



Perlindungan Hukum terhadap Korban Kejahatan Pornografi Berbasis Teknologi Artificial Intelligence

Rini Apriyani^{1*}, Reza Pramasta Gegana², Nurafifah Ayu Puspitasari³

¹⁻³ Program Studi Sarjana Hukum, Fakultas Hukum, Universitas Mulawarman, Indonesia

*Penulis Korespondensi: nurafifahpnj@gmail.com

Abstract. *The rapid development of Artificial Intelligence has enabled the creation of deepfake pornography by manipulating a person's face, voice, or image without consent. This practice threatens privacy, dignity, reputation, and the psychological condition of victims, while Indonesian law has not yet regulated it explicitly. This study analyzes the forms of legal protection for victims of Artificial Intelligence-based pornographic crimes and the legal measures available to restore their reputation. The research uses a doctrinal method by examining legislation, legal principles, books, scientific articles, and other relevant legal materials through qualitative analysis. The findings show that the Pornography Law, the Electronic Information and Transactions Law, the Personal Data Protection Law, the Sexual Violence Crimes Law, and the Criminal Code can serve as legal bases, but their provisions remain fragmented and require extensive interpretation. Victims may receive preventive and repressive protection, including content removal, legal assistance, psychological rehabilitation, restitution, and the right to be forgotten. However, weak digital forensic capacity, delayed content removal, social stigma, and the absence of specific Artificial Intelligence regulation limit effective recovery. Legal reform must therefore clarify prohibited conduct, responsibility, platform obligations, and integrated victim recovery.*

Keywords: *Artificial Intelligence; Deepfake Pornography; Legal Protection; Reputation Recovery; Victimology.*

Abstrak. Perkembangan *Artificial Intelligence* memungkinkan pelaku membuat pornografi deepfake melalui manipulasi wajah, suara, atau gambar seseorang tanpa persetujuan. Perbuatan tersebut mengancam privasi, martabat, nama baik, dan kondisi psikologis korban, sedangkan hukum Indonesia belum mengaturnya secara eksplisit. Penelitian ini bertujuan menganalisis bentuk perlindungan hukum terhadap korban kejahatan pornografi berbasis *Artificial Intelligence* dan upaya hukum untuk memulihkan nama baik korban. Penelitian menggunakan metode doktrinal dengan menelaah peraturan perundang-undangan, asas hukum, buku, artikel ilmiah, dan bahan hukum lain yang relevan, kemudian menganalisisnya secara kualitatif. Hasil penelitian menunjukkan bahwa Undang-Undang Pornografi, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Undang-Undang Tindak Pidana Kekerasan Seksual, dan Kitab Undang-Undang Hukum Pidana dapat menjadi dasar perlindungan, tetapi pengaturannya masih tersebar dan membutuhkan penafsiran. Korban dapat memperoleh perlindungan preventif dan represif berupa penghapusan konten, bantuan hukum, rehabilitasi psikologis, restitusi, dan hak untuk dilupakan. Pelaksanaannya masih menghadapi keterbatasan forensik digital, lambatnya penghapusan konten, stigma sosial, dan belum adanya regulasi khusus. Karena itu, pembaruan hukum perlu memperjelas perbuatan terlarang, pertanggungjawaban, kewajiban platform, dan mekanisme pemulihan korban secara terpadu.

Kata kunci: *Artificial Intelligence; Pemulihan Nama Baik; Perlindungan Hukum; Pornografi Deepfake; Viktimologi.*

1. LATAR BELAKANG

Perkembangan masyarakat berjalan beriringan dengan kemajuan teknologi yang semakin kompleks. *Artificial Intelligence* menjadi salah satu bentuk perkembangan tersebut karena mampu mengolah data, mengenali pola, membuat proyeksi, dan menyelesaikan tugas yang sebelumnya membutuhkan campur tangan manusia secara langsung. Teknologi ini memberi manfaat dalam pendidikan, kesehatan, industri kreatif, komunikasi, dan berbagai kegiatan sehari-hari. Kemampuan yang sama juga membuka peluang penyalahgunaan ketika pengguna memanfaatkan sistem kecerdasan buatan untuk memanipulasi suara, gambar, atau video seseorang.

Salah satu bentuk penyalahgunaan yang menimbulkan persoalan hukum adalah *deepfake* (Chesney & Citron, 2019). Teknik ini dapat mengganti wajah atau suara seseorang dalam gambar dan video sehingga hasilnya tampak menyerupai objek asli (Rahayu & Santoso, 2023). Ketika pelaku menempatkan wajah seseorang ke dalam konten seksual tanpa persetujuan, teknologi tersebut berubah menjadi sarana pornografi berbasis kecerdasan buatan. Pornografi *deepfake* tidak memerlukan akses langsung terhadap tubuh korban karena pelaku cukup memperoleh foto atau rekaman yang tersedia di ruang digital.

Pornografi berbasis *Artificial Intelligence* menimbulkan kerugian yang lebih luas daripada persoalan kesusilaan. Korban dapat mengalami rasa takut, malu, tekanan sosial, kehilangan rasa aman, gangguan psikologis, serta kerusakan nama baik di lingkungan keluarga, pendidikan, pekerjaan, dan masyarakat (Kasita, 2022). Konten yang telah tersebar juga mudah disimpan, digandakan, dan diproduksi ulang sehingga korban berhadapan dengan risiko viktimisasi berulang (Mutmainnah et al., 2024). Kondisi ini menempatkan pornografi *deepfake* sebagai bentuk kekerasan berbasis gender daring yang menyentuh hak privasi, martabat manusia, dan kendali korban atas data pribadinya.

Hukum positif Indonesia telah memiliki beberapa ketentuan yang dapat digunakan untuk menindak produksi dan penyebaran konten pornografi. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi melarang produksi, distribusi, dan penyediaan pornografi (Republik Indonesia, 2008). Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik mengatur penyebaran muatan yang melanggar kesusilaan melalui sistem elektronik (Republik Indonesia, 2024). Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual memuat hak korban atas penanganan, perlindungan, dan pemulihan (Republik Indonesia, 2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi melengkapi dasar perlindungan ketika pelaku menggunakan, mengubah, atau menyebarkan data pribadi korban tanpa hak (Republik Indonesia, 2022).

Walaupun sejumlah peraturan dapat digunakan, hukum Indonesia belum menyebut pornografi berbasis *Artificial Intelligence* secara tegas (Putra, 2024). Aparat penegak hukum masih harus menafsirkan unsur pornografi, kesengajaan, manipulasi digital, penggunaan data pribadi, dan pertanggungjawaban pihak yang terlibat. Kesenjangan ini dapat menimbulkan perbedaan penerapan hukum dan membuat korban sulit memperoleh penanganan yang cepat, terutama ketika konten telah beredar di banyak platform (Natalia & Layang, 2024). Penelitian terdahulu juga menunjukkan bahwa penggunaan Undang-Undang Pornografi dan Undang-Undang Informasi dan Transaksi Elektronik menghadapi keterbatasan interpretasi terhadap

konten yang sepenuhnya dihasilkan atau dimanipulasi oleh sistem kecerdasan buatan (Chairani et al., 2024).

Sejumlah penelitian terdahulu telah membahas kebijakan perumusan hukum pidana terhadap praktik *deepfake*, pertanggungjawaban pidana pelaku, serta kedudukan perbuatan, pemidanaan, dan kekosongan norma dalam kejahatan pornografi berbasis kecerdasan buatan (Andani, 2025; Lestari, 2024; Mahardika, 2025). Berbeda dari kajian tersebut, penelitian ini menempatkan korban sebagai pusat analisis. Kebaruan penelitian terletak pada pembahasan terpadu mengenai perlindungan preventif dan represif serta pemulihan nama baik korban melalui penghapusan konten, penerapan hak untuk dilupakan, rehabilitasi, restitusi, dan dukungan kelembagaan.

Berdasarkan uraian tersebut, penelitian ini menjawab dua permasalahan. Pertama, bagaimana bentuk perlindungan hukum terhadap korban kejahatan pornografi berbasis teknologi *Artificial Intelligence*. Kedua, bagaimana upaya pemulihan nama baik korban setelah konten manipulatif dibuat atau disebar. Penelitian ini bertujuan menganalisis kedua persoalan tersebut agar dapat memberikan sumbangan akademis bagi ilmu hukum serta masukan praktis bagi pemerintah, aparat penegak hukum, lembaga perlindungan korban, dan penyelenggara sistem elektronik.

2. KAJIAN TEORITIS

Teori perlindungan hukum

Perlindungan hukum menggunakan perangkat hukum untuk membela subjek hukum dan menjamin terpenuhinya hak yang dilanggar. Philipus M. Hadjon membagi perlindungan hukum menjadi perlindungan preventif dan represif (Hadjon et al., 2011). Perlindungan preventif bekerja sebelum pelanggaran terjadi melalui pembentukan norma, pengawasan, pendidikan, dan sistem pencegahan. Perlindungan represif diberikan setelah pelanggaran melalui penegakan hukum, penyelesaian sengketa, pemidanaan, ganti kerugian, rehabilitasi, dan pemulihan hak (Hadjon et al., 2011).

Pembagian tersebut relevan untuk menilai perlindungan korban pornografi berbasis *Artificial Intelligence*. Perlindungan preventif mencakup larangan produksi dan distribusi konten pornografi, perlindungan data pribadi, literasi digital, pengawasan platform, dan penggunaan teknologi pendeteksi konten manipulatif. Perlindungan represif mencakup proses pelaporan, penyelidikan, penuntutan, penjatuhan sanksi, penghapusan konten, bantuan hukum, rehabilitasi psikologis, serta pembayaran restitusi. Dengan kerangka ini, negara tidak berhenti

pada penghukuman pelaku, tetapi juga mengurangi risiko kejahatan dan memulihkan posisi korban.

Perlindungan korban juga membutuhkan kepastian mengenai perbuatan yang dilarang dan pihak yang bertanggung jawab. Kejahatan *deepfake* dapat melibatkan pengguna yang memberikan perintah, pembuat atau pengelola aplikasi, penyebar konten, serta platform yang memfasilitasi peredaran (Reza et al., 2026). Hukum pidana tetap harus menilai kendali manusia, pengetahuan, kesengajaan, dan kontribusi masing-masing pihak. Pendekatan tersebut mencegah pelaku mengalihkan tanggung jawab kepada sistem kecerdasan buatan yang pada dasarnya bekerja berdasarkan perintah, data, dan pengendalian manusia (Zumarno et al., 2026).

Teori viktimologi

Viktimologi mengkaji korban, proses terjadinya viktimisasi, hubungan korban dengan pelaku, dampak kejahatan, serta bentuk perlindungan dan pemulihan yang dibutuhkan (Rohmat, 2024). Kajian ini tidak menempatkan korban sebagai pihak pasif, tetapi memperhatikan pengalaman, kerugian, kerentanan, dan hak korban selama proses peradilan. Viktimologi juga membantu hukum menentukan langkah untuk mencegah korban baru dan mengurangi risiko reviktimisasi (Rohmat, 2024). Dalam hukum pidana, perhatian tersebut diwujudkan melalui perlindungan fisik dan psikis, bantuan hukum, restitusi, kompensasi, rehabilitasi, dan jaminan keamanan (Kenedi, 2020).

Korban pornografi *deepfake* menghadapi bentuk viktimisasi yang khas karena tubuhnya tidak selalu terlibat secara langsung, tetapi identitas dan wajahnya digunakan untuk membangun kesan seolah-olah korban melakukan tindakan seksual (Kasita, 2022). Masyarakat yang tidak dapat membedakan konten asli dan hasil manipulasi dapat memberikan stigma, menyalahkan korban, atau menyebarkan kembali konten tersebut. Akibatnya, penderitaan korban berlangsung di ruang digital dan sosial secara bersamaan (Mutmainnah et al., 2024). Perspektif viktimologi menuntut sistem hukum untuk menghapus konten, menghentikan penyebaran, mengoreksi informasi yang merugikan, dan memulihkan rasa aman serta nama baik korban.

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum doktrinal. Penelitian doktrinal dilakukan melalui studi kepustakaan untuk menganalisis norma, asas, konsep, dan doktrin hukum yang berkaitan dengan perlindungan korban pornografi berbasis *Artificial Intelligence*. Pendekatan yang digunakan meliputi pendekatan perundang-undangan dan pendekatan konseptual. Pendekatan perundang-undangan menelaah kesesuaian dan hubungan

antarketentuan, sedangkan pendekatan konseptual digunakan untuk memahami perlindungan hukum, viktimologi, pertanggungjawaban, dan pemulihan nama baik.

Bahan hukum primer terdiri atas Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, serta Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. Bahan hukum sekunder terdiri atas buku, jurnal, skripsi, tesis, dan artikel ilmiah yang membahas pornografi, *deepfake*, perlindungan korban, viktimologi, serta penegakan hukum digital. Bahan hukum tersier berupa kamus dan sumber penunjang untuk menjelaskan istilah yang digunakan.

Peneliti mengumpulkan bahan hukum melalui studi dokumen, kemudian mengelompokkannya berdasarkan dua fokus penelitian. Fokus pertama membahas dasar hukum dan bentuk perlindungan korban, sedangkan fokus kedua membahas pemulihan nama baik melalui penghapusan konten, hak untuk dilupakan, restitusi, rehabilitasi, dan pendampingan. Bahan hukum dianalisis secara kualitatif dengan menafsirkan ketentuan, menghubungkan konsep, membandingkan ruang lingkup pengaturan, dan menemukan kekosongan atau keterbatasan norma. Hasil analisis disajikan secara deskriptif dan argumentatif untuk menjawab rumusan masalah.

4. HASIL DAN PEMBAHASAN

Perlindungan hukum terhadap korban pornografi berbasis *Artificial Intelligence*

Pornografi berbasis *Artificial Intelligence* memiliki karakter yang berbeda dari pornografi konvensional. Pelaku tidak harus merekam tubuh korban karena foto wajah yang tersedia secara terbuka dapat diunduh, diolah, dan ditempelkan pada tubuh orang lain. Konten yang dihasilkan dapat terlihat meyakinkan dan mudah disebarkan dalam waktu singkat. Perbedaan tersebut memengaruhi pembuktian, penentuan kesengajaan, penelusuran pelaku, dan kemampuan korban untuk menghentikan peredaran konten.

Tabel 1. Perbedaan Pornografi Berbasis *Artificial Intelligence* dan Pornografi Non-AI

Aspek	Pornografi berbasis AI	Pornografi non-AI
Cara memperoleh konten	Rekayasa digital dapat menggunakan foto atau rekaman korban yang tersedia di media sosial.	Konten berasal dari dokumentasi langsung, perekaman tersembunyi, peretasan, atau penyebaran materi intim.
Objek yang dimanipulasi	Wajah, suara, atau identitas korban ditempatkan pada tubuh atau adegan yang tidak pernah dilakukan korban.	Foto atau video menampilkan tubuh atau tindakan yang benar-benar direkam.

Pembuktian	Mebutuhkan pemeriksaan keaslian, jejak digital, perintah pengguna, dan keterlibatan sistem kecerdasan buatan.	Berfokus pada asal rekaman, persetujuan, penguasaan, dan penyebaran konten.
Risiko pengulangan	Konten dapat diproduksi ulang menggunakan foto yang sama meskipun satu unggahan telah dihapus.	Konten tetap dapat disalin dan disebar, tetapi tidak selalu dapat dibuat ulang tanpa materi awal.
Kebutuhan pemulihan	Penghapusan konten harus disertai pencegahan produksi ulang, pemulihan reputasi, dan dukungan psikologis.	Penghapusan, penghentian penyebaran, pemulihan reputasi, dan dukungan korban.

Sumber: Diolah dari hasil penelitian berdasarkan Chesney dan Citron (2019), Kasita (2022), serta Pramodya et al. (2024).

Tabel 1 menunjukkan bahwa kerugian korban tidak dapat dinilai hanya dari keberadaan gambar atau video. Pelaku membangun representasi palsu yang menempatkan identitas korban dalam adegan seksual tanpa persetujuan. Korban kemudian menanggung akibat seolah-olah konten tersebut benar, padahal korban tidak pernah melakukan perbuatan yang ditampilkan. Karakter ini memperkuat kebutuhan perlindungan yang berorientasi pada penghentian penyalahgunaan identitas dan pemulihan nama baik.

Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi menjadi dasar pertama untuk menilai konten yang memuat kecabulan atau eksploitasi seksual melalui berbagai media (Republik Indonesia, 2008). Ruang lingkup gambar, ilustrasi, foto, animasi, dan bentuk pesan lain dapat digunakan untuk menjangkau hasil manipulasi digital (Chazawi, 2016). Larangan memproduksi, membuat, memperbanyak, menggandakan, menyebarkan, menyiarkan, dan menyediakan pornografi dapat diarahkan kepada pembuat maupun penyebar konten (Republik Indonesia, 2008). Undang-undang tersebut tidak menjelaskan teknologi *deepfake*, penggunaan perintah pada sistem kecerdasan buatan, atau penggunaan wajah korban yang berasal dari data publik.

Undang-Undang Informasi dan Transaksi Elektronik memberikan dasar ketika pelaku mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya dokumen elektronik bermuatan melanggar kesusilaan. Ketentuan mengenai serangan terhadap kehormatan atau nama baik juga dapat digunakan dalam keadaan tertentu. Walaupun demikian, inti pornografi *deepfake* tidak selalu terletak pada tuduhan verbal, tetapi pada eksploitasi seksual dan manipulasi identitas. Penerapan ketentuan pencemaran nama baik secara tunggal berisiko mengabaikan dimensi kekerasan seksual, privasi, dan pengendalian data pribadi korban (Natalia & Layang, 2024).

Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual memperkuat kedudukan korban melalui hak atas penanganan, perlindungan, dan pemulihan (Republik Indonesia, 2022). Hak tersebut meliputi informasi mengenai proses hukum, layanan hukum, layanan kesehatan, penguatan psikologis, pendampingan, perlindungan dari ancaman,

serta pemulihan sosial. Kerangka ini penting karena korban pornografi berbasis kecerdasan buatan sering mengalami tekanan yang tidak selesai hanya dengan pemidanaan pelaku (Apriana et al., 2025). Negara perlu memastikan korban tetap memperoleh layanan sejak pelaporan sampai tahap pemulihan jangka panjang.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga relevan ketika pelaku mengambil foto, wajah, atau data lain untuk membuat konten tanpa persetujuan (Republik Indonesia, 2022). Wajah seseorang dapat menjadi data pribadi karena mampu mengidentifikasi subjek data, sedangkan pengubahan dan penyebarannya merupakan bentuk pemrosesan. Perlindungan data pribadi memberi dasar untuk menuntut penghentian pemrosesan, penghapusan, dan pertanggungjawaban atas penggunaan data yang melawan hukum. Penerapan norma tetap membutuhkan kemampuan menelusuri pihak yang mengumpulkan data, mengoperasikan sistem, dan menyebarkan hasil manipulasi (Zumarno et al., 2026).

Kitab Undang-Undang Hukum Pidana memuat ketentuan mengenai pornografi dan serangan terhadap kehormatan yang dapat digunakan sesuai unsur perbuatan (Republik Indonesia, 2023). Norma tersebut tetap harus diterapkan berdasarkan asas legalitas dan pembuktian kesalahan pelaku. Dalam konteks kecerdasan buatan, pengguna yang memilih foto korban, memberikan perintah, mengatur hasil, menyimpan, dan menyebarkan konten tetap memiliki kendali manusia atas rangkaian perbuatan (Reza et al., 2026). Karena itu, penggunaan sistem kecerdasan buatan tidak menghapus pertanggungjawaban ketika pelaku mengetahui akibat perbuatannya dan tetap menghendaki atau menerima risiko tersebut.

Perlindungan preventif dan represif

Perlindungan preventif perlu dimulai dari norma yang jelas mengenai larangan membuat, memiliki untuk tujuan penyebaran, memperjualbelikan, mengancam dengan, dan mendistribusikan pornografi *deepfake* tanpa persetujuan. Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 telah memberikan arahan etika penggunaan kecerdasan artifisial (Kementerian Komunikasi dan Informatika Republik Indonesia, 2023). Surat edaran belum setara dengan larangan pidana yang mengikat secara khusus. Pemerintah perlu menghubungkan etika teknologi dengan kewajiban hukum bagi pengembang, penyedia aplikasi, dan platform digital. Pengaturan tersebut harus memuat pengamanan desain, mekanisme pelaporan, penyimpanan bukti, pembatasan akses, serta tindakan cepat terhadap konten ilegal.

Literasi digital juga menjadi bagian penting dari perlindungan preventif. Masyarakat perlu memahami bahwa foto yang diunggah secara terbuka dapat disalahgunakan, tetapi

penggunaan foto tersebut tetap menjadi tanggung jawab pelaku dan tidak dapat menjadi alasan untuk menyalahkan korban. Pendidikan digital perlu membahas pengamanan akun, persetujuan penggunaan data, cara mengenali manipulasi, prosedur pelaporan, dan larangan menyebarkan ulang konten (Mutmainnah et al., 2024). Pendekatan ini dapat mengurangi penyebaran sekunder dan mencegah stigma yang memperberat penderitaan korban.

Platform digital memegang peran strategis karena konten biasanya beredar melalui media sosial, layanan pesan, forum, atau penyimpanan daring. Penyelenggara sistem elektronik perlu menyediakan jalur pelaporan yang mudah, menjaga kerahasiaan korban, melakukan penilaian cepat, membatasi akses, dan menghapus konten yang melanggar. Sistem pencocokan jejak digital dapat digunakan untuk mencegah pengunggahan ulang konten yang sama, sedangkan penyimpanan terbatas atas bukti diperlukan agar penghapusan tidak menghilangkan dasar penyidikan. Keseimbangan antara penghapusan cepat dan preservasi bukti harus diatur dalam prosedur yang melibatkan platform dan aparat penegak hukum.

Perlindungan represif bekerja setelah kejahatan terjadi. Korban harus memperoleh akses pelaporan yang aman, pemeriksaan yang tidak menyalahkan korban, pendampingan hukum, perlindungan identitas, serta informasi perkembangan perkara. Aparat penegak hukum perlu menelusuri perangkat, akun, alamat jaringan, riwayat perintah, metadata, transaksi, dan jalur penyebaran untuk menentukan keterlibatan setiap pihak (Wibowo et al., 2023). Kapasitas forensik digital sangat menentukan karena bukti dapat dihapus, dimodifikasi, atau ditempatkan pada layanan yang berada di luar wilayah hukum Indonesia.

Penegakan hukum juga harus membedakan pembuat, pemesan, pemilik untuk tujuan distribusi, penyebar, dan pihak yang memperoleh keuntungan (Reza et al., 2026). Perbedaan tersebut diperlukan agar pertanggungjawaban sesuai dengan perbuatan dan tingkat kesalahan masing-masing. Pengembang atau platform tidak otomatis bertanggung jawab atas setiap penyalahgunaan, tetapi tanggung jawab dapat muncul ketika mereka mengetahui risiko, mengabaikan laporan, atau tidak menjalankan kewajiban pencegahan yang ditentukan hukum (Zumarno et al., 2026). Pendekatan tanggung jawab berlapis dapat menghindari kekosongan perlindungan tanpa mengabaikan asas kesalahan dan proses hukum yang adil.

Tabel 2. Pemetaan Dasar Hukum dan Bentuk Perlindungan Korban

Instrumen hukum	Ruang perlindungan	Keterbatasan penerapan
Undang-Undang Pornografi	Larangan produksi, pembuatan, penggandaan, penyebaran, dan penyediaan pornografi.	Belum menyebut manipulasi wajah, perintah AI, dan produksi ulang konten secara khusus.
Undang-Undang Informasi dan Transaksi Elektronik	Penindakan distribusi muatan kesusilaan, perlindungan informasi elektronik, dan penghapusan informasi yang tidak relevan.	Penghapusan membutuhkan prosedur dan sering terlambat setelah konten tersebar luas.

Undang-Undang Perlindungan Data Pribadi	Perlindungan atas pengumpulan, penggunaan, perubahan, dan penyebaran data pribadi tanpa hak.	Pelaku, pengendali, dan jalur pemrosesan data sulit diidentifikasi.
Undang-Undang Tindak Pidana Kekerasan Seksual	Hak atas penanganan, perlindungan, pemulihan, restitusi, layanan hukum, medis, psikologis, dan sosial.	Penerapan terhadap pornografi deepfake memerlukan penafsiran dan koordinasi lembaga.
Kitab Undang-Undang Hukum Pidana	Ketentuan pornografi dan serangan terhadap kehormatan sesuai unsur perbuatan.	Belum merinci pertanggung-jawaban dalam rantai penggunaan sistem kecerdasan buatan.

Sumber: Diolah dari Undang-Undang Nomor 44 Tahun 2008, Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022, Undang-Undang Nomor 12 Tahun 2022, dan Undang-Undang Nomor 1 Tahun 2023.

Pemulihan nama baik korban

Pemulihan nama baik merupakan bagian utama dari perlindungan korban karena konten *deepfake* membangun gambaran palsu yang dapat dipercaya oleh masyarakat. Pemidanaan pelaku tidak otomatis menghilangkan unggahan, salinan, hasil pencarian, atau penilaian negatif terhadap korban. Karena itu, pemulihan harus berjalan bersama proses pidana dan tidak menunggu putusan berkekuatan hukum tetap ketika keselamatan serta reputasi korban membutuhkan tindakan segera. Pemulihan tersebut mencakup penghentian penyebaran, penghapusan konten, koreksi informasi, perlindungan identitas, dukungan psikologis, serta pemulihan sosial dan ekonomi.

Hak untuk dilupakan atau *right to be forgotten* memberikan dasar bagi seseorang untuk meminta penghapusan informasi elektronik yang tidak relevan dan merugikan dirinya (Republik Indonesia, 2016). Dalam kasus pornografi berbasis kecerdasan buatan, prinsip ini penting karena konten tidak menggambarkan perbuatan nyata korban. Penghapusan dapat diarahkan kepada unggahan, tautan, hasil pencarian, salinan tersimpan pada layanan publik, dan akun yang terus menyebarkan materi. Pelaksanaannya menghadapi kendala ketika konten disimpan secara pribadi, disebar ulang, dipindahkan ke platform lain, atau diproduksi kembali dengan menggunakan foto korban yang sama (Suryokencono & Isyraq, 2025).

Mekanisme penghapusan perlu sederhana dan berorientasi pada korban. Korban seharusnya dapat melaporkan satu peristiwa melalui jalur terpadu tanpa mengulang cerita dan mengirim konten sensitif kepada banyak pihak. Platform perlu memberikan tanda terima, batas waktu pemeriksaan, informasi tindakan, dan mekanisme keberatan. Aparat penegak hukum tetap dapat menyimpan salinan bukti secara terbatas dan aman agar penghapusan publik tidak menghambat penyidikan.

Pemulihan psikologis harus tersedia karena korban dapat mengalami trauma, kecemasan, depresi, rasa malu, dan ketakutan terhadap penyebaran ulang (Rohmat, 2024). Lembaga Perlindungan Saksi dan Korban, unit pelayanan perempuan dan anak, tenaga kesehatan, psikolog, dan pendamping hukum perlu bekerja secara terkoordinasi (Kenedi, 2020).

Pendampingan tidak boleh berhenti setelah laporan dibuat karena proses hukum dan peredaran konten dapat berlangsung dalam waktu panjang. Perlindungan juga harus mencegah tekanan, ancaman, perundungan, dan penyebaran identitas korban selama pemeriksaan dan pemberitaan.

Restitusi dapat digunakan untuk mengganti kerugian materiil dan immateriil yang timbul akibat kejahatan. Kerugian materiil dapat berupa biaya kesehatan, pendampingan, keamanan digital, kehilangan pekerjaan, dan biaya hukum, sedangkan kerugian immateriil berkaitan dengan penderitaan, trauma, rusaknya reputasi, dan hilangnya kesempatan. Penilaian kerugian immateriil memang tidak mudah, tetapi kesulitan tersebut tidak boleh menghilangkan hak korban. Putusan perlu memperhitungkan kemampuan pelaku, mekanisme pembayaran, penyitaan aset, dan alternatif pemulihan ketika pelaku tidak mampu membayar.

Pemulihan nama baik juga membutuhkan tindakan komunikasi publik secara hati-hati. Dalam keadaan tertentu, korban memerlukan pernyataan resmi bahwa konten merupakan hasil manipulasi, bukan rekaman asli. Klarifikasi dapat dikeluarkan oleh aparat, lembaga pendidikan, tempat kerja, atau platform sesuai konteks dan atas persetujuan korban. Langkah ini harus menjaga kerahasiaan serta tidak mengulang penyebaran konten yang justru memperluas kerugian.

Kesenjangan pengaturan dan arah pembaruan hukum

Hasil penelitian menunjukkan bahwa perlindungan korban telah memiliki dasar hukum, tetapi dasar tersebut tersebar dalam beberapa undang-undang. Setiap undang-undang mengatur bagian yang berbeda, yaitu pornografi, distribusi elektronik, data pribadi, kekerasan seksual, dan pemulihan korban. Pemisahan ini membuat aparat harus membangun hubungan antarnorma ketika menangani satu peristiwa. Kondisi tersebut dapat menimbulkan ketidakpastian, terutama terhadap pembuatan konten yang belum disebarkan, kepemilikan untuk tujuan tertentu, tanggung jawab penyedia teknologi, dan kewajiban platform.

Pembaruan hukum perlu merumuskan pornografi *deepfake* secara jelas sebagai pembuatan atau manipulasi konten seksual yang menampilkan identitas seseorang tanpa persetujuan. Norma juga perlu membedakan pembuatan, penguasaan untuk tujuan penyebaran, ancaman penyebaran, distribusi, perdagangan, dan pengulangan produksi. Pengaturan harus tetap mengecualikan penggunaan yang sah untuk penegakan hukum, penelitian, pendidikan, atau kepentingan lain yang memiliki dasar dan pengamanan memadai. Rumusan yang rinci dapat menjaga kepastian hukum sekaligus mencegah kriminalisasi yang terlalu luas.

Pertanggungjawaban perlu berangkat dari kendali manusia. Pengguna yang memilih korban, menyediakan data, memberi perintah, menerima hasil, memperbaiki keluaran, dan menyebarkannya merupakan pihak utama yang harus dimintai pertanggungjawaban. Pihak lain dapat dimintai tanggung jawab sesuai pengetahuan, kendali, keuntungan, dan kewajiban hukum yang dilanggar. Model ini mempertahankan asas kesalahan sekaligus mengakui bahwa kejahatan digital dapat berlangsung melalui rantai perbuatan yang melibatkan lebih dari satu pihak.

Pembaruan hukum juga harus mewajibkan respons cepat terhadap korban. Aturan perlu menentukan batas waktu penghapusan sementara, preservasi bukti, penanganan unggahan ulang, komunikasi lintas platform, dan kerja sama lintas negara. Aparat penegak hukum membutuhkan pelatihan serta fasilitas forensik digital untuk memeriksa metadata, jejak perintah, perangkat, dan pola manipulasi. Lembaga perlindungan korban perlu memperoleh prosedur khusus agar bantuan hukum, psikologis, sosial, dan restitusi dapat berjalan sejak awal.

Dengan demikian, perlindungan yang efektif harus menggabungkan pendekatan preventif dan represif. Pendekatan preventif menutup peluang penyalahgunaan melalui norma, desain teknologi, literasi, dan pengawasan, sedangkan pendekatan represif menindak pelaku serta memulihkan korban setelah kejahatan terjadi (Apriana et al., 2025). Pendekatan viktimologi memastikan bahwa ukuran keberhasilan tidak hanya dilihat dari jumlah pelaku yang dihukum, tetapi juga dari berhentinya peredaran konten, pulihnya rasa aman, dan kembalinya nama baik korban (Mahardika, 2025). Arah pembaruan tersebut sesuai dengan kebutuhan perlindungan yang komprehensif dalam menghadapi perubahan pola kejahatan digital.

5. KESIMPULAN DAN SARAN

Perlindungan hukum terhadap korban kejahatan pornografi berbasis *Artificial Intelligence* saat ini bersumber dari Undang-Undang Pornografi, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Undang-Undang Tindak Pidana Kekerasan Seksual, dan Kitab Undang-Undang Hukum Pidana. Ketentuan tersebut dapat digunakan untuk menindak pembuat dan penyebar, melindungi data pribadi, serta memberikan hak atas penanganan dan pemulihan. Namun, pengaturannya masih tersebar dan belum menjelaskan pornografi deepfake, rantai pertanggungjawaban, kewajiban platform, dan mekanisme pencegahan produksi ulang secara khusus. Perlindungan korban harus memadukan langkah preventif berupa regulasi, literasi digital, pengawasan teknologi, dan

mekanisme pelaporan dengan langkah represif berupa penyidikan, pemidanaan, penghapusan konten, bantuan hukum, rehabilitasi psikologis, restitusi, dan perlindungan dari stigma.

Pemulihan nama baik perlu ditempatkan sebagai bagian inti dari penyelesaian perkara karena penghukuman pelaku tidak otomatis menghilangkan konten atau penilaian negatif terhadap korban. Pemerintah perlu membentuk aturan yang lebih spesifik mengenai pembuatan dan penyebaran pornografi berbasis kecerdasan buatan, memperkuat kapasitas forensik digital, serta menetapkan kewajiban respons cepat bagi penyelenggara sistem elektronik. Lembaga perlindungan korban harus menyediakan layanan terpadu yang menjaga kerahasiaan, memfasilitasi penghapusan konten, memberikan pendampingan psikologis dan hukum, serta membantu pengajuan restitusi. Penelitian berikutnya dapat menguji pelaksanaan mekanisme penghapusan konten dan pemulihan korban pada kasus konkret agar pembaruan hukum tidak berhenti pada rumusan normatif.

UCAPAN TERIMA

Bagian ini disediakan bagi penulis untuk menyampaikan ucapan terima kasih, baik kepada pihak penyandang dana penelitian, pendukung fasilitas, atau bantuan ulasan naskah. Bagian ini juga dapat digunakan untuk memberikan pernyataan atau penjelasan, apabila artikel ini merupakan bagian dari skripsi/tesis/disertasi/makalah konferensi/hasil penelitian.

DAFTAR REFERENSI

- Andani, I. K. (2025). *Pertanggungjawaban pidana deepfake mengandung unsur pornografi melalui Artificial Intelligence (AI)*. Universitas Borneo Tarakan.
- Apriana, M., Fransisco, & Nugroho, A. (2025). Perlindungan hukum bagi perempuan korban tindak pidana kejahatan *Artificial Intelligence (AI)* deepfake berdasarkan Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual. *Journal of Social and Economics Research*, 7(1), 57–75. <https://doi.org/10.54783/jser.v7i1.796>
- Chairani, M. A., Yitawati, K., & Pradhana, A. P. (2024). Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake. *Jurnal Rechtsens*, 13(1), 81–96. <https://doi.org/10.56013/rechtsens.v13i1.2668>
- Chazawi, A. (2016). *Tindak Pidana Pornografi* (Edisi pertama). Sinar Grafika. <https://jdih.kemenkoinfra.go.id/tindak-pidana-pornografi>
- Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>
- Hadjon, P. M., Martosoewignjo, R. S. S., Basah, S., Manan, B., Marzuki, L., ten Berge, J. B. J. M., van Buuren, P. J. J., & Stroink, F. A. M. (2011). *Pengantar Hukum Administrasi Indonesia* (Cetakan ke-11). Gadjah Mada University Press.

- Indonesia, K. K. dan I. R. (2023). *Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial*. Kementerian Komunikasi dan Informatika Republik Indonesia. https://jdih.komdigi.go.id/produk_hukum/view/id/883/t/surat+edaran+menteri+komunikasi+dan+informatika+nomor+9+tahun+2023
- Kasita, I. D. (2022). Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) di Era Pandemi Covid-19. *Jurnal Wanita Dan Keluarga*, 3(1), 16–26. <https://doi.org/10.22146/jwk.5202>
- Kenedi, J. (2020). *Perlindungan Saksi dan Korban: Studi Perlindungan Hukum Korban Kejahatan dalam Sistem Peradilan di Indonesia* (Edisi pertama). Pustaka Pelajar.
- Lestari, N. S. (2024). *Kebijakan formulasi hukum pidana atas praktik deepfake dilihat dari perspektif kejahatan siber dan pornografi* [Universitas Sriwijaya]. <https://repository.unsri.ac.id/145395/>
- Mahardika, M. I. (2025). Tinjauan yuridis terhadap pelaku deepfake porn sebagai kekerasan gender berbasis online menurut UU Pornografi. *Lex Privatum*, 14(5), 1–15. <https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/60226>
- Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika teknologi deepfake sebagai masa depan hoaks yang semakin meningkat: Solusi strategis ditinjau dari literasi digital. *UPGRADE: Jurnal Pendidikan Teknologi Informasi*, 1(2), 67–72. <https://doi.org/10.30812/upgrade.v1i2.3702>
- Natalia, C., & Layang, I. W. B. S. (2024). Perlindungan hukum bagi korban pornografi deepfake dalam konteks hukum Indonesia. *Jurnal Kertha Desa*, 12(5), 4462–4473. <https://ojs.unud.ac.id/index.php/kerthadesa/article/view/114714>
- Putra, H. I. (2024). *Perlindungan hukum terhadap korban penyalahgunaan Artificial Intelligence (AI) berupa deepfake pornografi menurut peraturan perundang-undangan* [Universitas Jambi]. <https://repository.unja.ac.id/id/eprint/65718>
- Rahayu, R. A. S., & Santoso, H. (2023). Analysis of Fake Face Images: Detecting the Authenticity of Manipulated Images Using Variational Autoencoder Methods and Deep Neural Network Forensics. *SIBATIK Journal*, 2(9), 2701–2726. <https://doi.org/10.54443/sibatik.v2i9.1312>
- Reza, D., Utama, M., & Yuningsih, H. (2026). Artificial Intelligence-Generated Deepfake Pornography: A Normative Analysis of Criminal Liability and Victim Protection in Indonesian Law. *Ius Poenale*, 7(1), 1–10. <https://doi.org/10.25041/ip.v7i1.4738>
- Rohmat, N. (2024). *Hukum Kriminologi dan Viktimologi* (H. T. Samudra (ed.)). K-Media. <https://kmedia.co.id/product/hukum-kriminologi-dan-viktimologi/>
- Suryokencono, P., & Isyraq, R. F. (2025). Perlindungan hukum berupa pemulihan nama baik terhadap korban tindak pencemaran nama baik melalui situs deepfake. *National Multidisciplinary Sciences*, 3(4), 587–596. <https://proceeding.unmuhjember.ac.id/index.php/nms/article/view/719>
- Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (2024). <https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024>
- Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (2022). <https://peraturan.bpk.go.id/Details/207944/uu-no-12-tahun-2022>

- Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (2016).
<https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016>
- Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022).
<https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi (2008).
<https://peraturan.bpk.go.id/Details/39740/uu-no-44-tahun-2008>
- Wibowo, A., Wangsajaya, Y., & Surahmat, A. (2023). *Pemolisian Digital dengan Artificial Intelligence*. PT RajaGrafindo Persada–Rajawali Pers.
<https://www.rajagrafindo.co.id/produk/pemolisian-digital-dengan-artificial-intelligence/>
- Zumarno, G. C., Lesmana, S. J., & Indayatun, R. (2026). Bridging Legal Gaps in AI-Generated Deepfake Pornography: A Comparative Approach to Privacy and Digital Ethics. *Jurnal Ius Constituendum*, 11(2), 237–263. <https://doi.org/10.26623/jic.v11i2.12664>