik juga mencatat bahwa penegakan hukum atas deepfake menuntut peningkatan kapasitas teknologi aparat, mulai dari identifikasi hingga investigasi (Darmawan et al., 2025), dan hambatan pembuktian forensik

Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.

digital serta rendahnya kemampuan memverifikasi konten berbasis AI disebut sebagai penyebab ketidakefektifan yang sistemik (Jurnal USM Law Review, 2025).

c. Faktor Sarana dan Fasilitas

IASC merupakan sarana terpenting dalam penanganan penipuan keuangan digital karena mempertemukan korban, lembaga keuangan, dan OJK dalam satu mekanisme pemblokiran rekening. Hingga 30 September 2026, IASC menerima 702.342 laporan, memverifikasi 1.372.483 rekening yang dilaporkan, dan memblokir 702.833 rekening di antaranya; dana korban yang berhasil diblokir mencapai Rp 811,1 miliar (GARTONnews, 2026). Capaian ini nyata, tetapi perbandingan dengan skala kerugian menunjukkan batasnya.

Per 14 Januari 2026, OJK melaporkan kerugian Rp9,1 triliun dengan dana yang berhasil diblokir atau diselamatkan Rp432 miliar (Law-justice.co, 2026), atau sekitar 4,7 persen. Pada 30 September 2026, dari Rp811,1 miliar dana terblokir, Rp207,16 miliar telah dikembalikan kepada korban (GARTONnews, 2026), atau sekitar 25,5 persen. Kedua rasio ini adalah hasil perhitungan penulis dari angka kumulatif pada tanggal yang sama dan bersifat indikatif, karena data tersebut mencakup seluruh penipuan digital, bukan hanya yang berbasis AI. Hambatan utamanya adalah kecepatan: sekitar 80 persen laporan disampaikan lebih dari 12 jam setelah kejadian, sedangkan dana hasil penipuan dapat berpindah keluar dari rekening dalam waktu kurang dari satu jam (Law-justice.co, 2026). Jarak waktu antara kecepatan pelaku dan kecepatan sistem inilah yang menurut penulis menjelaskan rendahnya rasio pemulihan.

d. Faktor Masyarakat

Jumlah laporan yang tinggi menunjukkan kesadaran melapor yang tumbuh, tetapi keterlambatan pelaporan menandakan bahwa korban belum menjadikan pelaporan segera sebagai refleks. Dari 702.342 laporan, 367.586 disampaikan langsung oleh korban melalui IASC dan 334.756 melalui bank dan penyedia sistem pembayaran (GARTONnews, 2026). Di tingkat daerah, OJK Daerah Istimewa Yogyakarta mencatat lebih dari 12.000 laporan dengan kerugian lebih dari Rp100 miliar hingga akhir September 2026 dan memfokuskan edukasi pada pelajar yang aktif menggunakan gawai (ANTARA, 2026). Literasi digital yang rendah juga disebut sebagai faktor yang memperbesar kerentanan korban deepfake (Jurnal USM Law Review, 2025).

e. Faktor Kebudayaan

Penipuan berbasis AI bekerja pada budaya kepercayaan terhadap figur otoritas: korban lebih mudah percaya ketika pesan tampak datang dari pejabat atau tokoh yang dikenal. Pada kasus yang diungkap Bareskrim, modusnya adalah video bantuan uang yang kemudian meminta korban mentransfer biaya administrasi (Antara, 2025). Perlu dicatat pula kehati-hatian metodologis: seorang narasumber ahli yang dikutip media menyatakan bahwa banyak penipuan yang beredar tidak memakai AI, melainkan rekayasa sosial (Liputan6, 2025c). Ini berarti pengukuran penipuan berbasis AI sulit dilakukan tanpa pencatatan yang memilah modus, dan kebijakan penegakan hukum seharusnya mulai dari pembenahan data.

3.3 Sintesis: Efektivitas yang Parsial

Berdasarkan lima indikator yang ditetapkan pada bagian metode, penulis menyimpulkan bahwa efektivitas penegakan hukum bersifat parsial. Penilaian pada Tabel 2 merupakan penilaian analitis penulis berdasarkan data yang ditelaah, bukan hasil pengukuran kuantitatif baku.

Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.

Tabel 2. Penilaian efektivitas penegakan hukum (analisis penulis)

Indikator	Penilaian	Dasar penilaian
Kepastian norma	Sedang	Norma tersedia (Pasal 492 KUHP, UU ITE, UU PDP), tetapi tanpa definisi dan pemberatan
Penindakan terhadap pelaku	Sedang	Kasus berprofil tinggi terungkap dan dilimpahkan, tetapi cakupannya tampak selektif
Kecepatan intervensi	Rendah	Sekitar 80% laporan terlambat lebih dari 12 jam; dana dapat berpindah kurang dari 1 jam
Pemulihan kerugian	Rendah	Dana terblokir sekitar 4,7% dari kerugian; yang dikembalikan sekitar 25,5% dari dana terblokir
Pencegahan	Rendah	Perpres AI belum terbit, belum ada kewajiban pelabelan, literasi masih terbatas

Sumber: Data Diolah, 2026

Dalam kerangka Friedman (1975), substansi hukum sudah tersedia dalam bentuk dasar, tetapi struktur (kapasitas lembaga dan koordinasi) dan budaya hukum (kecepatan melapor, literasi) belum mengimbangi kecepatan kejahatan. Dengan kata lain, hambatan terbesar ada pada kecepatan dan koordinasi, bukan semata pada banyaknya pasal.

3.4 Arah Penguatan

Berdasarkan temuan di atas, penulis mengajukan lima langkah yang saling melengkapi.

1. **Kepastian norma**

Pembentuk undang-undang perlu mempertimbangkan definisi teknis konten sintetis dan pemberatan pidana bagi penipuan yang memakai rekayasa identitas berbasis AI, dengan tetap menjaga keseimbangan antara perlindungan korban dan kebebasan berekspresi sebagaimana diingatkan kajian terdahulu (Jurnal USM Law Review, 2025). Sambil menunggu perubahan norma, kepolisian dan kejaksaan dapat menyusun pedoman teknis bersama tentang pemilihan pasal untuk kasus penipuan berbasis AI agar tidak terjadi disparitas.

2. **Kecepatan intervensi**

Mekanisme pemblokiran rekening dan penundaan transaksi perlu didorong ke arah respons hampir seketika, dengan dasar kewenangan dan standar waktu yang jelas bagi bank, penyedia sistem pembayaran, OJK, PPATK, dan kepolisian. Mekanisme ini harus disertai jaminan prosedural bagi pemilik rekening yang diblokir.

3. **Kapasitas forensik**

Investasi pada laboratorium forensik digital, alat deteksi konten sintetis, dan pelatihan penyidik, penuntut umum, dan hakim, sejalan dengan rekomendasi kajian tentang kapasitas aparat (Darmawan et al., 2025).

4. **Tanggung jawab platform**

Penetapan Perpres Etika AI beserta kewajiban pelabelan konten AI perlu dipercepat, dan kewajiban platform untuk menurunkan konten penipuan secara cepat perlu dipertegas. Pertanggungjawaban platform dalam penyebaran konten *deepfake* penipuan sudah mulai dikaji dalam literatur (Jurnal Progres, 2025), tetapi belum memiliki rumusan norma yang tegas.

Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.

5. Literasi, data, dan kerja sama internasional

Edukasi tentang verifikasi identitas lintas saluran, pembiasaan pelaporan segera, serta pencatatan modus yang memilah penggunaan AI pada sistem pelaporan nasional agar kebijakan dapat diukur. Kerja sama internasional juga penting: Konvensi PBB menentang Kejahatan Siber yang diadopsi Majelis Umum PBB pada 24 Desember 2024 bertujuan memperkuat kerja sama internasional dalam pertukaran bukti elektronik (United Nations General Assembly, 2024), dan OJK sendiri menekankan pertukaran informasi yang cepat serta kolaborasi lintas sektor dan lintas negara dalam penanganan *scam* (OJK, 2026b).

4. PENUTUP

4.1 Simpulan

Pertama, penipuan berbasis AI di Indonesia dapat dijerat melalui Pasal 492 KUHP Nasional, Pasal 28 ayat (1) dan Pasal 35 UU ITE, serta UU Perlindungan Data Pribadi, tetapi belum ada definisi, pemberatan, dan kewajiban pelabelan yang spesifik, sehingga ketidakpastian kualifikasi menjadi persoalan utama. Kedua, efektivitas penegakan hukum bersifat parsial: penindakan terhadap pelaku yang terungkap berjalan, sedangkan kecepatan intervensi, pemulihan kerugian, dan pencegahan masih lemah, tercermin dari dana terblokir sekitar 4,7 persen dari kerugian yang dilaporkan dan dana kembali sekitar 25,5 persen dari dana terblokir. Ketiga, penguatan perlu menyentuh norma, kecepatan lintas lembaga, kapasitas forensik, tanggung jawab platform, dan literasi masyarakat secara bersamaan.

4.2 Saran

Pemerintah dan DPR disarankan mempertimbangkan penguatan norma yang spesifik terhadap rekayasa identitas berbasis AI dan segera menetapkan Perpres Etika AI. Kepolisian, kejaksaan, OJK, PPATK, dan penyelenggara sistem pembayaran disarankan menyusun protokol bersama untuk pembekuan dana secara cepat. Penelitian lanjutan disarankan menggunakan data putusan pengadilan dan wawancara dengan penyidik, jaksa, dan korban untuk menguji temuan normatif artikel ini secara empiris.

5. DAFTAR PUSTAKA

ANTARA. (2026, 16 Oktober). OJK DIY catat laporan "scam" tembus 12 ribu kasus. https://m.antaranews.com/amp/berita/5791765/ojk-diy-catat-laporan-scam-tembus-12-ribu-kasus

Antara. (2025). Bareskrim sebut telah limpahkan kasus "deepfake" pejabat ke kejaksaan. https://www.antaranews.com/berita/4792345/bareskrim-sebut-telah-limpahkan-kasus-deepfake-pejabat-ke-kejaksaan

Antara Foto. (2025, 7 Februari). Ungkap kasus deepfake AI pejabat negara. https://www.antarafoto.com/id/view/2443117/ungkap-kasus-deepfake-ai-pejabat-negara

CNBC Indonesia. (2026, 30 Oktober). RI atur AI sesuai risiko, Komdigi beberkan isi regulasinya. https://www.cnbcindonesia.com/tech/20261030162941-37-781009/ri-atur-ai-sesuai-risiko-komdigi-beberkan-isi-regulasinya

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan hukum terhadap penyalahgunaan deepfake pada pornografi anak di era artificial intelligence di Indonesia. Jurnal Penelitian Serambi Hukum, 18(1), 42–54. https://www.journal.uniba.ac.id/index.php/SH/article/view/1257

Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Friedman, L. M. (1975). The legal system: A social science perspective. Russell Sage Foundation.

GARTONnews. (2026). IASC terima 702 ribu laporan penipuan, OJK berhasil kembalikan dana korban Rp207,16 miliar. https://www.gartonnews.com/nasional/amp/102917772384/iasc-terima-702-ribu-laporan-penipuan-ojk-berhasil-kembalikan-dana-korban-rp20716-miliar

Hukumonline. (n.d.). Cara menentukan pasal untuk menjerat pelaku penipuan online. https://www.hukumonline.com/klinik/a/cara-menentukan-pasal-untuk-menjerat-pelaku-penipuan-ionline-i-lt5d1ad428d8fa3/

Jurnal Progres. (2025). Pertanggung jawaban hukum platform media sosial terhadap penyebaran konten deepfake berbasis artificial intelligence dalam kasus penipuan berkedok ritual uang gaib Ujang Busthomi. https://journal.lpkd.or.id/index.php/Progres/article/view/3110

Jurnal USM Law Review. (2025). Deepfake sebagai bentuk kejahatan siber baru: Tantangan kriminalisasi dalam hukum pidana Indonesia. Jurnal USM Law Review, 8(3), 2421–2445. https://journals.usm.ac.id/index.php/julr/article/view/13060

Law-justice.co. (2026). OJK ungkap kerugian triliunan akibat scam. https://www.law-justice.co/artikel/203152/ojk-ungkap-kerugian-triliunan-akibat-scam/

Liputan6. (2025a, 23 Januari). Polisi tangkap pelaku penipuan deepfake video wajah Prabowo. https://www.liputan6.com/news/read/5893778/polisi-tangkap-pelaku-penipuan-deepfake-video-wajah-prabowo

Liputan6. (2025b, 26 Januari). 5 fakta terkait polisi tangkap pelaku penipuan AI deepfake, catut nama Prabowo, Gibran, hingga Sri Mulyani. https://www.liputan6.com/news/read/5896373/5-fakta-terkait-polisi-tangkap-pelaku-penipuan-ai-deepfake-catut-nama-prabowo-gibran-hingga-sri-mulyani

Liputan6. (2025c, 23 Januari). Polisi ungkap penipuan modus teknologi AI deepfake, catut pejabat negara. https://www.liputan6.com/news/read/5892824/polisi-ungkap-penipuan-modus-teknologi-ai-deepfake-catut-pejabat-negara

Mahkamah Agung RI. (2026). Transisi hukum pidana baru. MariNews. https://marinews.mahkamahagung.go.id/artikel/transisi-hukum-pidana-baru-0Ng

Marzuki, P. M. (2017). Penelitian hukum (Edisi revisi). Prenadamedia Group.

Mahkamah Konstitusi Republik Indonesia. (2016). Putusan Nomor 20/PUU-XIV/2016 (7 September 2016).

Otoritas Jasa Keuangan. (2026a, 21 Januari). Siaran pers SP 15/GKPB/OJK/I/2026: Indonesia Anti-Scam Centre berhasil kembalikan Rp161 miliar dana masyarakat korban scam. https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/IASC-Berhasil-Kembalikan-Rp161-Miliar-Dana-Masyarakat-Korban-Scam.aspx

Otoritas Jasa Keuangan. (2026b, 6 Juli). Siaran pers: OJK ingatkan bahaya scam yang semakin meluas, PBB apresiasi peran OJK dalam penanganan scam. https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/Seminar-Anti-Scam-OJK-UNODC-2026.aspx

Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.

Prahassacitta, V. (2016, 22 November). Kedudukan CCTV sebagai alat bukti hukum pidana pasca putusan MK 2016. Business Law Binus. https://business-law.binus.ac.id/2016/11/22/kedudukan-cctv-sebagai-alat-bukti-hukum-pidana-pasca-putusan-mk-2016/

Soekanto, S. (2008). Faktor-faktor yang mempengaruhi penegakan hukum. RajaGrafindo Persada.

United Nations General Assembly. (2024). Resolution 79/243: United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes. https://digitallibrary.un.org/record/4071955

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana.

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Copyright © 2026 THE AUTHOR(S). This article is distributed under a Creative Commons Attribution-NonCommercial 4.0 International license.