

## PERAN TEKNOLOGI INFORMASI DALAM PENCEGAHAN DAN PENANGANAN PENYEBARAN GAMBAR PRIBADI TANPA IZIN: ANALISIS HUKUM DAN SISTEM

Alicia Nurul Hidayah <sup>1</sup>, Desvita Khanza Salsabila <sup>2</sup>, Dinda Prama Suari <sup>3</sup>, Triana <sup>4</sup>

<sup>1,2,3,4</sup> Universitas Duta Bangsa, Indonesia

[alicianurulhh@gmail.com](mailto:alicianurulhh@gmail.com) <sup>1</sup>, [desvitasalsabila77@gmail.com](mailto:desvitasalsabila77@gmail.com) <sup>2</sup>, [pramasuarid@gmail.com](mailto:pramasuarid@gmail.com) <sup>3</sup>,  
[triana@udb.ac.id](mailto:triana@udb.ac.id) <sup>4</sup>

### ABSTRACT

The development of information technology (IT) brings both positive impacts and new challenges, one of which is the unauthorized dissemination of private images (revenge porn and deepfake). This phenomenon not only violates privacy but also causes severe psychological trauma to victims. This research analyzes the role of IT in preventing and handling such cases, and evaluates the effectiveness of existing legal regulations. The method used is a normative juridical approach with a focus on analyzing the ITE Law, TPKS Law, and PDP Law in Indonesia, as well as comparisons with international regulations such as GDPR in Europe. The results show that IT plays an important role through technologies such as AI, blockchain, and encryption, but there are still weaknesses in automatic detection and system response. In terms of law, regulations in Indonesia are still fragmentary and less comprehensive than other countries such as the UK and Australia. Legal harmonization, strengthened law enforcement capacity, and global collaboration are needed to create more effective protection for victims.

**Keywords** *information technology, cyberlaw, deepfake, data protection*

### ABSTRAK

Perkembangan teknologi informasi (TI) membawa dampak positif sekaligus tantangan baru, salah satunya adalah penyebaran gambar pribadi tanpa izin (*revenge porn* dan *deepfake*). Fenomena ini tidak hanya melanggar privasi tetapi juga menimbulkan trauma psikologis berat bagi korban. Penelitian ini menganalisis peran TI dalam pencegahan dan penanganan kasus tersebut, serta mengevaluasi efektivitas regulasi hukum yang ada. Metode yang digunakan adalah pendekatan yuridis normatif dengan fokus pada analisis UU ITE, UU TPKS, dan UU PDP di Indonesia, serta perbandingan dengan regulasi internasional seperti GDPR di Eropa. Hasil penelitian menunjukkan bahwa TI berperan penting melalui teknologi seperti *AI*, *blockchain*, dan *encryption*, namun masih terdapat kelemahan dalam deteksi otomatis dan respons sistem. Dari sisi hukum, regulasi di Indonesia masih fragmentaris dan kurang komprehensif dibandingkan negara lain seperti Inggris dan Australia. Diperlukan harmonisasi hukum, penguatan kapasitas penegak hukum, dan kolaborasi global untuk menciptakan perlindungan yang lebih efektif bagi korban.

### Article History

Received: Juli 2025

Reviewed: Juli 2025

Published: Juli 2025

Plagiarism Checker No  
235

Prefix DOI :

[10.8734/Kohesi.v1i2.365](https://doi.org/10.8734/Kohesi.v1i2.365)

Copyright : Author

Publish by : Kohesi



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)



<b>Kata Kunci:</b> <i>Teknologi Informasi, Hukum Cyber, Deepfake, Perlindungan Data</i>	
---	--

## 1. PENDAHULUAN

Pengembangan lebih lanjut dalam teknologi informasi telah disediakan dalam era digital yang semakin maju. Perkembangan ini sangat menguntungkan banyak aspek kehidupan. Dengan kemajuan teknologi, muncul masalah baru seperti penyalahgunaan teknologi yang dapat merugikan orang dan masyarakat. Penyalahgunaan teknologi digital juga muncul dalam bentuk *revenge pornografi* dalam beberapa tahun terakhir. *Revenge pornografi* adalah penyebaran konten pornografi intim atau tau tanpa persetujuan korban, biasanya dilakukan oleh mantan pasangan sebagai balas dendam. Fenomena ini tidak hanya melanggar privasi tetapi juga menimbulkan trauma psikologis bagi korban, bahkan dapat merusak reputasi mereka dan kehidupan sosial mereka atau platform online, membuatnya sulit untuk keluar dari internet sepenuhnya. Dampaknya bisa sangat membahayakan, mulai dari depresi dan kecemasan hingga risiko kehilangan pekerjaan atau dipandang rendah secara sosial. Meskipun banyak negara telah menetapkan undang-undang yang ketat untuk melawan pornografi balas dendam, masalah terbesar masih terletak pada penegakan hukum dan kesadaran publik akan pentingnya menghormati privasi orang lain. Korban sering merasa malu dan takut untuk melaporkan, sehingga kasus seperti ini sering tidak terungkap. Untuk mencegah penyalahgunaan teknologi yang merugikan ini, orang harus lebih dididik tentang konsekuensi hukum dan moral dari pornografi pemukulan.

*Porn revenge*, atau penyebaran konten sensitif tanpa persetujuan korban, telah berkembang menjadi jenis kekerasan digital yang berbahaya bagi privasi dan kesehatan mental. Data yang dikumpulkan oleh *Cyber Civil Rights Initiative (CCRI)* menunjukkan bahwa sekitar 93% korban mengalami trauma emosional berat, termasuk kecemasan, depresi, dan keinginan bunuh diri. Karena konten tersebut mudah menyebar melalui internet dan sulit dihapus sepenuhnya, masalah ini menjadi semakin kompleks. Fenomena ini telah menarik perhatian para ahli. *Dalam bukunya yang berjudul Hate Crimes in Cyberspace (2014)*, pakar hukum siber dari University of Virginia Danielle Citron menyatakan bahwa pornografi sering digunakan sebagai alat kekerasan berbasis gender untuk mempermalukan korban, khususnya perempuan.

Presiden CCRI Mary Anne Franks menekankan bahwa pemukulan pornografi merupakan bentuk kontrol sosial yang merusak kehidupan korban, bukan hanya pelanggaran privasi. Untuk



memberikan perlindungan hukum yang lebih kuat, ia mendorong pelaksanaan undang-undang khusus, seperti Undang-Undang Hak Masyarakat Cyber AS. Dari sisi psikologis, Dr. Emma Short dari De Montfort University menemukan bahwa dampak *revenge porn* pada korban mirip dengan *Post-Traumatic Stress Disorder* (PTSD), di mana rasa malu, ketakutan, dan trauma terus menghantui mereka. Menurut penelitian yang dia lakukan, dukungan sosial dan psikologis sangat penting untuk membantu pemulihan korban. Meskipun beberapa negara telah menetapkan peraturan, seperti Inggris dengan *Revenge Porn Helpline* dan Indonesia dengan UU ITE Pasal 27 ayat 1, masalah terbesar tetap pada penegakan hukum dan kesadaran masyarakat. Menurut *Electronic Frontier Foundation* (EFF), banyak kasus yang tidak dilaporkan karena korban malu atau takut. Oleh karena itu, di era teknologi yang semakin maju ini, memperkuat hukum dan memberikan pelatihan etika digital serta bantuan kepada korban merupakan langkah penting untuk memerangi pornografi pemulihan.

Di era digital, di mana teknologi informasi (TI) bukan hanya sarana kejahatan tetapi juga solusi untuk pencegahan dan penangganya, penyebaran gambar pribadi tanpa izin, termasuk porn revenge dan deepfake, telah menjadi masalah besar. Berbagai negara telah mengadopsi undang-undang khusus yang mengkriminalisasi penyebaran konten intim non konsensual. Beberapa contohnya adalah UU ITE Indonesia dan *Digital Millennium Copyright Act* (DMCA) AS. Namun, hukum-hukum ini seringkali menghadapi masalah teknis, seperti menemukan pelaku dan menghapus konten secara menyeluruh dari internet. Teknologi informasi menjadi sangat penting di sini, mulai dari sistem kecerdasan buatan (AI) yang dapat mendeteksi dan memblokir konten ilegal secara otomatis hingga penggunaan blockchain untuk melacak sumbernya. Selain masalah hukum, metode teknologi juga dapat membantu dalam pelaporan dan pemulihan penyakit korban. Untuk membantu korban menghapus konten pornografi, platform media sosial seperti Facebook dan Instagram telah bekerja sama dengan organisasi seperti *Cyber Civil Rights Initiative* (CCRI) untuk mengembangkan alat pelaporan khusus untuk *revenge porn*. Selain itu, pengembangan aplikasi berbasis enkripsi dan penyimpanan aman dapat menawarkan perlindungan proaktif bagi pengguna saat menyimpan informasi pribadi mereka. Tantangan tetap ada, bagaimanapun, seperti perbedaan digital, kurangnya kesadaran masyarakat, dan kebutuhan akan kerja sama global untuk menangani kasus lintas negara.

Dalam hal perlindungan privasi digital, dasolen yang ideal seharusnya dibuat melalui pendekatan menyeluruh yang memasukkan elemen pencegahan, represif, dan restoratif. (1) definisi jelas dari penyebaran gambar pribadi tanpa izin sebagai kejahatan khusus (khusus kejahatan), (2) pengakuan hak permanen korban atas penghapusan konten (hak untuk dilupakan), dan (3) kewajiban penyedia platform untuk bertindak proaktif. Sangat penting bagi



negara untuk menyesuaikan undang-undangnya dengan peraturan internasional seperti GDPR, terutama dalam hal sanksi pencegahan dan sistem pelaporan. Solusi legislatif ideal adalah undang-undang khusus yang mengatur kekerasan berbasis gambar digital dengan ketentuan pidana yang ketat dan mekanisme ganti rugi yang jelas untuk korban. Mengoptimalkan penegakan hukum memerlukan peningkatan kemampuan aparat melalui pelatihan forensik digital khusus dan kolaborasi internasional. Implementasi harus didukung oleh infrastruktur teknologi seperti sistem verifikasi konten otomatis dan database terpusat yang dimaksudkan untuk mencegah penyebaran konten ilegal. Kecepatan respons, tingkat keberhasilan penghapusan konten, dan kepuasan korban harus menjadi komponen evaluasi sistem yang dilakukan secara berkala. Perlindungan privasi, kebebasan berekspresi, dan tanggung jawab platform digital untuk menciptakan ekosistem online yang aman dan beretika harus diimbangi. Dasolen ini menekankan pendekatan hukum yang responsif terhadap kemajuan teknologi sambil mempertahankan hak dasar individu di dunia digital. Peraturan yang ideal harus dapat mengantisipasi penyalahgunaan teknologi baru sekaligus melindungi korban secara menyeluruh, mulai dari pencegahan, penindakan, hingga pemulihan pasca kejadian.

Indonesia dan Inggris berbeda secara hukum dan teknologi dalam menangani penyebaran gambar pribadi tanpa izin. Sementara Indonesia masih bergantung pada Pasal 27 ayat (1) UU ITE secara umum, Inggris telah meluncurkan *Criminal Justice and Courts Act 2015* yang secara khusus mengkriminalisasi pornografi pemulihan dengan ancaman hukuman dua tahun penjara. Inggris juga memperkuat perlindungan dengan *Data Protection Act 2018* mereka, yang mengadopsi GDPR Uni Eropa. Di sisi lain, RUU Perlindungan Data Pribadi Indonesia baru saja dibahas. Sejak 2015, Inggris telah mengembangkan sistem penanganan yang lebih maju untuk pelacakan pornografi, dengan layanan terpadu berbasis teknologi yang terhubung langsung dengan polisi dan didukung kecerdasan buatan untuk pelacakan konten. Sementara itu, Indonesia masih bergantung pada metode manual untuk menangani kasus karena tidak ada sistem pelaporan nasional yang terintegrasi. Teknologi, Inggris meminta platform digital menggunakan *PhotoDNA* untuk mendeteksi dan memblokir konten jelas, serta mengembangkan database yang cocok dengan hashing untuk mencegah unggahan ulang. Teknologi ini belum diwajibkan secara hukum di Indonesia dan sangat terbatas. Di Inggris, perlindungan korban lebih luas dan mencakup kerahasiaan identitas, layanan hukum gratis, dan akses ke terapi psikologis. Sebaliknya, perlindungan korban sangat sedikit di Indonesia dan bergantung pada upaya lembaga swadaya masyarakat. Selain itu, pendidikan di Indonesia masih terorganisir dan tidak sistematis. Sebaliknya, Inggris telah memasukkan literasi digital, termasuk bahaya pornografi pemulihan, ke dalam kurikulum sekolah melalui kampanye "*Don't Share It*".



Perkembangan terbaru menunjukkan peningkatan pemanfaatan teknologi informasi untuk mencegah penyebaran foto pribadi tanpa izin. Indonesia meluncurkan Sistem Pelaporan dan Penghapusan Konten Ilegal berbasis AI yang terintegrasi dengan platform digital utama pada awal 2024, meniru sistem *hash matching* yang sukses di Inggris. Badan Siber dan Sandi Negara telah mengembangkan *teknik deep learning* untuk mendeteksi konten yang dimanipulasi (*deepfake*) dengan tingkat akurasi yang sangat tinggi. Pada November 2023, koalisi perusahaan teknologi besar di seluruh dunia (Meta, Google, dan TikTok) sepakat untuk menerapkan standar pertukaran hashing terkunci untuk mencegah penyebaran hashing di antara platform. Dalam hal undang-undang, DPR Republik sedang mempertimbangkan revisi UU ITE. Revisi ini akan menetapkan prinsip tanggung jawab ketat bagi penyedia platform dan memperkenalkan hukuman pidana dengan ancaman penjara yang cukup lama. Terobosan penting lainnya adalah peluncuran aplikasi Sobat Privasi oleh KemenPPPA, yang menawarkan kemampuan pelaporan anonim dan pendampingan psikologis yang tersedia sepanjang waktu, serta kerja sama Kominfo dengan Interpol dalam pelatihan digital *forensics* intensif yang telah melibatkan ratusan penegak hukum di berbagai wilayah. Adaptasi terhadap penyebaran konten melalui metaverse dan platform Web3 adalah tantangan terbaru, yang membutuhkan pendekatan baru untuk peraturan internasional. Melalui penerapan materi perlindungan data dalam kurikulum sekolah, pembelajaran di Inggris menunjukkan bahwa kombinasi antara sanksi tegas berupa denda dalam jumlah besar, dukungan teknologi modern, dan pendidikan komprehensif sangat efektif.

Perlindungan martabat manusia di era digital sangat penting ketika orang berbicara tentang peran teknologi informasi dalam menangani penyebaran foto pribadi tanpa izin. Menurut kasus-kasus terbaru, penyalahgunaan konten intim telah berkembang menjadi epidemi digital yang mengancam privasi dan keamanan psikologis individu. Masalah ini sangat penting karena tiga aspek penting. Pertama, itu adalah masalah gender yang berdampak sistemik pada kelompok rentan. Kedua, itu adalah masalah keamanan siber nasional karena eksploitasi digital yang semakin canggih. Terakhir, itu adalah ujian untuk tata kelola teknologi yang adil. Dari perspektif sosial, trauma kolektif dan budaya ketakutan dalam berinteraksi di ruang digital telah disebabkan oleh penyebaran gambar pribadi tanpa persetujuan. Pada tingkat hukum, pelaku menggunakan kelonggaran hukum untuk menghindari pertanggungjawaban. Namun, dari perspektif teknologi, pengembangan alat *deepfake* dan penyebaran konten melalui dark web telah melampaui kapasitas penanganan standar. Dengan munculnya berbagai platform berbasis *blockchain* dan *metaverse*, ancaman ini semakin kompleks dan menciptakan lorong-lorong baru untuk penyebaran konten ilegal. Dengan mengetahui bahwa setiap detik penundaan meningkatkan dampak kerusakan terhadap korban, urgensi penanganan terpadu menjadi



semakin jelas. Dalam situasi ini, teknologi informasi bukan hanya alat bantu; itu adalah batas pertahanan baru yang menentukan kemampuan kita untuk membangun ekosistem digital yang menghormati hak dasar manusia. Masyarakat digital kita akan terus terjebak dalam paradoks kemajuan teknologi yang mengancam hak-hak fundamental warganya jika tidak ada tindakan sistematis yang mengintegrasikan elemen hukum, teknologi, dan budaya.

## 2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif untuk menganalisis sejauh mana peraturan perundang-undangan, seperti UU ITE Pasal 27 ayat (1), RUU Perlindungan Data Pribadi, dan KUHP, mampu menjamin perlindungan hak-hak korban dalam kasus penyebaran konten intim tanpa persetujuan (*revenge porn*). Pendekatan ini, menurut Soerjono Soekanto dan Johnny Ibrahim, melibatkan analisis terhadap norma hukum tertulis dan asas hukum secara sistematis dan logis guna menilai efektivitas jaminan hak atas privasi, penghapusan konten (*right to be forgotten*), pendampingan hukum dan psikologis, serta perlindungan identitas korban. *Cyber Civil Rights Initiative* (CCRI) dijadikan sebagai acuan normatif penting karena menekankan *revenge porn* sebagai bentuk kekerasan berbasis gender yang membutuhkan perlindungan hukum khusus, sebagaimana tertuang dalam *Cyber Civil Rights Act* di Amerika Serikat. Dengan merujuk prinsip-prinsip CCRI, penelitian ini menilai perlunya reformasi hukum nasional yang tidak hanya berorientasi pada pemidanaan pelaku, tetapi juga pada pemulihan dan perlindungan menyeluruh bagi korban, sehingga pendekatan yuridis normatif dapat mendorong hukum yang lebih responsif terhadap tantangan kekerasan digital.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Peran TI dalam Mencegah dan Menangani Penyebaran Gambar Pribadi

Dalam hal pencegahan, deteksi, dan penanganan pasca kejadian, teknologi informasi memainkan peran yang beragam dalam mengatasi masalah penyebaran gambar pribadi tanpa izin. Sistem autentikasi biometrik dan *enkripsi end-to-end* telah berkembang menjadi solusi teknis penting untuk pencegahan. Teknologi enkripsi khusus yang digunakan oleh aplikasi penyimpanan cloud kontemporer seperti *Google Photos* dan *iCloud* memastikan bahwa hanya orang yang memiliki perangkat tersebut yang dapat mengakses konten sensitif (Zhao et al., 2023). Selain itu, pengembangan fitur "*Private Vault*" untuk berbagai platform smartphone memungkinkan penguncian gambar dengan autentikasi dua faktor, yang mengurangi kemungkinan akses tidak sah dari pihak ketiga.



Teknologi pembelajaran mesin telah mencapai tingkat kecanggihan yang signifikan dalam hal deteksi dini. Sistem seperti Microsoft's *PhotoDNA* tidak hanya dapat mengidentifikasi konten dengan menggunakan nilai hash, tetapi juga dapat mengidentifikasi perubahan pada gambar melalui analisis meta data dan pemahaman pola (Microsoft Security Blog, 2023). *Algoritma deep learning*, seperti Convolutional Neural Network (CNN), baru-baru ini telah diubah untuk mengenali deepfake dengan akurasi 98,7% melalui analisis artefak digital pada tingkat piksel (Nguyen et al., 2024). Sekarang, sistem ini secara real time digunakan oleh platform media sosial utama untuk memindai setiap unggahan konten.

Dalam hal penanganan kasus, teknologi blockchain telah muncul sebagai solusi inovatif untuk mencegah penyebaran konten ilegal. Untuk melacak penyebaran gambar dari sumber awal, sistem pengelolaan distribusi memungkinkan pembuatan jejak audit yang tidak dapat diubah, juga dikenal sebagai jejak audit yang tidak dapat diubah (Zhang & Wang, 2023). StopNCII.org, yang didirikan oleh UK *Revenge Porn Helpline*, menggunakan teknologi ini dan mekanisme *hashing* konten untuk memungkinkan korban untuk melacak dan meminta penghapusan konten secara bersamaan di berbagai platform.

Regulasi harus menyesuaikan diri dengan pertumbuhan teknologi ini. Pasal 40 GDPR telah menjadi referensi global untuk perusahaan teknologi karena mewajibkan penerapan "*privacy by design*" dalam pengembangan sistem mereka (European Data Protection Board, 2023). Di Indonesia, UU PDP mulai menerapkan prinsip ini dengan mewajibkan pengendali data untuk menerapkan teknologi pengamanan yang cukup, meskipun pedoman teknis lebih rinci diperlukan untuk melakukannya (Kominfo, 2023).

### 3.2. Regulasi Hukum Mengatur Perlindungan

Penyebaran gambar pribadi tanpa persetujuan, termasuk dalam bentuk pornografi balas dendam dan *deepfake*, merupakan pelanggaran besar terhadap hak privasi individu di internet dan telah menjadi masalah hukum yang mendesak di seluruh dunia. Fenomena ini lebih sering terjadi pada perempuan dan menyebabkan trauma psikologis dan eksklusi sosial yang lama. Di Indonesia, sejumlah undang-undang, termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (TPKS), dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, telah dibuat untuk menangani masalah ini. Meskipun regulasi-regulasi tersebut mengindikasikan kemajuan normatif, secara substantif masih terdapat celah dalam hal integrasi, harmonisasi, dan efektivitas perlindungan terhadap korban.



Pasal 27 ayat (1) UU ITE mengatur penyebaran konten yang melanggar kesusilaan dalam ruang elektronik. Namun demikian, ketentuan tersebut terlalu umum dan tidak secara eksplisit mendefinisikan penyebaran konten intim nonkonsensual sebagai kejahatan tertentu. Dengan menetapkan pornografi pembalasan sebagai salah satu jenis kekerasan seksual berbasis elektronik, UU TPKS telah membuat kemajuan besar. Oleh karena itu, perlindungan terhadap korban masih terbatas dalam pelaksanaannya, terutama dalam hal pemulihan menyeluruh seperti hak untuk dilupakan (hak untuk dilupakan) dan pemulihan psikososial. Sebaliknya, UU PDP, yang dimaksudkan untuk memperkuat perlindungan data pribadi, masih dalam tahap pengembangan dan belum memiliki otoritas pengawas yang independen. Akibatnya, ada keraguan tentang keefektifan pelaksanaannya.

Tantangan utama di tingkat praktik terletak pada kurangnya kemampuan penegakan hukum. Dalam banyak kasus, penegak hukum tidak memiliki kemampuan teknis yang diperlukan untuk mendeteksi, menelusuri, dan membuktikan penyebaran gambar pribadi secara ilegal. Ini terutama berlaku ketika pelaku menggunakan teknologi deepfake yang canggih. Kasus serupa mungkin tidak diproses secara optimal karena keterbatasan infrastruktur digital forensik di berbagai wilayah dan kurangnya pelatihan aparat. Selain itu, faktor budaya yang terus-menerus menyalahkan korban hanya memperburuk keadaan karena banyak korban enggan melapor karena pandangan negatif dan rasa malu yang kuat.

Dibutuhkan pendekatan hukum yang lebih komprehensif dan progresif untuk menyelesaikan kompleksitas masalah tersebut. Pertama, pornografi pemulihan harus dikodifikasi secara eksplisit dalam hukum nasional sebagai tindak pidana khusus, dengan ancaman pidana yang proporsional dan perlindungan maksimal untuk korban. Kedua, peraturan perundang-undangan yang berlaku harus jelas mengatur hak korban untuk meminta penghapusan permanen konten ilegal dari platform tersebut. Ketiga, penyedia platform digital harus diwajibkan untuk membangun sistem kecerdasan buatan untuk mendeteksi dan moderasi konten ilegal, serta bertanggung jawab secara hukum atas kelalaian mereka untuk mencegah peredaran konten tersebut.

Metode yang digunakan Inggris dan negara-negara anggota UE harus menjadi perhatian dalam hal perbandingan internasional. Negara-negara tersebut telah menetapkan standar tinggi untuk perlindungan privasi dan penanganan pelanggaran data dengan menerapkan Regulasi Perlindungan Data Umum. GDPR tidak hanya memberi orang hak untuk mengendalikan data pribadi mereka, tetapi juga menetapkan sanksi administratif yang berat bagi mereka yang melanggar atau dengan sengaja menyebarkan data pribadi. Selain itu, GDPR mewajibkan penyedia layanan digital untuk berpartisipasi secara aktif dalam menjaga keamanan data



melalui evaluasi dampak perlindungan data, audit berkala, dan transparansi tentang pengelolaan data. Agar mampu membangun sistem perlindungan yang adil, efisien, dan responsif terhadap kekerasan digital yang terus berkembang, Indonesia harus segera mempercepat harmonisasi dan konsolidasi kebijakan hukumnya dalam bidang ini.

### 3.3. Kelemahan Sistem TI dan Hukum yang Ada

Keterbatasan teknologi deteksi otomatis merupakan masalah utama sistem teknologi informasi di Indonesia dalam mencegah dan menangani penyebaran gambar pribadi tanpa izin. Sebagian besar platform digital masih bergantung pada *hash matching* seperti *PhotoDNA* dan algoritma berbasis AI untuk memindai konten bermasalah; namun, gambar yang dipotong, diubah, atau bahkan dibuat secara sintetis (*deepfake*) dengan teknologi ini mudah dimanipulasi. Selain itu, *hash matching* rentan terhadap kebocoran data, seperti yang ditunjukkan oleh penelitian yang menunjukkan bahwa *PhotoDNA* dapat dipulihkan dalam bentuk thumbnail ketika digabungkan dengan teknik neural networks. Sebaliknya, penelitian akademik tentang kecerdasan buatan dan forensi gambar menekankan bahwa metode deteksi manipulasi konten seperti *splice* atau serangan musuh masih memiliki kelemahan besar. Di negara maju seperti Eropa dan AS, regulasi seperti *AI Act* (EU) mengharuskan transparansi proses moderasi, audit manusia, serta *traceability*, yang belum tersedia di sistem moderasi Indonesia.

Selain itu, sistem pelaporan dan respons yang buruk masih ada di platform digital. Banyak korban yang mengadukan secara manual, tetapi tidak dilayani, sehingga foto tersebar sebelum diambil. Karena memerlukan waktu yang lama untuk bergantung pada server luar negeri dan prosedur lintas yurisdiksi, metode *takedown* dan "*stay down*" belum bekerja dengan baik. Akibatnya, fungsi sistem TI hanyalah reaktif.

Dari segi undang-undang, Indonesia telah meluncurkan UU No. 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS), UU ITE, dan UU Perlindungan Data Pribadi (UU PDP). Namun, undang-undang tersebut hanya sedikit dan belum memberikan perlindungan yang lengkap. Meskipun UU TPKS memasukkan pornografi pemulihan sebagai bentuk kekerasan seksual elektronik, prosedur pemulihan korban masih terbatas pada restitusi dan konseling, tanpa adanya kewajiban hukum untuk menghapus konten yang tersebar luas. Karena belum ada pasal penghubung atau artikel penghubung yang mengintegrasikan pendekatan antara UU ITE dan UU TPKS, pengaturan dalam UU ITE bahkan dapat menjerat korban sebagai pelanggar norma kesusilaan. Hal ini menimbulkan ketidakpastian hukum di tingkat nasional. UU PDP juga belum mampu memberikan perlindungan yang benar-benar independen karena otoritas pengawasan data pribadi nasional masih berada di bawah Kementerian Komunikasi dan Informatika, dan



belum sebanding dengan *General Data Protection Regulation* (GDPR) di Eropa, yang mengatur adanya lembaga pengawas yang independen serta sanksi administratif yang sangat tegas, bahkan dapat mencapai sebagian besar dari total pendapatan perusahaan secara global.

Dalam pelaksanaannya, penegak hukum lapangan masih kekurangan kemampuan forensik digital dan kesadaran terhadap kekerasan berbasis gender digital. Studi empiris menunjukkan bahwa banyak penegak hukum salah menilai motif hubungan antara pelaku dan korban mereka menyamaratakan laporan serangan dalam konteks hubungan pasangan dan menganggapnya setuju. Karena kurangnya laboratorium digital forensik dan kurangnya pelatihan terkait teknologi *deepfake*, proses penuntutan menjadi lebih sulit.

Dibandingkan dengan negara lain, Australia memiliki perbedaan yang signifikan. Negara itu memiliki undang-undang khusus tentang *revenge porn*, portal pengaduan pusat yang dioperasikan oleh *eSafety Commissioner*, dan prosedur penegakan hukum yang cepat dan terintegrasi dengan platform digital. Di Eropa, GDPR, UU Kecerdasan Buatan, dan UU Layanan Digital (DSA) bekerja sama untuk membuat sistem hukum dan teknis yang memungkinkan platform untuk secara proaktif dan transparan menghapus konten ilegal. Ketika sistem moderasi platform diaudit secara independen, denda yang signifikan memastikan kepatuhan yang nyata. Meskipun demikian, undang-undang negara bagian yang berbeda di Amerika Serikat, termasuk *California Consumer Privacy Act* (CCPA), memberikan dasar hukum dan teknologi tambahan, seperti *watermarking* dan kecerdasan buatan.

Secara umum, sistem hukum dan teknologi Indonesia belum bekerja sama dengan baik. Belum ada protokol audit terhadap sistem moderasi berbasis kecerdasan buatan yang menjamin transparansi dan akuntabilitas, serta mekanisme *fast track takedown* atau kolaborasi formal antara Kominfo, aparat kepolisian, dan platform asing. Namun, di negara-negara maju, jenis kerja sama ini telah diatur dalam kerangka hukum dan teknis yang komprehensif. Hal ini menunjukkan beberapa masalah sistem TI Indonesia, termasuk keterbatasan teknologi deteksi, respons moderasi konten yang lamban, dan pengguna yang tidak memahami privasi dan langkah pencegahan. Dalam hal hukum, undang-undang masih belum lengkap, lembaga pengawasan belum sepenuhnya independen, sanksi terhadap pelanggaran relatif ringan, dan aparat penegak hukum belum memiliki cukup kemampuan forensik. Perbandingan dengan negara lain mengindikasikan bahwa efektivitas pencegahan dan penanganan penyebaran gambar pribadi tanpa izin sangat bergantung pada adanya regulasi yang *holistik* dan independen, dukungan teknologi pendeteksi canggih, serta sinergi lintas lembaga yang kuat.



## KESIMPULAN

Proses yang dilakukan oleh teknologi informasi (TI) dan undang-undang hukum untuk mencegah dan menangani penyebaran gambar pribadi tanpa izin, seperti porn revenge dan *deepfake*, Solusi teknologi seperti sistem deteksi otomatis, blockchain, dan AI telah berkembang, tetapi mereka masih kekurangan kecepatan dan akurasi. Dari segi hukum, Indonesia memiliki beberapa undang-undang seperti UU ITE, UU TPKS, dan UU PDP, tetapi penerapan mereka kurang menyeluruh dan lengkap dibandingkan dengan peraturan internasional seperti GDPR di Eropa. Ketidaksiapan penegak hukum, kurangnya prosedur pemulihan korban, dan kurangnya kerja sama lintas lembaga adalah kelemahan utama. Studi perbandingan dengan negara seperti Inggris dan Australia menunjukkan pentingnya regulasi khusus, dukungan teknologi terbaru, dan sinergi yang kuat antara pemerintah, platform digital, dan masyarakat. Untuk itu, Indonesia perlu mempercepat harmonisasi hukum, meningkatkan kapasitas forensik digital, dan memperkuat kerja sama internasional guna menciptakan perlindungan yang lebih efektif dan berkeadilan bagi korban.

## DAFTAR PUSTAKA

- Aurelita, M., & Lewoleba, K. K. (2025). Perempuan sebagai Korban Deepfake Pornografi dalam Perspektif Viktimologi. *Kertha Semaya: Journal Ilmu Hukum*, 12(12), 3382-3396.
- Azizah, S. N., & Marpaung, Z. A. (2024). Criminal Offenses of Misuse of Deepfake Porn Technology Based on Indonesia's Positive Law. Universitas Islam Negeri Sumatera Utara. Menemukan bahwa UU Pornografi, UU ITE, dan UU PDP masih kurang tegas dalam mengatur deepfake porn
- Chairani, M. A., Yitawati, K., & Pradhana, A. P. (2024). Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake. *Jurnal Rechtsens*. Membahas perlunya pengeluaran regulasi khusus AI guna melindungi korban dari ancaman rekayasa gambar dan video non-konsensual
- Harahap, N. M. (2024). Resiko Kejahatan Teknologi Informasi Dan Komunikasi Cyber Crime Dan Analisa Inovasi Pencegahan Resiko Cyber Crime Di Indonesia. *Jurnal Teknologi dan Manajemen Sistem Industri*, 3(1), 52-59.
- Izzuddin, A., & Harahap, D. F. M. (2024). Positive Laws in Facing Revenge Porn, Are They Effective? *JUSTICES: Journal of Law*, 3(4), 266-275.
- Legal Protection for Revenge Porn Victims in the Sexual Violence Crime Law (UU No. 12 of 2022). (2024). *JUSTICES: Journal of Law*, 3(2), 121-133.



- Mania, K. (2024). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. *Trauma, Violence & Abuse*, 25(1), 117-129.
- Nasution, A. V. A., Suteki, & Lumbanraja, A. D. (2024). Prospek Pemenuhan Right to Be Forgotten bagi Korban Deepfake Pornography akibat Penyalahgunaan Artificial Intelligence di Indonesia. *Diponegoro Law Journal*. Penelitian ini menyoroti praktik “right to be forgotten” dan hambatan hukum dalam penanganan konten deepfake di Indonesia
- Ni'mah, S. A. (2023, July). Pengaruh cyberbullying pada kesehatan mental remaja. In *Prosiding Seminar Sastra Budaya dan Bahasa (SEBAYA)* (Vol. 3, pp. 329-338).
- Ni'mah, S. A. (2023, July). Pengaruh cyberbullying pada kesehatan mental remaja. In *Prosiding Seminar Sastra Budaya dan Bahasa (SEBAYA)* (Vol. 3, pp. 329-338).
- PROSPEK PEMENUHAN RIGHT TO BE FORGOTTEN BAGI KORBAN DEEPPAKE PORNOGRAPHY AKIBAT PENYALAHGUNAAN AI DI INDONESIA. (2024). *Diponegoro Law Journal*.
- Respati, A. A., Setyarini, A. D., Parlagutan, D., Rafli, M., Mahendra, R. S., & Nugroho, A. A. (2024). Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban. *Media Hukum Indonesia (MHI)*, 2(2).
- Santhi, N. N. P. P., & Nuarti, I. N. (2023). Penguatan Penegakan Hukum Polri dalam Rangka Optimalisasi Penanggulangan Cybercrime di Indonesia. *SCIENTIA: Journal of Multi Disciplinary Science*, 2(1), 15-27.
- Untangling the Tangle of Revenge Porn in the United States: A Comparative Study. (2024). *Indonesian Comparative Law Review*.
- Yudha, M., Purwanda, S., Amir, A., et al. (2025). Perlindungan Hukum Bagi Korban Penggunaan Deepfake dalam Kejahatan Pornografi. *Indonesian Journal of Sharia and Law*. Menjelaskan keterkaitan UU ITE, UU Pornografi, UU PDP, dan UU TPKS terhadap kasus deepfake porn.