

NO VIRAL, NO JUSTICE: PERLINDUNGAN HUKUM PEREMPUAN KORBAN DEEPPAKE PORNOGRAFI DALAM PERSPEKTIF HUKUM SIBER INDONESIA

Camila Nadya Rachman¹, Nadya Putri Ashari², Nita Wulan Dari³, Madiha Dzakiyyah Chairunnisa⁴

^{1,2,3,4}Universitas Terbuka, Indonesia

Email: camilanadyarachman@ecampus.ut.ac.id

Abstrak

Penyalahgunaan kecerdasan buatan (AI) generatif memicu maraknya Kekerasan Seksual Berbasis Elektronik (KSBE) berupa *deepfake* pornografi tanpa persetujuan yang merugikan privasi perempuan. Belum tersedianya regulasi khusus dan minimnya akuntabilitas platform memunculkan fenomena “*No Viral, No Justice*”, di mana korban terpaksa memviralkan kasusnya demi keadilan. Penelitian ini bertujuan menganalisis perlindungan hukum siber bagi korban serta mengkaji dampak fenomena tersebut terhadap penegakan hukum di Indonesia. Melalui pendekatan kualitatif sosio-hukum (*socio-legal*), data dihimpun via wawancara mendalam bersama tujuh klaster pemangku kepentingan (Kemenkomdigi, Bareskrim Polri, Komnas HAM, Komnas Perempuan, LBH APIK, SAFEnet, Akademisi Hukum) dan studi dokumen hukum melalui reduksi data, triangulasi, serta analisis tematik. Hasil penelitian menunjukkan kerangka hukum saat ini (UU ITE, UU TPKS, UU PDP) memiliki celah hukum (*legal gap*) terkait rekayasa *AI prompt-to-image*. Ketergantungan pada viralitas mengancam kepastian hukum dan memicu reviktimisasi. Penelitian ini menyimpulkan pentingnya aturan khusus AI berperspektif korban, penetapan tanggung jawab platform, serta perbaikan sistem penegakan hukum agar bekerja mandiri tanpa desakan publik.

Kata Kunci: *Deepfake Pornografi, Hukum Siber, No Viral No Justice, Perlindungan Hukum Perempuan, Regulasi AI.*

Abstract

Generative AI misuse drives a surge in Electronic-Based Sexual Violence (KSBE) through non-consensual deepfake pornography, violating women's privacy. The absence of specific regulations and platform accountability fuels the “No Viral, No Justice” phenomenon, compelling victims to publicize cases for redress. This study aims to analyze cyber law protections for victims and examine the impact of this phenomenon on Indonesian law enforcement. Using a qualitative socio-legal approach, data were gathered via in-depth interviews with seven stakeholder clusters (Kemenkomdigi, Bareskrim Polri, Komnas HAM, Komnas Perempuan, LBH APIK, SAFEnet, Legal Academics) and legal document analysis using data reduction, triangulation, and thematic synthesis. Findings reveal that current cyber laws (UU ITE, UU TPKS, UU PDP) contain legal gaps regarding prompt-to-image AI manipulation. Furthermore, relying on virality undermines legal certainty and risks victim revictimization. This study emphasizes the need for victim-centric AI regulations, platform accountability, and law enforcement reforms to operate independently without public pressure.

Keywords: *Deepfake Pornography, Cyber Law, No Viral No Justice, Legal Protection for Women, AI Regulation.*

A. PENDAHULUAN

Kehadiran dan pesatnya perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*) telah memperluas kemampuan manusia dalam menghasilkan, mengolah, dan memanipulasi konten digital. Namun, melesatnya kecanggihan AI yang tidak diimbangi oleh kesiapan regulasi memicu *digital harm* ketika fitur *Image Generator* (Grok AI) dieksploitasi untuk memproduksi dan menyebarkan konten deepfake pornografi non-konsensual (Yanto, 2025). Eskalasi kejahatan di ruang digital Indonesia menunjukkan tren yang mengkhawatirkan. Data resmi penanganan aduan Direktorat Pengendalian Ruang Digital Kemenkomdigi merekam bahwa sepanjang periode 20 Oktober 2024 hingga 6 Agustus 2026, pemerintah telah menangani sedikitnya 922.620 konten bermuatan pornografi (Kemenkomdigi, 2026). Dari akumulasi angka tersebut, platform X menduduki jajaran atas saluran media sosial paling rawan dengan menyumbang 68.054 konten pornografi, jauh melampaui platform lain seperti Meta (2.799 konten) maupun TikTok (34 konten) (Kemenkomdigi, 2026). Fenomena ini sejalan dengan temuan Dittipidsiber Bareskrim Polri yang mencatat bahwa 40% hingga 50% laporan Kekerasan Seksual Berbasis Elektronik (KSBE) kini secara eksplisit memuat unsur manipulasi AI *deepfake* (Mabes Polri, 2026). Ditressiber Polda Metro Jaya juga mencatat 154 laporan khusus terkait pornografi online dari total 4.271 kasus siber sepanjang 2025 (Mabes Polri, 2025). Perkembangan teknologi generatif ini memangkas hambatan teknis pembuatan (*barrier to entry*), di mana rekayasa digital yang dahulu membutuhkan keahlian editing tingkat tinggi kini dapat dieksekusi oleh siapa saja dalam hitungan detik (Yanto, 2025).

Manifestasi konkret dari ancaman ini terlihat pada kasus deepfake pornografi yang memanipulasi wajah guru dan siswi SMA di Semarang untuk kemudian disebar dan diperjualbelikan di platform X (Utami, 2025). Dalam perspektif *Gender Legal Theory* dan *Intersectional Gender Theory*, kejahatan ini bukan sekadar persoalan manipulasi teknologi, melainkan bentuk nyata kekerasan berbasis gender yang merenggut otonomi tubuh, privasi, dan representasi diri perempuan (Hunt, 2025). Dampaknya merusak reputasi dan martabat korban secara permanen serta memicu trauma psikologis yang mendalam. Kerugian tersebut kian diperberat oleh arsitektur teknologi platform media sosial itu sendiri. Melalui kerangka *Code Is Law* yang dikembangkan Lawrence Lessig, perilaku di ruang siber tidak hanya dibatasi oleh hukum formal, tetapi juga oleh *code* atau desain fitur teknologi yang menentukan kemungkinan suatu tindakan (Ayomi, Rahawarin and Hammar, 2026). Dalam kasus ini, penyedia platform menyediakan arsitektur berpemodelan longgar dan memonetisasinya melalui paket berlangganan berbayar (X Premium) tanpa disertai sistem pencegahan, pembatasan etis, maupun deteksi dini yang memadai. Akibatnya, pembiaran berbasis desain teknis (*technical design negligence*) ini memperluas ruang terjadinya kekerasan digital berbasis AI.

Kondisi tersebut mempertegas adanya kesenjangan hukum (*legal gap*) yang nyata di Indonesia. Kerangka hukum positif saat ini seperti Undang-Undang Tindak Pidana Kekerasan Seksual (UU TPKS) (Pemerintah Indonesia, 2022a), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) (Pemerintah Indonesia, 2024), serta Undang-Undang Pelindungan Data Pribadi (UU PDP) (Pemerintah Indonesia, 2022b) masih memiliki keterbatasan normatif karena belum menjangkau spesifikitas rekayasa AI generatif (*prompt-to-image*) dan belum mengatur pertanggungjawaban hukum penyedia platform (*platform liability*) secara eksplisit. Ketertinggalan regulasi nasional yang baru menginisiasi draf Peraturan Presiden tentang Tata Kelola AI membuat negara gagap memberikan perlindungan terintegrasi dari hulu ke hilir, terutama jika dibandingkan dengan komprehensifnya kerangka regulasi *European Union AI Act* (European Union, 2024). Ketiadaan norma hukum khusus AI dan ketidaktegasan aturan pertanggungjawaban platform ini berdampak langsung pada proses penegakan hukum pidana. Aparat Penegak Hukum (APH) sering kali terhambat oleh kerumitan birokrasi penanganan bukti siber, proses pembuktian yang kaku, serta lambatnya respons penanganan awal kasus.

Akibat lambannya birokrasi penegakan hukum dan ketiadaan kepastian penanganan laporan, timbul fenomena "*No Viral, No Justice*" di mana korban atau masyarakat terpaksa memviralkan kasus kejahatan siber di media sosial agar memperoleh perhatian dan tindakan cepat dari institusi kepolisian (Dachi, 2024) (Hafiduddin *et al.*, 2026). Meskipun perhatian publik dan masifnya simpati di media sosial efektif mendorong penanganan kasus oleh APH, mekanisme ini menjadi bumerang yang memicu terjadinya viktimisasi sekunder (*secondary victimization*) (Setiawan, Tohari and Alid, 2026). Ketika kasus disebarluaskan demi mengejar respons penegak hukum, identitas dan konten manipulatif korban justru semakin terekspos secara luas. Korban terpaksa menghadapi stigma sosial, *victim-blaming*, pemeriksaan berulang yang tidak sensitif gender, hingga erosi kepercayaan publik atas perbuatan yang tidak pernah mereka lakukan. Dengan demikian, proses pencarian keadilan melalui jalur viralitas justru menghasilkan penderitaan berlipat ganda bagi korban. (Zakki and Aini, 2026)

Mengatasi kompleksitas permasalahan di atas memerlukan reorientasi kerangka hukum melalui perspektif *Responsive Law* yang dikembangkan oleh Philippe Nonet dan Philip Selznick (Lailiyah, 2025). Konsep ini menempatkan hukum sebagai institusi sosial yang tidak boleh kaku atau sekadar mempertahankan aturan formal, melainkan harus responsif terhadap perkembangan kebutuhan masyarakat dan tujuannya dalam mewujudkan keadilan nyata (Lailiyah, 2025). Berbeda dengan penelitian-penelitian terdahulu yang umumnya mengkaji KSBE sebatas dari kacamata hukum pidana konvensional, penelitian ini menawarkan kebaruan (*novelty*) dengan secara spesifik menelaah titik temu antara penyalahgunaan teknologi AI deepfake (Grok AI), pertanggungjawaban platform, serta fenomena "*No Viral, No Justice*" sebagai variabel penentu kepastian hukum. Atas dasar tersebut, penelitian ini bertujuan untuk menganalisis bentuk rekonstruksi perlindungan hukum siber yang ideal bagi korban deepfake pornografi berbasis AI, sekaligus merumuskan mekanisme penegakan hukum yang responsif guna mengeliminasi risiko viktimisasi sekunder di Indonesia.

B. METODE

Penelitian ini menggunakan pendekatan kualitatif sosio-hukum (*socio-legal research*) yang diintegrasikan dengan penelitian hukum normatif. Pendekatan ini dipilih guna membedakan dan memetakan secara komprehensif kesenjangan antara aturan hukum tertulis (*law in books*) dengan realita penegakan hukum di lapangan (*law in action*). Pendekatan interdisipliner ini krusial untuk menguraikan fenomena "*No Viral, No Justice*", ketidakjelasan pertanggungjawaban penyedia platform (*platform liability*), serta efektivitas perlindungan hukum bagi korban Kejahatan Seksual Berbasis Elektronik (KSBE), khususnya pada kasus eksploitasi fitur kecerdasan buatan (*Generative AI*) Grok di platform X. Guna mengkaji permasalahan secara komprehensif, penelitian ini mengombinasikan tiga pendekatan utama: pendekatan perundang-undangan (*statute approach*) untuk menguji kecukupan norma dan celah hukum pada UU TPKS, UU ITE, UU PDP, KUHP, Permenkominformo No. 5/2020, serta arah pembentukan Perpres Tata Kelola AI; pendekatan konseptual (*conceptual approach*) untuk merumuskan kerangka pertanggungjawaban entitas AI dan platform (*Code is Law*) serta konsep viktimologi siber; dan pendekatan sosiologi hukum (*socio-legal approach*) untuk menganalisis dinamika sosial, fenomena *victim-blaming*, hingga hambatan struktural-birokratis penegakan hukum di lapangan. Data primer penelitian ini diperoleh melalui wawancara mendalam (*in-depth interview*) bersama 13 (tiga belas) orang narasumber kunci. Penentuan narasumber dilakukan secara sengaja (*purposive sampling*) berdasarkan kriteria keterlibatan langsung dalam penanganan kasus KSBE, perumusan kebijakan siber, maupun advokasi hak-hak digital. Narasumber tersebut terbagi ke dalam 7 (tujuh) klaster lembaga utama:

1. Kementerian Komunikasi dan Digital (Kemenkomdigi): 2 orang pejabat Direktorat Pengendalian Ruang Digital yang berwenang dalam kebijakan pemblokiran konten dan pengawasan Penyelenggara Sistem Elektronik (PSE).
2. Dittipidsiber Bareskrim Polri: 2 orang penyidik senior kejahatan siber yang menangani pembuktian forensik digital dan penyidikan kasus *deepfake*.
3. Komnas Perempuan: 1 orang komisioner/subkomisi pemantauan yang menangani advokasi kebijakan berperspektif korban KSBE.
4. Komnas HAM: 3 orang analis kebijakan HAM di bidang perlindungan ruang digital dan privasi.
5. LBH APIK Jakarta: 2 orang advokat pendamping hukum korban kekerasan berbasis gender dan KSBE.
6. SAFEnet: 2 orang aktivis dan peneliti hak-hak digital yang memantau kebebasan berekspresi dan kejahatan siber.
7. Akademisi Hukum Pidana: 1 orang pakar hukum pidana dan hukum kecerdasan buatan yang mengkaji teori hukum dan viktimologi.

Selain data primer, data sekunder dikumpulkan melalui studi kepustakaan yang mencakup bahan hukum primer (UU TPKS, UU ITE, UU PDP, KUHP, dan Permenkominformasi), bahan hukum sekunder (laporan tahunan resmi Komnas Perempuan dan Komnas HAM, *white paper* kementerian, buku teks hukum, serta artikel jurnal ilmiah bereputasi), dan bahan hukum tersier. Seluruh data kualitatif diolah menggunakan teknik Analisis Tematik (*Thematic Analysis*) melalui lima tahapan sistematis:

1. Transkripsi *Verbatim*: Rekaman audio dan video hasil wawancara diubah menjadi teks transkrip utuh kata demi kata, lalu diperiksa kembali secara manual untuk menjaga keaslian narasi narasumber.
2. Pengodean (*Initial Coding*): Peneliti menyisir transkrip dan memberikan kode pada poin-poin penting, seperti hambatan forensik digital, reviktimisasi, *legal gap*, tanggung jawab platform, dan akses keadilan.
3. Kategorisasi Tema: Kode-kode awal dikelompokkan ke dalam tema utama (seperti: Kendala Penegakan Hukum & Forensik, Dampak Sekunder Viralisasi Kasus, serta Arah Rekonstruksi Hukum AI).
4. Triangulasi Data: Validitas temuan diuji dengan membandingkan keterangan antar-narasumber (penyidik, lembaga pendamping, dan akademisi) serta mencocokkan data wawancara dengan isi regulasi dan laporan statistik resmi.
5. Interpretasi Data: Temuan disusun ke dalam bentuk narasi analitis dan matriks korelasi yang dibahas menggunakan kerangka *Gender Legal Theory*, konsep *Code Is Law*, teori Viktimisasi Sekunder, dan teori *Responsive Law*.

Mengingat penelitian ini mengkaji isu kekerasan seksual digital yang sensitif, seluruh proses riset menerapkan prinsip etika penelitian secara ketat. Peneliti memperoleh persetujuan tertulis/lisan (*Informed Consent*) dari seluruh narasumber, menjamin anonimitas identitas narasumber melalui penyamaran kode/inisial, serta menerapkan pendekatan berperspektif korban (*victim-centered approach*) untuk mencegah terjadinya trauma berulang (*revictimization*).

C. HASIL DAN PEMBAHASAN

Perkembangan teknologi kecerdasan buatan (AI) generatif khususnya fitur pembuatan gambar seperti Grok di platform X telah memperluas spektrum kekerasan digital, dari pelecehan siber konvensional hingga dampak buruk yang secara khusus terkait dengan AI generatif. Fenomena pornografi *deepfake* tanpa persetujuan merupakan bentuk eksploitasi tubuh secara digital, di mana citra visual seseorang dimanipulasi tanpa izin mereka, sehingga merenggut otonomi digital serta merusak martabat dan reputasi mereka secara permanen.

Untuk mengkaji kompleksitas seputar penyebaran konten semacam itu beserta respons hukum yang terkait, tabel di bawah ini menyajikan statistik resmi mengenai penanganan aduan dari Direktorat Pengendalian Ruang Digital Kementerian Komunikasi dan Digital serta pihak kepolisian.

Tabel 1. Data Aduan Konten Pornografi Deepfake Berdasarkan Platform Media Sosial (2026)

Platform Media Sosial	Jumlah Konten Ditangani	Persentase (%)
Platform X	68.054	95,99%
Telegram	2.130	3,00%
Platform Lainnya	720	1,01%
Total	70.904	100,00%

Sumber: Diolah dari Data Aduan Direktorat Pengendalian Ruang Digital Kemenkomdigi (2026).

Tabel 1 mengonfirmasi adanya kerentanan masif pada Platform X, yang mencakup 68.054 konten (95,99%) dari total keseluruhan konten yang dibandingkan di berbagai platform media sosial. Kerentanan ini selaras dengan teori "*Code is Law*" (Kode adalah Hukum) dari Lawrence Lessig, yang menegaskan bahwa perilaku pengguna di dunia maya tidak hanya dibatasi oleh hukum formal, tetapi secara mendasar dibentuk oleh arsitektur kode dan desain platform. Monetisasi fitur pembuatan gambar yang minim regulasi melalui paket berlangganan berbayar (X Premium) tanpa adanya mekanisme pengamanan yang memadai menunjukkan bahwa desain platform tersebut secara pasif memfasilitasi dampak buruk di ranah digital demi keuntungan komersial.

Tabel 2. Pemetaan Penanganan Laporan Kejahatan Siber dan Pergeseran Modus KSBE (Data Kepolisian 2025–2026)

Institusi Penegak	Jenis Laporan/Modus	Jumlah Laporan/Proporsi
Ditressiber Polda Metro Jaya	Laporan Pornografi Online	154 Laporan (3,60%)
Ditipidsiber Bareskrim Polri	Laporan KSBE memuat Manipulasi AI <i>Deepfake</i>	40% – 50% dari total KSBE

Sumber: Diolah dari Laporan Kinerja Ditressiber Polda Metro Jaya dan Bareskrim Polri (2025–2026).

Berdasarkan Tabel 2, meskipun laporan pornografi online pada Ditressiber Polda Metro Jaya tercatat sebanyak 154 laporan (3,60%), data Bareskrim Polri menunjukkan pergeseran kualitatif yang signifikan: 40% hingga 50% laporan Kekerasan Seksual Berbasis Elektronik (KSBE) kini memuat unsur manipulasi AI *deepfake*. Rekayasa digital yang dahulu membutuhkan keahlian teknis tinggi kini dapat dieksekusi siapa saja dalam hitungan detik (*barrier to entry* yang sangat rendah).

Ditinjau dari dinamika regulasi dan penindakan di tingkat pemerintah, Kemenkomdigi sempat mengambil tindakan tegas berupa tindakan pemblokiran terhadap fitur Grok AI di Indonesia. Menurut penjelasan Bu Dini dari Direktorat Pengendalian Ruang Digital Kemenkomdigi:

"Waktu itu ada dua hal yang menjadi atensi sebelum kami memutuskan untuk melakukan pemblokiran terhadap AI Grok. Pertama, terkait dengan tanda daftar dari Grok itu sendiri yang memang belum mendaftarkan sistem elektroniknya ke dalam pendaftaran Penyelenggara Sistem Elektronik (PSE) di Komdigi. Lalu yang kedua adalah karena terkait dengan penyalahgunaan fitur Grok untuk memproduksi konten-konten deepfake yang bermuatan seksual. Jadi dua hal ini yang kemudian menjadi dasar kami untuk melakukan pemblokiran... penanganan terhadap pelanggaran atas Pasal 27 Ayat (1) UU ITE."

Langkah pemblokiran tersebut diikuti oleh proses negosiasi dan komitmen penyesuaian teknis oleh pihak pengembang (Platform X). Bu Dini (Kemenkomdigi) menambahkan:

"X kemudian melakukan penyesuaian terhadap fitur-fitur yang mereka miliki di aplikasi Grok ini... Penyesuaian yang dilakukan antara lain: untuk pengguna yang bisa meminta Grok melakukan edit gambar atau produksi konten harus pengguna yang berstatus premium atau subscribe. Selain itu, untuk konten-konten yang bermuatan seksual dengan keyword-keyword tertentu misalnya meminta edit gambar dengan pakaian tertentu itu sudah tidak bisa lagi dilakukan oleh AI Grok."

Kendati demikian, tantangan struktural penegakan hukum di ranah digital tetap mengemuka akibat ketiadaan kantor perwakilan resmi Platform X di Indonesia. Hal ini memperlambat proses komunikasi dan mitigasi masalah lokal. Bu Dini (Kemenkomdigi) menegaskan:

"X tidak memiliki kantor maupun perwakilan khusus di Indonesia... Pihak yang bisa hadir biasanya berasal dari tingkat regional di luar Indonesia, yang terdekat di Singapura. Selain itu, karena mereka tidak memiliki tim khusus di Indonesia, agak lebih sulit bagi mereka untuk menangkap aspek-aspek lokal serta norma yang berlaku di negara kita."

Di sisi lain, batas waktu penindakan (*takedown*) konten eksplisit juga menghadapi kendala birokrasi dan koordinasi. Secara normatif, Kemenkomdigi menetapkan sanksi tegas apabila platform tidak merespons perintah *takedown* dalam kurun waktu 1x24 jam. Sebagaimana dipaparkan oleh Bu Dini (Kemenkomdigi):

"Khusus untuk konten yang berkaitan dengan pornografi, aturannya sudah sangat jelas. Ketika Komdigi menyampaikan perintah take down, pihak platform harus melaksanakannya dalam waktu 1x24 jam. Apabila tidak ditindaklanjuti... ada sanksi berjenjang yang dapat dikenakan... mulai dari Surat Teguran 1, Surat Teguran 2, penetapan denda administratif, hingga pemutusan akses (pemblokiran) layanan."

Namun, dalam praktiknya di lapangan, mekanisme *takedown* yang diakses oleh masyarakat atau organisasi bantuan hukum sering kali memakan waktu lama karena kerumitan alur administrasi. Sebagaimana diungkapkan oleh Mbak Sarah dari Divisi Penanganan Kasus LBH APIK Jakarta:

"Prosedur takedown konten via Komdigi sangat lambat dan birokratis. Sejauh ini LBH APIK belum pernah berhasil melakukan takedown konten secara cepat hanya melalui surat resmi ke Komdigi. Respon surat Komdigi bisa memakan waktu 1 hingga 2 bulan."

Ditinjau dari *Gender Legal Theory*, fenomena *deepfake* pornografi merupakan bentuk Kekerasan Berbasis Gender Online (KBGO) yang menasar tubuh dan identitas perempuan. Hambatan hukum saat ini timbul karena kerangka hukum positif Indonesia seperti UU No. 12/2022 tentang TPKS, UU No. 1/2024 tentang ITE, dan UU No. 27/2022 tentang PDP belum secara eksplisit mengatur spesifisitas teknologi AI generatif dan belum memiliki payung hukum khusus AI yang memadai. Sebagaimana diakui oleh pihak Kemenkomdigi melalui Bu Yoshi:

"Kebetulan kalau terkait kebijakan regulasi khusus AI, saat ini masih dalam tahap penyusunan... Untuk saat ini, penanganan konten AI menggunakan seluruh regulasi yang berkaitan dengan pelanggaran konten itu sendiri (seperti UU ITE dan KUHP)... jika memanipulasi foto seseorang hingga bermuatan pornografi, maka yang diterapkan adalah UU ITE dan UU Pornografi."

Ketiadaan norma hukum eksplisit mengenai AI generatif ini berdampak pada penolakan laporan di tingkat kepolisian. Sebagaimana diungkapkan oleh Mbak Tessa dari Divisi Kebebasan Berekspreasi SAFEnet:

"Belum ada definisi hukum yang mengatur mengenai deepfake atau bahkan media sintetis berbasis AI secara eksplisit dan normatif yuridis dalam peraturan perundang-undangan di Indonesia... Ketika ada korban mengadu karena kasusnya baru berupa ancaman pemerasan (blackmail) dan konten deepfake-nya belum disebarluaskan,

polisi menganggap belum ada kerugian materiil yang timbul sehingga laporan ditolak."

Kondisi tersebut diperberat oleh hambatan pembuktian teknis yang membebankan korban. Mbak Sarah (LBH APIK) menambahkan:

"Hambatan terbesar dalam pembuktian kasus deepfake adalah ketersediaan foto asli (sebelum dimanipulasi/diedit) sebagai pembanding. Banyak korban hanya menyimpan foto yang sudah diedit atau foto aslinya sudah terhapus. Tanpa foto pembanding, penyidik sering menjadikan itu alasan untuk memandekkan perkara."

Akibat kebuntuan saluran hukum formal dan lambatnya prosedur penanganan, timbul fenomena *"No Viral, No Justice"*, di mana viralitas di media sosial dijadikan instrumen taktis oleh korban untuk memicu atensi publik dan mempercepat penindakan oleh aparat. Ditinjau dari teori viktimisasi sekunder (*secondary victimization*), tindakan ini menjadi pilihan simalakama bagi korban.

Mbak Liya dari LBH APIK Jakarta menjelaskan akar permasalahan fenomena ini:

"Fenomena itu muncul karena sistem hukum kita tidak bekerja secara responsif. Penyintas sampai di LBH APIK saja sudah merupakan perjuangan berat. Ketika laporan diproses ke polisi, substansi, struktur, dan budaya hukum yang masih bias gender membuat korban merasa tidak mendapat keadilan, sehingga mencari keadilan alternatif dengan memviralkan/spill pelaku."

Hal ini dipertegas oleh Mbak Sinta dari Tim Penanganan Aduan SAFEnet:

"Memviralkan kasus sebenarnya merupakan jalan terakhir yang terpaksa dipilih oleh korban setelah ia tidak mendapatkan keadilan di mana pun... Padahal, dengan melakukan itu ia harus mempertaruhkan identitas dirinya ke publik, serta harus menunjukkan bukti-bukti intim yang sebetulnya berisiko membuat pelaku melaporkan balik korban atas tuduhan pencemaran nama baik."

Proses memviralkan kasus ini akhirnya mengekspos korban pada reviktimisasi berulang di ruang digital berupa penyalahan korban (*victim-blaming*), perundungan, hingga risiko kriminalisasi menggunakan Pasal Pencemaran Nama Baik UU ITE. Sebagaimana ditambahkan oleh Mbak Sinta (SAFEnet):

"Sekarang polanya bergeser. Cara mereka menyudutkan korban saat ini adalah: 'Ya ini risiko kamu bermain internet' atau 'Kamu harus paham, ini konsekuensi kalau kamu mengunggah foto di akun yang tidak dikunci atau akun publik.' Ini menjadi salah satu bentuk reviktimisasi baru terhadap korban... Publik sekarang sudah tidak bisa lagi menyalahkan pakaian korban karena teknologinya sudah bisa mengedit foto apa saja."

Ketergantungan penegakan hukum pada viralitas jelas mencederai prinsip kepastian hukum (*certainty of law*) serta kesetaraan di hadapan hukum (*equality before the law*). Berdasarkan perspektif *Responsive Law* (Philippe Nonet & Philip Selznick), institusi dan regulasi hukum Indonesia tidak boleh kaku pada aturan formal semata (*law in books*), melainkan harus adaptif dan responsif terhadap pemenuhan keadilan nyata bagi korban (*law in action*). Kerangka perlindungan hukum yang ideal menuntut hadirnya penetapan regulasi khusus AI, pembentukan SOP pembuktian digital yang sensitif gender, serta koordinasi terpadu antara Kemenkomdigi, Kepolisian, dan platform digital agar penanganan kasus *deepfake* dapat berjalan secara cepat, pasti, dan independen sejak laporan awal diterima tanpa bergantung pada perhatian publik di media sosial.

D. KESIMPULAN

Eskalasi kejahatan *deepfake* pornografi non-konsensual berbasis AI generatif (Grok AI) di platform X membuktikan adanya kelemahan mendasar pada desain platform digital serta kesenjangan hukum (*legal gap*) di Indonesia. Kerangka hukum positif saat ini (UU TPKS, UU ITE, dan UU PDP) belum secara eksplisit menjangkau spesifisitas rekayasa AI generatif

(*prompt-to-image*) dan pertanggungjawaban penyedia platform (*platform liability*). Ketiadaan norma khusus AI, tiadanya kantor perwakilan resmi platform di Indonesia, serta prosedur pembuktian digital yang kaku menyebabkan saluran hukum formal sering kali mengalami kebuntuan dan menolak laporan korban.

Kebuntuan tersebut melahirkan fenomena "*No Viral, No Justice*", di mana korban terpaksa memanfaatkan tekanan publik di media sosial guna mempercepat penindakan oleh aparat penegak hukum. Namun, jalur viralitas ini menjadi bumerang yang memicu viktimisasi sekunder (*secondary victimization*), karena korban harus menghadapi penyalahan korban (*victim-blaming*), erosi privasi, perundungan digital, hingga risiko kriminalisasi balik melalui pasal pencemaran nama baik. Ketergantungan penegakan hukum pada viralitas secara nyata mencederai prinsip kepastian hukum dan kesetaraan di hadapan hukum (*equality before the law*).

Guna mengeliminasi risiko viktimisasi sekunder dan mewujudkan perlindungan hukum yang ideal, diperlukan rekonstruksi hukum siber yang adaptif melalui perspektif *Responsive Law*. Pemerintah dan DPR perlu merealisasikan regulasi khusus AI (seperti Perpres Tata Kelola AI atau RUU AI) yang berperspektif korban, menetapkan pertanggungjawaban ketat bagi platform, menyusun SOP pembuktian digital yang sensitif gender, serta membangun mekanisme koordinasi terpadu antara Kemenkomdigi, Kepolisian, dan platform digital agar penanganan kasus *deepfake* dapat berjalan cepat, pasti, dan proaktif sejak laporan awal diajukan tanpa harus menunggu kasus menjadi viral.

DAFTAR PUSTAKA

- Ayomi, M., Rahawarin, Y. F., & Hammar, I. I. R. (2026). Urgensi Reformulasi Pertanggungjawaban Pidana Dalam Tindak Pidana Artificial Intelligence Di Indonesia Pasca KUHP Nasional. *Mansinam Law Review*, 2(1), 61-78. <https://doi.org/10.67267/jvcvh958>.
- Dachi, K. S. Y. (2024). Perlindungan Hukum Terhadap Korban Kekerasan Seksual Berbasis Elektronik. *Legalitas: Jurnal Hukum*, 16, 114–121.
- European Union. (2024). *Rules for trustworthy artificial intelligence in the EU*. Available at: <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32024R1689>.
- Hafiduddin, M., Hasbullah, A., Munir, A., Eldavi, A. Z. U., & Lusiawati, D. (2026). Hukum Siber Di Era Digital: Rekonstruksi Penanggulangan Kejahatan Deepfake Dalam Perspektif Hukum Pidana Indonesia Dan Maqāṣid Al-Syarī'ah. *SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum*, 5(4), 1325-1336. <https://doi.org/10.55681/seikat.v5i4.3370>.
- Hunt, E. C. (2025). Deep-Fake Revenge Porn: The intersection of Artificial Intelligence and Revenge porn for a Modern Attack on Women (*Capstone Projects and Master's Theses*).
- Kemenkomdigi. (2026). *Laporan Data Penanganan Konten Pengendalian Ruang Digital Periode 2024–2026*. Kemenkomdigi.
- Lailiyah, F. (2025). Analisis Pengaturan Hukum Tindak Pidana Cyber Crime Phising di Indonesia Berdasarkan Prespektif Hukum Responsif. Available at: <https://repository.ibrahimy.ac.id/handle/123456789/541>.
- Mabes Polri. (2025). *Polda Metro Jaya Tangani 4.271 Laporan Kasus Siber Sepanjang 2025*. Available at: <https://portal.divhumas.polri.go.id/id/explore/polda-metro-jaya-tangani-4271-laporan-kasus-siber-sepanjang-2025-2c174e23>
- Mabes Polri. (2026). *Deepfake AI Jadi Modus Baru Kejahatan Digital, Korban Diperas Lewat Foto Rekayasa*. Available at: <https://mediahub.polri.go.id/in/image/detail/505858-deepfake-ai-jadi-modus-baru-kejahatan-digital-korban-diperas-lewat-foto-rekayasa>
- Sijabat, A.S.U. and Lukitasari, D. (2024). Konten gambar dan video pornografi deepfake

- sebagai suatu bentuk tindak pidana pencemaran nama baik. *Jurnal Recidive*, 13(2).
- Setiawan, R., Tohari, M., & Alid, I. H. (2026). Risiko ‘Double Victimisation’ pada Korban Kekerasan Seksual Berbasis Elektronik (KSBE) dalam Penegakan Hukum Deepfake Pornografi. *Lex Journal: Kajian Hukum & Keadilan*, 10.
- Seveney, M. C., Wicaksono, D. B., & Soetijono, I. K. (2025). Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis AI (Artificial Intelligence) Pada Konten Pornografi. *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda*, 31(2), 97–106. <https://doi.org/10.46839/disiplin.v31i2.1167>
- Sutrianto, E.P., Siahaan, P.G., Saragih, C.O., Rumahorbo, D.M. and Hutajulu, B.A. (2026). Tanggung Jawab Hukum Siber Terhadap Pelanggaran Hak Cipta oleh Output Generative Artificial Intelligence (AI). *JERUMI: Journal of Education Religion Humanities and Multidisciplinary*, 4(1), 744–750.
- Undang-undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual.
- Undang-undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.
- Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
- Utami, K.D. (2025) *Korban Konten Pornografi "Deepfake" di Semarang Tuntut Pelaku Jadi Tersangka*. Available at: <https://www.kompas.id/artikel/korban-konten-pornografi-deepfake-di-semarang-tuntut-pelaku-jadi-tersangka> (Accessed: September 6, 2026).
- Yanto, O. (2025) “Etika Penggunaan Kecerdasan Buatan dalam Pendidikan Hukum,” *Jurnal Hukum & Pembangunan*, 54.
- Zakki, M.Z. and Aini, I.Q. (2026) “Antara Keadilan dan Sensasi: Kajian Fenomena No Viral No Justice dalam Penegakan Hukum Pidana,” *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, 4.
- Zulfikar,. Partahan., V., A., Erick., S. (2025). Urgensi Model Kerangka Yuridis Adaptif Terhadap Deepfake Ai (Artificial Intelligence) Dalam Perspektif Hukum Siber. *Jurnal Pendidikan Sejarah dan Riset Sosial Humaniora*, 8(6). 915-925