

Perlindungan Hukum terhadap Korban Kejahatan Siber di Indonesia: Tantangan dan Prospek Penegakan Hukum

Legal Protection for Cybercrime Victims in Indonesia: Challenges and Prospects of Law Enforcement

Henny Saida Flora ^{a*}, Maidin Gultom ^b

^{a,b} Ilmu Hukum, Fakultas Hukum, Universitas Katolik Santo Thomas, Medan, Indonesia

*Email korespondensi: hennysaida@yahoo.com

ABSTRAK

Peningkatan tindak pidana siber di Indonesia belum diimbangi perlindungan hukum yang efektif bagi korban. Penelitian ini menganalisis arsitektur normatif perlindungan korban kejahatan siber, mengidentifikasi hambatan penegakannya, dan merumuskan model penguatan. Metode yang digunakan adalah penelitian hukum normatif dengan dimensi yuridis empiris melalui pendekatan perundang-undangan, konseptual, kasus, dan perbandingan. Bahan hukum primer meliputi Undang-Undang Informasi dan Transaksi Elektronik beserta dua perubahannya, Undang-Undang Perlindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana 2023, Kitab Undang-Undang Hukum Acara Pidana 2025, serta rezim perlindungan saksi dan korban. Hasil penelitian menunjukkan arsitektur normatif tampak lengkap tetapi terputus pada rantai pemulihan: undang-undang siber berwatak pengendalian konten dan pemidanaan pelaku, hak subjek data sukar ditagih karena otoritas pengawas belum berdiri, sedangkan restitusi digantungkan pada pemidanaan pelaku. Hambatan tersebar pada tiga lapisan sistem hukum, yaitu substansi yang kabur dan berkekosongan, struktur yang terbatas kapasitas forensik dan koordinasinya, serta budaya hukum yang ditandai pelaporan rendah dan praktik menyalahkan korban. Penelitian ini menawarkan model perlindungan hukum terintegrasi yang bertumpu pada empat pilar aktor dan tiga fase perlindungan, dengan kebaruan berupa penempatan penyedia layanan digital dan keuangan sebagai pemikul kewajiban kehati-hatian yang dapat dituntut pengguna.

Kata Kunci: Perlindungan Korban Kejahatan Siber, Hukum Siber Indonesia, Pemulihan Hak Korban, Restitusi Dan Kompensasi, Model Perlindungan Terintegrasi.

ABSTRACT

The rise of cybercrime in Indonesia has not been matched by effective legal protection for victims. This study analyses the normative architecture of victim protection, identifies barriers to its enforcement, and formulates a strengthening model. It applies normative legal research with an empirical juridical dimension, using statutory, conceptual, case, and comparative approaches. Primary legal materials comprise the Electronic Information and Transactions Law and its two amendments, the Personal Data Protection Law, the 2023 Criminal Code, the 2025 Criminal Procedure Code, and the witness and victim protection regime. The findings show that the normative architecture appears complete yet breaks along the recovery chain: cyber legislation is oriented towards content control and offender punishment, data subject rights remain hard to enforce because the supervisory authority has not been established, and restitution is made contingent upon the offender's conviction. Barriers are distributed across three layers of the legal system, namely vague and incomplete substance, structures constrained by forensic capacity and weak coordination, and a legal culture marked by low reporting and victim blaming. The study proposes an integrated legal protection model resting on four actor pillars and three protection phases, its novelty lying in positioning digital and financial service providers as bearers of a duty of care enforceable by users.

Keywords: Cybercrime Victim Protection, Indonesian Cyber Law, Victim Rights Restoration, Restitution And Compensation, Integrated Protection Model.

Histori Jurnal: Artikel Masuk: 8 Agustus 2026 | Diterima: 20 September 2026 | Diterbitkan: 20 Oktober 2026

Format Sitasi:

Flora, H. S., & Gultom, M. (2026). Perlindungan Hukum terhadap Korban Kejahatan Siber di Indonesia: Tantangan dan Prospek Penegakan Hukum. *Iuris Notitia: Jurnal Ilmu Hukum*, 4(2), 201–224. DOI: <https://doi.org/10.69916/iuris.v4i2.632>

1. PENDAHULUAN

Ruang digital Indonesia tumbuh jauh lebih cepat daripada perangkat hukum yang seharusnya menjaganya. Setiap penambahan pengguna internet, layanan keuangan digital, dan platform niaga membuka permukaan serangan baru sekaligus memperbanyak orang yang bisa dirugikan. Kejahatan siber pun tidak lagi berupa insiden teknis yang sesekali muncul, ia telah bermetamorfosis menjadi pola kriminalitas dominan abad ini, sebagaimana pencurian konvensional mendominasi abad sebelumnya (Hawdon, 2021). Pandemi global telah mempercepat pergeseran tersebut: aktivitas kerja, belajar, dan transaksi berpindah ke jaringan, dan bersamanya berpindah pula peluang eksploitasi (Monteith et al., 2021). Namun, yang sering luput dari perbincangan kebijakan adalah sisi korban. Penipuan daring, pencurian identitas, peretasan akun, pemerasan seksual berbasis citra, hingga penyalahgunaan data pribadi meninggalkan luka yang bertumpuk. Studi berskala nasional di Belanda menunjukkan bahwa dampak kejahatan siber terhadap kesejahteraan emosional korban setara, dan pada beberapa dimensi bahkan melampaui, dampak kejahatan konvensional yang setara jenisnya (Borwell et al., 2024). Korban kejahatan properti siber melaporkan stres peritraumatik yang lebih tinggi, sementara korban kejahatan seksual siber mengalami kerusakan citra diri yang lebih dalam. Wawancara mendalam terhadap korban di negara yang sama menemukan pola yang mereka sebut sebagai pukulan ganda, tiga, bahkan empat lapis: kerugian finansial, tekanan psikologis, keterlihatan publik atas kekorbanan, dan viktimisasi yang tidak berhenti pada satu titik waktu (Notté et al., 2021). Korban peretasan menggambarkannya sebagai pelanggaran atas ruang digital pribadi, bukan sekadar kehilangan akses (Palassis et al., 2021). Dampak ini tidak berhenti pada guncangan sesaat. Tinjauan lintas disiplin memperlihatkan bahwa penipuan merusak kesejahteraan korban dalam rentang panjang: mulai dari kecemasan, rasa malu, hilangnya kepercayaan diri dalam urusan keuangan, hingga keretakan relasi sosial (Kassem, 2023). Pada kelompok lanjut usia, kerugian material bertaut erat dengan tekanan emosional, dan lamanya data disalahgunakan menjadi prediktor kuat distres (DeLiema et al., 2021). Demikian pula korban pemerasan seksual finansial yang melaporkan kecemasan bertahan berbulan-bulan setelah insiden (O'Malley, 2023). Tinjauan cakupan atas sekstorsi menemukan prevalensi 0,7–5,0 persen pada remaja dan 4,0–18,7 persen pada orang dewasa, dengan tingkat pelaporan yang sangat rendah akibat rasa malu, ketakutan, dan persepsi negatif terhadap polisi maupun platform digital (Ray & Henry, 2024). Di negara berpendapatan rendah dan menengah, kekerasan seksual berbasis teknologi juga dibentuk oleh norma patriarkal yang membuat korban perempuan menanggung stigma tambahan (Sheikh & Rogers, 2023).

Secara global, literatur kontemporer telah memetakan dinamika viktimisasi siber ke dalam tiga tema utama. Pertama, terkait pengalaman korban dan respons sistem peradilan; studi kualitatif di Ghana merekam bagaimana korban menilai sistem peradilan lamban dan tidak efektif sehingga mereka merasa tak berdaya (Mensah et al., 2023), sementara analisis komunitas daring di Tiongkok menunjukkan keragaman modus viktimisasi yang sangat mengikuti karakter medianya (Lee, 2021). Kedua, terkait perilaku pelaporan (*reporting behavior*); tinjauan kritis dua dekade riset penipuan identitas di Amerika Serikat menegaskan minimnya penelitian tentang dampak layanan bagi korban (Irvin-Erickson, 2024). Estimasi berbasis capture-recapture atas serangan ransomware di Belanda menemukan hanya sekitar 41 persen serangan terhadap perusahaan besar dan 40 persen terhadap perusahaan menengah yang dilaporkan ke polisi (Meurs et al., 2025). Survei terhadap korban muda pelecehan berbasis teknologi menemukan angka pelaporan yang jauh lebih memprihatinkan, yakni hanya 7,3 persen ke platform dan 4,8 persen ke aparat, dengan hanya 29,8 persen responden yang menilai respons polisi membantu (Colburn et al., 2023). Ketiga, terkait erosi kepercayaan publik; analisis dua dekade data viktimisasi nasional Amerika Serikat memperlihatkan penurunan pemberitahuan kejahatan kepada polisi yang disertai dengan meningkatnya ketidakpercayaan korban terhadap daya tanggap kepolisian (Xie et al., 2023). Pola serupa muncul pada penipuan kripto (Holt & Cross, 2024) dan penipuan asmara, yang pelaporannya sempat naik ketika media populer mengangkatnya lalu kembali turun (Grant & Buil-Gil, 2025). Karakteristik pelaku juga

memengaruhi keputusan ini; korban yang mengenali pelaku sebagai pasangan atau mantan pasangan justru lebih enggan mencari bantuan hukum (Mumford et al., 2022).

Dalam konteks Indonesia, kajian hukum berkembang pada jalur yang sedikit berbeda dan sangat berfokus pada kecukupan norma. Penelitian tentang perlindungan korban penyebaran data pribadi menyimpulkan bahwa kerangka yang ada masih meninggalkan celah panduan yang jelas bagi individu (Enggarsasi et al., 2024). Kajian mengenai kekerasan seksual berbasis elektronik menunjukkan bahwa peraturan yang tersedia belum sensitif korban dan lemah dalam perspektif hak asasi (Zaltina & Nurtjahyo, 2024), sementara analisis hukum feminis menyoroti bagaimana budaya patriarkal dan minimnya pemahaman aparat mengenai konsep persetujuan mendorong viktimisasi sekunder (Violin & Nafi, 2022). Studi terbaru yang menggabungkan analisis normatif dan empiris atas kekerasan seksual daring menemukan bahwa Pasal 27 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) lebih mengatur konten daripada melindungi korban, sehingga posisi prosedural korban melemah (Purnama Pratiwi et al., 2025). Pada ranah pemulihan, penelitian doktrinal atas putusan pengadilan memperlihatkan bahwa hak korban atas kompensasi dan restitusi digantungkan pada pemidanaan pelaku, sehingga banyak korban tidak pernah menerima apa pun (Ali et al., 2022). Celah lain terletak pada ketiadaan sanksi atas keterlambatan pembayaran restitusi, yang justru membuka pintu viktimisasi sekunder (Aprilianda & Fibriansyah, 2021). Kritik yang lebih struktural datang dari kajian atas evolusi perlindungan korban di Indonesia, yang membaca kerangka Undang-Undang Perlindungan Saksi dan Korban beserta lembaganya sebagai produk logika fungsionalisasi: korban diakui dalam bentuk, tetapi disubordinasikan dalam substansi karena perlingkungannya bergantung pada kegunaannya bagi proses peradilan (Pangaribuan, 2026). Pembaruan legislatif memang terus berjalan. Kitab Undang-Undang Hukum Pidana (KUHP) yang baru mengubah lanskap kejahatan siber sekaligus mengurangi tumpang tindih dengan UU ITE (Suseno et al., 2025). Namun, tinjauan sistematis lintas yurisdiksi mengingatkan bahwa keberadaan legislasi bukan jaminan; yang menentukan adalah kemutakhiran, kejelasan, dan kapasitas penegakannya (Khan et al., 2022). Kritik terhadap kebijakan penanggulangan kejahatan siber di Indonesia menunjukkan bahwa model reaktif tidak efektif, sedangkan model penegakan preventif menuntut kemampuan teknis yang belum dimiliki sebagian besar aparat (Raharjo et al., 2022). Analisis atas kesiapan hukum siber Indonesia juga menemukan sejumlah praktik daring menyimpang yang belum terdefinisi dalam literatur hukum sehingga lolos dari jangkauan norma (Manullang, 2022), sementara pendekatan tata kelola yang baik mengungkap ketegangan antara kebutuhan penegakan dan fasilitasi ekonomi digital (Marwan et al., 2022).

Meskipun literatur global dan nasional telah berkembang pesat, terdapat kesenjangan penelitian (*research gap*) yang belum terjembatani. Literatur internasional sangat kaya pada dimensi viktimologis dan perilaku pelaporan, tetapi jarang menautkannya pada arsitektur normatif satu yurisdiksi secara utuh. Sebaliknya, literatur hukum Indonesia kuat pada analisis pasal demi pasal, namun cenderung berhenti pada rekomendasi normatif tanpa membedah mengapa norma yang secara tekstual memadai tetap gagal menghasilkan pemulihan. Kajian yang ada juga umumnya bersifat sektoral: satu tulisan membahas data pribadi, tulisan lain membahas kekerasan seksual daring, dan tulisan berikutnya membahas restitusi, tanpa dirangkai menjadi satu penilaian sistemik. Lebih jauh, perspektif aparat penegak hukum (penyidik siber, penuntut, hakim, pejabat lembaga perlindungan korban) hampir tidak pernah dijadikan bahan analisis primer dalam kajian hukum Indonesia mengenai kejahatan siber. Akibatnya, hingga saat ini belum tersedia model perlindungan hukum yang menyatukan dimensi substansi, struktur, dan budaya hukum secara koheren bagi korban kejahatan siber di Indonesia.

Celah itulah yang hendak diisi oleh penelitian ini. Kebaruan (*novelty*) penelitian ini terletak pada tiga kontribusi utama. Pertama, ia membaca perlindungan korban kejahatan siber sebagai persoalan sistem hukum yang utuh, mengadopsi teori sistem hukum Lawrence Friedman, dengan menempatkan analisis pada tiga lapis: substansi, struktur, dan budaya hukum, alih-alih memandangnya sebagai kekurangan satu undang-undang. Kedua, ia mengintegrasikan lima instrumen yang selama ini dibaca terpisah, yaitu UU ITE beserta dua perubahannya, UU Perlindungan Data Pribadi, KUHP 2023, Rancangan/KUHAP 2025, serta rezim perlindungan saksi dan korban, ke dalam satu matriks perlindungan yang menunjukkan secara presisi di mana hak korban terputus. Ketiga, ia menawarkan model perlindungan hukum terintegrasi yang menempatkan penyedia layanan digital dan lembaga perlindungan korban sebagai simpul yang setara dengan aparat penegak hukum, bukan sekadar pelengkap. Berdasarkan uraian tersebut, penelitian ini diarahkan untuk menjawab tiga pertanyaan hukum utama:

1. Bagaimana arsitektur normatif perlindungan hukum terhadap korban kejahatan siber di Indonesia ter-

susun, dan sejauh mana ia menjamin hak korban atas perlindungan dan pemulihan? 2. Apa saja hambatan substantif, struktural, dan kultural yang membuat perlindungan tersebut belum bekerja sebagaimana dirancang? 3. Model perlindungan hukum seperti apa yang dapat memperkuat akses keadilan bagi korban kejahatan siber di Indonesia?

Tujuan penelitian ini adalah untuk menganalisis ketiga persoalan tersebut secara sistematis dan merumuskan kerangka penguatan yang dapat dioperasionalkan oleh pembentuk undang-undang, aparat penegak hukum, regulator sektor digital, dan lembaga perlindungan korban.

2. METODE PENELITIAN

Penelitian ini menerapkan desain penelitian hukum normatif yang diperkaya dengan dimensi yuridis-empiris (*socio-legal research*). Kombinasi metodologis ini dipilih sebagai konsekuensi logis dari rumusan masalah yang menuntut pembacaan tidak hanya terhadap teks norma (*law in books*), tetapi juga terhadap efektivitas penerapannya dalam realitas penegakan hukum (*law in action*). Pendekatan hibrida ini selaras dengan tren mutakhir kajian hukum digital, di mana konstruksi normatif harus diuji terhadap implementasi empiris untuk mengungkap ketegangan antara regulasi dan praktik di lapangan, sebagaimana diterapkan dalam kajian efektivitas perlindungan korban kekerasan seksual daring (Purnama Pratiwi et al., 2025) dan tata kelola hukum digital (Marwan et al., 2022).

Untuk membedah kompleksitas permasalahan, penelitian ini memanfaatkan empat pendekatan hukum secara berlapis dan saling melengkapi. Pendekatan perundang-undangan (*statute approach*) digunakan sebagai tulang punggung analisis untuk menelusuri hierarki, koherensi, dan sinkronisasi norma antarinstrumen, sebagaimana lazim diterapkan dalam pemetaan kejahatan siber dalam regulasi pidana terbaru (Suseno et al., 2025). Pendekatan konseptual (*conceptual approach*) dikerahkan untuk membedah konstruksi doktrinal mengenai perlindungan hukum, hak korban, dan mekanisme pemulihan. Selanjutnya, pendekatan kasus (*case approach*) diterapkan untuk menelaah bagaimana norma diterjemahkan dalam praktik peradilan, menguji jarak antara teks hukum dan hasil putusan, khususnya terkait kompensasi dan restitusi (Ali et al., 2022, Laia et al., 2025). Terakhir, pendekatan perbandingan (*comparative approach*) digunakan secara terbatas namun strategis untuk menerangkan pilihan kelembagaan dan praktik terbaik, mengacu pada studi pembentukan otoritas pengawas data pribadi di yurisdiksi lain (Aisy et al., 2025, Triyanti et al., 2025).

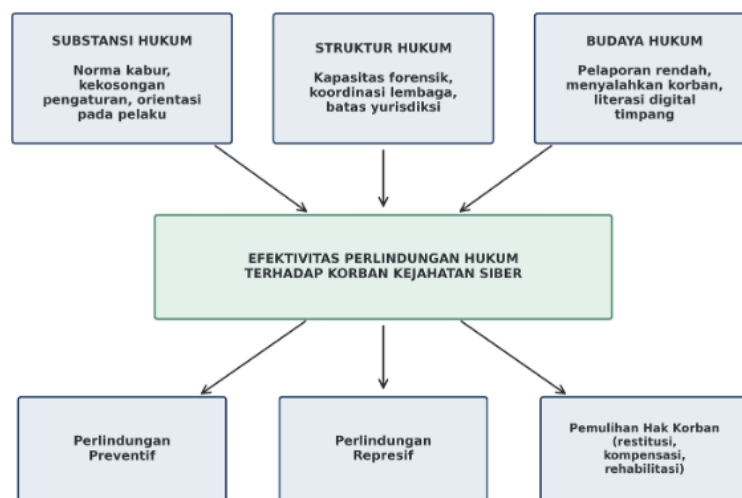
Bahan hukum yang dikumpulkan diklasifikasikan secara ketat menjadi tiga tingkatan untuk menjamin validitas argumen. Bahan hukum primer mencakup instrumen normatif inti, yaitu Undang-Undang Informasi dan Transaksi Elektronik beserta dua perubahannya, Undang-Undang Perlindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana 2023, Kitab Undang-Undang Hukum Acara Pidana 2025, rezim Perlindungan Saksi dan Korban, Undang-Undang Tindak Pidana Kekerasan Seksual, serta Convention on Cybercrime (Council of Europe, 2001) sebagai rujukan komparatif. Bahan hukum sekunder terdiri atas artikel jurnal ilmiah bereputasi yang terindeks pada pangkalan data internasional, dengan prioritas pada literatur yang terbit dalam lima tahun terakhir untuk menjamin kemutakhiran argumen. Bahan hukum tersier meliputi kamus hukum dan indeks istilah teknis forensik digital untuk memastikan ketepatan definisi operasional.

Penelusuran bahan hukum sekunder dilakukan melalui protokol yang terstruktur dan sistematis, menghindari penelusuran yang bersifat oportunistik. Kata kunci disusun dalam dua bahasa (Indonesia dan Inggris) untuk menjangkau kajian berkonteks Indonesia yang dipublikasikan dalam jurnal internasional, sebuah kebutuhan yang tercermin dari pemetaan bibliometrik riset kejahatan siber lintas batas (Zhao & Cheng, 2024). Proses penyaringan literatur mengikuti logika penapisan bertingkat ala tinjauan sistematis (*systematic review*): identifikasi awal, penyaringan relevansi berdasarkan abstrak, dan penilaian kelayakan penuh (*full-text assessment*) berdasarkan kesesuaian dengan klaim teoritis yang hendak dibangun (Khan et al., 2022, Sahak et al., 2025). Setiap rujukan yang lolos diverifikasi Digital Object Identifier (DOI)-nya untuk menjamin keaslian dan ketelusuran sumber.

Dimensi empiris dalam penelitian ini dirancang melalui sintesis kualitatif terhadap bukti-bukti empiris sekunder yang telah dipublikasikan, sebagai fondasi untuk membangun model teoretis yang kokoh. Artikel ini menyajikan konstruksi model yang diuji validitasnya terhadap temuan lapangan dari yurisdiksi komparatif yang relevan, seperti studi profesional penegak hukum di Belanda (Bekkers et al., 2025) dan analisis kapasitas penyidikan di Asia Tenggara (Sun et al., 2025). Strategi ini menjaga integritas epistemologis penelitian: setiap

klaim mengenai hambatan struktural atau budaya hukum ditopang oleh data empiris yang valid dari sumber yang kredibel, sementara proposisi model perlindungan yang ditawarkan berfungsi sebagai kerangka kerja yang siap diuji (*testable framework*) dalam agenda penelitian lapangan berikutnya.

Analisis data dilakukan secara kualitatif melalui interpretasi hukum yang mencakup interpretasi gramatikal untuk menetapkan makna tekstual, interpretasi sistematis untuk menguji koherensi antarinstrumen, dan interpretasi teleologis untuk menilai apakah penerapan norma masih melayani tujuan utama perlindungan korban. Hasil interpretasi tersebut kemudian dipetakan menggunakan kerangka teori sistem hukum Lawrence Friedman, yang membedakan analisis ke dalam tiga lapis: substansi, struktur, dan budaya hukum. Pemilahan ini memungkinkan identifikasi kegagalan perlindungan secara presisi pada lapisan yang tepat, alih-alih menyamaratkannya sebagai "lemahnya penegakan hukum". Teori perlindungan hukum, teori viktimologi, dan teori keadilan digunakan sebagai lensa analitis untuk memosisikan korban sebagai subjek pemegang hak dan mengevaluasi distribusi beban dalam mekanisme pemulihan. Penarikan kesimpulan dilakukan secara deduktif dari premis normatif menuju penilaian praktik, yang diakhiri dengan penalaran preskriptif berupa rumusan model perlindungan terintegrasi, sebagaimana divisualisasikan dalam kerangka analisis pada Gambar 1.



Gambar 1. Kerangka analisis tiga lapis sistem hukum terhadap perlindungan korban kejahatan siber. Sumber: hasil olahan penulis (2026)

3. HASIL DAN PEMBAHASAN

3.1. Arsitektur Normatif Perlindungan Korban Kejahatan Siber: Kelengkapan Tekstual dan Kesenjangan Operasional

Secara kuantitatif, kerangka regulasi Indonesia tampak memadai. Negara telah memiliki undang-undang khusus informasi elektronik yang telah mengalami dua kali perubahan, undang-undang perlindungan data pribadi, kitab hukum pidana baru, kitab hukum acara pidana baru, rezim perlindungan saksi dan korban beserta peraturan pelaksana, serta undang-undang tindak pidana kekerasan seksual. Namun, kelengkapan tekstual ini tidak serta-merta menjamin efektivitas perlindungan. Ketika dibaca dari perspektif korban—yang menghadapi kebocoran data, kerugian finansial, atau penyebaran citra tanpa persetujuan—pertanyaan mendasar yang muncul bukanlah "apakah norma tersedia?", melainkan "instrumen mana yang memberikan hak, dan kepada siapa hak tersebut dapat ditagih?". Kesenjangan antara kelengkapan normatif dan operasionalisasi inilah yang menjadi titik krusial analisis.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dirancang pada era ketika kekhawatiran utama legislator adalah keabsahan transaksi elektronik dan penyalahgunaan konten (Republik Indonesia, 2008). Orientasi ini dipertahankan secara konsisten melalui Undang-Undang Nomor 19 Tahun 2016 (Republik Indonesia, 2016) dan Undang-Undang Nomor 1 Tahun 2024 (Republik Indonesia, 2024). Analisis terhadap Pasal 27A dan 27B hasil perubahan kedua mengonfirmasi bahwa perumusan yang multitafsir justru melahirkan ketidakpastian hukum dan membatasi kebebasan berekspresi (Feka et al., 2025). Lebih jauh,

usulan dekriminalisasi pencemaran nama baik daring menilai bahwa pendekatan legislasi yang bersifat tambal sulam gagal menyelaraskan diri dengan praktik terbaik hak asasi manusia (Manitra et al., 2026). Rangkaian putusan Mahkamah Konstitusi atas delik reputasi juga menegaskan bahwa perdebatan hukum bertahun-tahun lebih berpusat pada kepastian hukum bagi terdakwa daripada pada pemulihan korban (Jaelani & Luthviati, 2021). Implikasinya jelas: undang-undang ini sejak awal berfungsi sebagai instrumen pengendalian konten dan pemidanaan pelaku, di mana korban diposisikan sebagai pelapor, bukan sebagai pemegang hak atas pemulihan. Temuan bahwa Pasal 27 ayat (1) lebih mengutamakan pengaturan konten daripada perlindungan korban memperkuat interpretasi ini (Purnama Pratiwi et al., 2025).

Berbeda dengan UU ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memperkenalkan pergeseran doktrinal yang signifikan dengan menempatkan subjek data sebagai pemegang hak, bukan sekadar objek pengaturan (Republik Indonesia, 2022b). Perbandingan dengan Personal Information Protection Act Korea Selatan menunjukkan kesamaan arsitektur hak dan larangan pemrosesan tanpa persetujuan eksplisit, meskipun terdapat perbedaan pada desain kelembagaannya (Shahrullah et al., 2024). Justru pada dimensi kelembagaan inilah kelemahan utama Indonesia terletak. Undang-undang mendelegasikan pembentukan lembaga pengawas kepada peraturan presiden, dan selama otoritas independen belum terbentuk, penegakan sanksi administratif tetap tidak berjalan meskipun kebocoran data terus berulang (Aisy et al., 2025). Studi mengenai model pengawasan berbasis prinsip akuntabilitas sampai pada kesimpulan yang sejalan: tanpa pengawas tunggal yang bertanggung jawab langsung kepada Presiden, perlindungan data dijalankan secara sektoral oleh masing-masing instansi dan kehilangan efektivitasnya (Yuspin et al., 2024). Kajian atas sektor publik menambahkan catatan kritis bahwa undang-undang memberikan ruang pengecualian yang terlalu longgar bagi institusi pemerintah untuk mengesampingkan hak subjek data (Rahman, 2025), sementara ketidaksinkronan dengan undang-undang administrasi kependudukan membiarkan aspek pengumpulan, pertukaran, dan pencegahan penyalahgunaan data tanpa pengaturan eksplisit (Triyanti et al., 2025). Pada sektor perbankan digital, ketidakcocokan antara regulasi otoritas jasa keuangan dan kebutuhan tata kelola data menghasilkan tafsir ganda serta celah tanggung jawab (Yuspin et al., 2023).

Kesenjangan antara pengakuan hak dan mekanisme penagihannya ini memiliki konsekuensi praktis yang nyata. Ketika data pribadi bocor, korban di Indonesia berhadapan dengan kerangka hukum yang mengakui haknya, namun belum menyediakan saluran operasional untuk menagihnya. Studi kasus kebocoran data pada sebuah marketplace besar menunjukkan bahwa dampak paling nyata adalah krisis kepercayaan konsumen, sementara mekanisme ganti rugi individual nyaris tidak tersentuh (Wibowo et al., 2024). Perbandingan lintas negara mengingatkan bahwa Indonesia pada periode sebelumnya tidak memiliki komisi perlindungan data maupun pengaturan sanksi pidana dan gugatan perdata atas pelanggaran data (Sudarwanto & Kharisma, 2021). Sebagian pekerjaan rumah tersebut kini telah terjawab secara normatif, namun implementasinya masih tertunda. Padahal, kepercayaan konsumen terbukti berkorelasi erat dengan keseriusan negara dalam menegakkan aturan keamanan data (Prastyanti & Sharma, 2024), dan integrasi teknologi peningkat privasi dengan standar regulasi yang ketat merupakan prasyarat perlindungan yang efektif dalam lingkungan niaga elektronik (Morić et al., 2024). Di ranah transaksi digital, hambatan bersifat berlapis: regulasi yang terfragmentasi, klausul baku yang tidak dapat dinegosiasikan, serta lembaga penyelesaian sengketa konsumen yang berkapasitas terbatas (Ariawan, 2025, Panjaitan et al., 2025).

Sementara itu, rezim perlindungan saksi dan korban menyediakan jalur pemulihan yang paling eksplisit, namun cakupannya terbatas. Undang-Undang Nomor 31 Tahun 2014 memberikan hak atas kompensasi dan restitusi untuk kategori tindak pidana tertentu (Republik Indonesia, 2014), yang tata caranya diatur lebih lanjut melalui Peraturan Pemerintah Nomor 7 Tahun 2018 (Republik Indonesia, 2018). Perbandingan dengan Malaysia dan Australia menunjukkan bahwa Indonesia sebenarnya tergolong progresif dalam memberikan hak khusus kepada enam kategori subjek yang dilindungi (Arsawati et al., 2024). Kendala utama terletak pada tahap eksekusi. Restitusi digantungkan pada penghukuman pelaku, dan pelaku kerap memilih menjalani pidana pengganti daripada membayar (Ali et al., 2022). Tidak adanya sanksi atas keterlambatan pembayaran menempatkan korban dalam ketidakpastian yang berkepanjangan, yang oleh para peneliti dikategorikan sebagai bentuk viktimisasi sekunder (Aprilianda & Fibriansyah, 2021). Bahkan pada tindak pidana kekerasan seksual, yang rezim pemulihannya paling maju berkat Undang-Undang Nomor 12 Tahun 2022 (Republik Indonesia, 2022a), kompensasi secara formal diposisikan sebagai substitusi restitusi, sehingga kehilangan makna sebagai tanggung jawab negara yang mandiri (Purwadi et al., 2024). Hambatan prosedural, minimnya pendampingan

hukum, dan lemahnya koordinasi antarlembaga semakin mempersempit akses korban terhadap restitusi (Indah & Dwiyatmi, 2024). Analisis struktural atas sejarah kelembagaan perlindungan korban menempatkan seluruh persoalan ini dalam satu penjelasan koheren: perlindungan dirancang mengikuti kegunaan korban bagi proses peradilan, sehingga berhenti sebagai pengakuan simbolik belaka (Pangaribuan, 2026).

Dua instrumen terbaru mengubah lanskap normatif dan patut dianalisis secara cermat. Kitab Undang-Undang Hukum Pidana yang disahkan melalui Undang-Undang Nomor 1 Tahun 2023 (Republik Indonesia, 2023) mencabut sejumlah ketentuan lama dan menata ulang delik pencemaran, penghinaan, pelanggaran privasi, ancaman, serta kesusilaan, sekaligus mengurangi tumpang tindih dengan Undang-Undang Informasi dan Transaksi Elektronik (Suseno et al., 2025). Sementara itu, Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, yang berlaku sejak 2 Januari 2026 (Republik Indonesia, 2025), secara eksplisit menempatkan penguatan hak korban sebagai salah satu materi muatan pokoknya dan mengakui alat bukti elektronik secara tegas. Ini merupakan pergeseran paradigmatis: untuk pertama kalinya dalam sejarah hukum acara pidana Indonesia, korban diposisikan sebagai subjek yang haknya diperkuat, bukan sekadar saksi pelapor. Namun, pengakuan normatif ini belum diimbangi oleh panduan teknis yang memadai, sehingga efektivitasnya dalam praktik masih harus diuji. Pemetaan komprehensif atas kelima instrumen tersebut terhadap empat fungsi perlindungan yang secara doktrinal harus tersedia bagi korban disajikan pada Tabel 1.

Tabel 1. Pemetaan instrumen hukum Indonesia terhadap empat fungsi perlindungan korban kejahatan siber

Instrumen Hukum	Pencegahan	Penindakan	Partisipasi Korban	Korban	Pemulihan
UU No. 11/2008 jo. UU No. 19/2016 jo. UU No. 1/2024 (ITE)	Terbatas; bertumpu pada pemblokiran konten	Kuat; sanksi pidana berat	Lemah; korban berkedudukan sebagai pelapor		Tidak diatur
UU No. 27/2022 (Perlindungan Data Pribadi)	Kuat; kewajiban pengendalian dan pemrosesan data	Sedang; sanksi administratif dan pidana	Sedang; hak subjek data diakui		Lemah; mekanisme ganti rugi belum operasional
UU No. 1/2023 (KUHP)	Sedang; perluasan delik berbasis teknologi	Kuat; delik siber ditata ulang	Lemah		Terbatas; restitusi sebagai pidana tambahan
UU No. 20/2025 (KUHP)	Tidak relevan	Kuat; bukti elektronik diakui tegas	Kuat; korban dinyatakan sebagai materi muatan pokok		Sedang; peraturan pelaksana belum terbit
UU No. 31/2014 jo. PP No. 7/2018 (Perlindungan Saksi dan Korban)	Tidak relevan	Sedang; melalui perlindungan saksi	Kuat; pendampingan dan perlindungan prosedural		Sedang; bersyarat peminanaan pelaku
UU No. 12/2022 (Tindak Pidana Kekerasan Seksual)	Sedang	Kuat	Kuat; layanan terpadu bagi korban		Sedang; kompensasi diposisikan sebagai substitusi restitusi

Sumber: disusun penulis dari analisis bahan hukum primer dan (Ali et al., 2022, Pangaribuan, 2026, Purwadi et al., 2024, Suseno et al., 2025)

Pemetaan pada Tabel 1 memperlihatkan pola yang konsisten. Fungsi pencegahan dan penindakan terlayani relatif baik oleh hampir semua instrumen. Fungsi partisipasi korban dalam proses mulai terlayani sejak berlakunya hukum acara pidana baru. Fungsi pemulihan, sebaliknya, hanya terlayani sebagian dan selalu bersyarat. Inilah lubang yang dimaksud: bukan ketiadaan norma, melainkan terputusnya rantai antara pengakuan hak dan mekanisme penagihannya. Kritik terhadap fondasi hukum transformasi digital Indonesia menyebut kondisi ini sebagai kerangka yang terfragmentasi dan reaktif, dengan koordinasi kelembagaan yang lemah (Anggono et al., 2025).

3.2. Hambatan Struktural: Defisit Kapasitas Forensik, Fragmentasi Kelembagaan, dan Hambatan Yurisdiksi

Efektivitas norma hukum pada akhirnya bergantung pada kapasitas aparat dalam menerjemahkannya menjadi pembuktian yang sah di pengadilan. Pada dimensi inilah hambatan struktural perlindungan korban kejahatan siber di Indonesia paling tampak nyata. Penelitian mengenai pemanfaatan forensik digital dalam pembuktian pemalsuan dokumen elektronik mencatat, berdasarkan data asosiasi profesi tahun 2023, bahwa Indonesia hanya memiliki 147 ahli forensik digital bersertifikat yang tersebar di seluruh wilayah nasional (Setiawan & Hartiwiningsih, 2025). Angka ini harus dibaca secara kontekstual terhadap luas wilayah, jumlah penduduk, dan volume laporan yang masuk setiap tahunnya. Bahkan dengan asumsi kapasitas kerja optimal, rasio antara jumlah ahli dan beban perkara menunjukkan ketimpangan yang signifikan. Implikasinya dapat diprediksi: antrean pemeriksaan yang panjang, prioritas penanganan yang jatuh pada perkara bernilai ekonomi besar, serta penumpukan laporan korban perorangan yang tidak terproses.

Keterbatasan kapasitas ini beririsan langsung dengan persoalan standarisasi. Barang bukti digital memiliki karakteristik volatil dan rentan dipertanyakan keasliannya. Kerangka validasi keandalan forensik digital menunjukkan bahwa dokumentasi rantai penguasaan barang bukti (*chain of custody*) harus dibakukan pada tiga level—teknologi, metode, dan penerapan—agar hakim maupun penasihat hukum dapat menguji laporan forensik secara terformalisasi (Stoykova & Franke, 2023). Studi eksperimental atas perangkat forensik bersumber terbuka (*open-source*) memperlihatkan bahwa perangkat gratis pun dapat menghasilkan bukti yang layak diterima pengadilan, sepanjang divalidasi melalui kerangka yang memenuhi standar Daubert (Ismail & Akram Zainol Ariffin, 2025). Temuan ini memiliki relevansi khusus bagi yurisdiksi dengan keterbatasan anggaran. Survei terhadap penuntut umum dan penyidik di Amerika Serikat menegaskan bahwa faktor penentu keberhasilan pembuktian digital bukanlah semata-mata ketersediaan perangkat, melainkan pelatihan yang memadai, spesialisasi penuntut dalam menangani bukti digital, serta hubungan kerja yang erat antara penyidik dan penuntut (Miller, 2023). Tinjauan sistematis di bidang forensik digital menyimpulkan bahwa hambatan terbesar justru terletak pada tahap akuisisi dan prapemrosesan bukti, yang diperparah oleh persoalan kesiapan, pelaporan, dan etika (Casino et al., 2022a). Perkembangan teknologi semakin memperumit keadaan: transformasi digital mengubah karakter kejahatan pada kecepatan yang melampaui kemampuan laboratorium forensik untuk mengejarinya (Klasén et al., 2024).

Dalam konteks Indonesia, permasalahan ini memasuki fase krusial. Hukum acara pidana yang berlaku sejak awal 2026 telah mengakui bukti elektronik secara eksplisit, namun pengakuan normatif tersebut belum diimbangi oleh prosedur autentikasi yang baku, mekanisme rantai penguasaan barang bukti yang rinci, maupun kualifikasi ahli forensik digital yang terstandar. Kekosongan regulasi turunan ini berpotensi melahirkan disparitas penilaian hakim antarpengadilan. Kondisi ini paralel dengan kritik yang telah lama ditujukan terhadap ketertinggalan pengaturan peradilan elektronik, yang selama bertahun-tahun bersandar pada instrumen di luar produk legislatif (Saputra et al., 2023). Tanpa peraturan pelaksana yang diterbitkan secara cepat, pengakuan normatif atas bukti elektronik berisiko berhenti sebagai kemajuan tekstual belaka. Kekosongan prosedural serupa telah lama membayangi kewenangan penyadapan, yang tersebar di berbagai undang-undang sektoral tanpa mekanisme dan prosedur baku, sehingga menempatkan Indonesia pada posisi rendah dalam indeks perlindungan hak privasi (Natamiharja et al., 2022). Ketidakjelasan prosedural semacam ini menghasilkan dampak ganda: melemahkan daya pembuktian sekaligus membuka ruang pelanggaran hak, dan keduanya sama-sama merugikan kepentingan korban.

Lapisan hambatan struktural kedua berkaitan dengan koordinasi kelembagaan. Analisis politik keamanan siber Indonesia menunjukkan bahwa lembaga-lembaga yang seharusnya menjadi simpul utama penanganan kejahatan siber menghadapi tumpang tindih mandat, ketidakpastian regulasi, serta ego sektoral, sementara undang-undang keamanan dan ketahanan siber secara khusus belum disahkan (Aji, 2025). Kajian mengenai tata kelola kontraterorisme siber sampai pada diagnosis serupa: berbagai institusi dengan kepentingan pertahanan dan keamanan yang beririsan dituntut untuk berkolaborasi, namun belum terdapat arsitektur kelembagaan yang mengikat mereka secara formal (Masyhar & Emovwodo, 2023). Urgensi pengaturan kecerdasan buatan dalam kaitannya dengan ketahanan siber menambah panjang daftar kebutuhan yang belum terpenuhi: koordinasi kelembagaan yang dijamin undang-undang, standar keamanan infrastruktur digital, kewajiban pelaporan insiden, serta peningkatan kapasitas sumber daya manusia (Ramli et al., 2026). Perbandingan regional memperlihatkan bahwa negara-negara Asia Tenggara secara umum masih berkutat pada pembangunan kapasitas

dasar, dan hal ini merupakan salah satu penyebab sindikat penipuan siber berpindah ke kawasan ini setelah penegakan hukum diperketat di yurisdiksi lain (Sun et al., 2025). Pemetaan bibliometrik atas riset keamanan siber ASEAN menunjukkan pertumbuhan publikasi yang pesat, namun belum terkonsolidasi menjadi kerangka kebijakan regional yang koheren (Ali et al., 2025).

Lapisan hambatan struktural ketiga adalah persoalan yurisdiksi. Kejahatan siber secara inheren melintasi batas negara sejak detik pertama insiden terjadi, sementara kewenangan penyidik nasional berhenti di garis perbatasan. Kajian sistematis mengenai penyidikan lintas batas dan bukti digital memperlihatkan bahwa heterogenitas kerangka hukum menciptakan hambatan waktu yang bukan sekadar memperlambat proses, melainkan kerap membuat pertukaran bukti menjadi mustahil (Casino et al., 2022b). Protokol Kedua Konvensi Budapest (Council of Europe, 2001) dirancang secara spesifik untuk menembus kebuntuan tersebut dan diyakini dapat memperkuat perlindungan korban lintas negara (Spiezia, 2022). Indonesia belum menjadi pihak pada konvensi ini, sehingga harus bersandar pada perjanjian bantuan hukum timbal balik (*mutual legal assistance*) bilateral yang prosedurnya panjang dan birokratis. Kerja sama regional memang berkembang: ASEAN telah menjalankan operasi bersama yang menyasar kejahatan siber, namun ketimpangan kapasitas antarnegara anggota membatasi efektivitas hasilnya (Sundram, 2024). Sementara itu, ekonomi penipuan daring di Asia Tenggara telah bermetamorfosis menjadi industri berskala besar yang beroperasi dalam kompleks tertutup dengan pekerja yang ditahan secara paksa (Franceschini et al., 2023), dengan modus phishing, investasi fiktif, dan pencurian identitas yang dikendalikan sindikat lintas negara (Luong & Ngo, 2024). Analisis terhadap sepuluh kasus penyidikan menunjukkan pembagian kerja yang konsisten antara komponen penipuan dan komponen pencucian uang, disertai elemen lokal yang sering luput dari perhatian penyidik (Lusthaus et al., 2023). Wawancara terhadap tiga puluh satu profesional di Belanda mengungkap bahwa tingkat penyelesaian perkara tetap rendah karena penyidikan tersendat pada lapisan kurir uang (*money mules*) dan tidak menjangkau lapisan atas jaringan (Bekkers et al., 2025).

Di luar tiga lapisan hambatan tersebut, terdapat pula ketegangan konseptual yang jarang mendapat perhatian memadai. Uni Eropa telah bergeser ke pendekatan administratif preventif untuk melindungi infrastruktur kritis, sementara lapisan pidana tetap dipertahankan; keduanya kini berjalan beriringan dengan gesekan yang belum sepenuhnya terselesaikan (Bartoli, 2025). Kecerdasan buatan memperlebar jurang ini karena instrumen internasional yang ada dirancang sebelum teknologi tersebut matang (Velasco, 2022). Bagi Indonesia, implikasi kebijakan dari dinamika ini cukup jelas: memilih satu jalur saja, pidana semata atau administratif semata, tidak akan memadai. Model reaktif terbukti tidak efektif, sedangkan model preventif menuntut kemampuan deteksi dan pelumpuhan yang belum dimiliki sebagian besar aparat. Dalam konteks ini, model kolaboratif yang melibatkan korporasi, perguruan tinggi, dan masyarakat sipil menjadi sintesis yang paling masuk akal (Raharjo et al., 2022).

3.3. Hambatan Substantif: Kekaburan Normatif, Kekosongan Regulasi, dan Ketidaksesuaian Orientasi Kebijakan

Hambatan substantif dalam perlindungan korban kejahatan siber di Indonesia beroperasi dalam tiga bentuk yang masing-masing menuntut respons kebijakan berbeda: kekaburan normatif, kekosongan regulasi, dan ketidaksesuaian orientasi kebijakan. Pemilahan ini penting karena ketiga bentuk hambatan tersebut memiliki akar masalah dan implikasi yang berbeda, sehingga tidak dapat ditangani melalui intervensi yang seragam. Analisis terhadap ketiga dimensi ini mengungkapkan bahwa kelemahan substantif tidak hanya terletak pada ketiadaan norma, melainkan juga pada kualitas norma yang ada.

Kekaburan normatif paling tampak pada rumusan delik yang bertumpu pada penilaian subjektif. Analisis terhadap Pasal 27A dan 27B Undang-Undang Nomor 1 Tahun 2024 menunjukkan bahwa definisi yang tidak jelas melahirkan efek gentar (*chilling effect*) pada jurnalis dan pengkritik pemerintah, sekaligus gagal memberikan perlindungan tambahan bagi korban sesungguhnya (Feka et al., 2025). Ketidakjelasan serupa muncul dalam perkara perjudian daring, ketika ketentuan yang ambigu menghasilkan ketidakpastian hukum dan penegakannya terhambat oleh keterbatasan pemahaman teknologi di kalangan aparat (Laia et al., 2025). Lebih jauh, praktik siber menyimpang yang belum terdefinisi dalam literatur hukum kerap lolos dari jangkauan norma dan diperlakukan sebagai perbuatan yang sah secara hukum (Manullang, 2022). Bagi korban, konsekuensi kekaburan ini bersifat langsung dan merugikan: laporan mereka berpotensi ditolak pada tahap penyelidikan karena perbuatan yang dialami tidak dapat dicocokkan dengan rumusan pasal mana pun secara meyakinkan.

Bentuk hambatan kedua adalah kekosongan regulasi, yang muncul ketika perkembangan teknologi bergerak lebih cepat daripada kapasitas legislasi untuk mengimbangnya. Perlindungan korban pornografi balas dendam (*revenge porn*) dan konten sintetis hasil rekayasa mendalam (*deepfake*) masih beragam bahkan di Uni Eropa: dari sembilan negara anggota yang dibandingkan, hanya tiga yang memiliki kriminalisasi khusus, dengan cakupan definisi yang berbeda-beda sehingga jalur penuntutan hak korban turut bervariasi (Mania, 2022). Indonesia belum memiliki ketentuan khusus mengenai konten sintetis, sehingga penanganannya bergantung pada penafsiran pasal-pasal umum yang tidak dirancang untuk konteks teknologi mutakhir. Persoalan ini akan semakin membesar seiring meluasnya pemanfaatan kecerdasan buatan dalam kejahatan siber, dan kebutuhan akan kerangka hukum berbasis risiko yang bersifat antisipatif telah diidentifikasi sebagai agenda mendesak (Ramli et al., 2026). Tinjauan sistematis lintas yurisdiksi mengingatkan bahwa legislasi kejahatan siber harus diperbarui secara berkala mengikuti kecepatan perkembangan teknologi bila hendak tetap relevan (Khan et al., 2022).

Kekosongan yang lebih fundamental terletak pada pengaturan tanggung jawab penyedia layanan digital. Perdebatan global telah bergeser dari model kekebalan perantara (*safe harbor*) menuju model kewajiban kehati-hatian (*duty of care*). Argumen yang berpengaruh menyatakan bahwa platform bukan sekadar penampung konten pasif, melainkan pembentuk ruang sosial melalui arsitektur dan algoritmanya, sehingga bahaya yang lahir dari ruang tersebut merupakan konsekuensi langsung dari cara ruang itu dikelola (Price, 2021). Kerangka regulasi Eropa bergerak ke arah kewajiban penilaian risiko dan transparansi, meskipun ketegangan dengan perlindungan kebebasan berekspresi belum sepenuhnya terselesaikan (Frosio & Geiger, 2023). Perbandingan lintas benua atas model tanggung jawab perantara menunjukkan kecenderungan penambahan beban pemantauan dan penghapusan konten, dengan risiko sensor berlebih apabila keseimbangan tidak terjaga (Machado & Aguiar, 2023). Tinjauan sistematis terbaru menegaskan bahwa inkonsistensi kerangka hukum antaryurisdiksi merupakan hambatan utama bagi akuntabilitas perantara (Sahak et al., 2025). Dalam konteks Indonesia, kewajiban penyelenggara sistem elektronik sebagian besar dibingkai sebagai kepatuhan administratif terhadap pemerintah, bukan sebagai kewajiban perdata terhadap pengguna yang dirugikan. Akibatnya, korban penipuan yang dananya mengalir melalui rekening penampung, atau korban penyebaran citra intim yang kontennya berulang kali diunggah kembali, tidak memiliki dasar gugatan yang jelas terhadap platform maupun penyedia jasa keuangan.

Bentuk hambatan ketiga adalah ketidaksesuaian orientasi kebijakan, yaitu situasi ketika norma tersedia namun diarahkan pada tujuan yang tidak sejalan dengan kepentingan pemulihan korban. Undang-Undang Informasi dan Transaksi Elektronik menyediakan sanksi pidana berat sekaligus mekanisme pemblokiran konten, namun tidak menyediakan mekanisme pemulihan kerugian bagi korban. Pemetaan atas penerapan keadilan restoratif dalam tindak pidana informasi dan transaksi elektronik menyimpulkan bahwa berbagai kebijakan yang ditempuh pemerintah lebih didorong oleh kebutuhan mengurangi kelebihan kapasitas lembaga pemasyarakatan daripada oleh tujuan memulihkan hak korban (Triasari et al., 2023). Pada kasus kekerasan seksual berbasis elektronik, ketergantungan pada bukti dokumen elektronik yang dipadukan dengan praktik menyalahkan korban (*victim blaming*) justru mempersempit ruang bagi korban untuk menuntut restitusi (Purnama Pratiwi et al., 2025). Kebutuhan mendesak akan aturan turunan yang berorientasi pada korban, termasuk mekanisme penghapusan cepat konten seksual eksplisit, telah lama diidentifikasi namun belum terjawab secara memadai (Zaltina & Nurtjahyo, 2024). Sementara itu, perlindungan data yang efektif dalam lingkungan niaga elektronik menuntut sinergi antara elemen hukum, teknologi, dan prosedur, bukan mengandalkan salah satunya secara parsial (Morić et al., 2024).

Ketiga bentuk hambatan substantif ini saling memperkuat dan menghasilkan efek kumulatif yang merugikan korban. Kekaburan normatif membuat laporan korban sulit diproses, kekosongan regulasi membiarkan bentuk-bentuk viktimisasi baru tanpa payung hukum yang memadai, dan ketidaksesuaian orientasi kebijakan mengalihkan fokus penegakan hukum dari pemulihan korban menuju tujuan lain yang tidak selalu sejalan. Pemahaman terhadap ketiga dimensi ini menjadi prasyarat bagi perumusan rekomendasi kebijakan yang tepat sasaran, sebagaimana akan diuraikan pada bagian pembahasan selanjutnya mengenai hambatan budaya hukum.

3.4. Hambatan Budaya Hukum: Defisit Pelaporan, Viktimisasi Sekunder, dan Asimetri Literasi Digital

Dimensi budaya hukum sering kali menjadi lapisan analisis yang terabaikan dalam kajian hukum konvensional karena tidak termanifestasi dalam bentuk pasal atau kelembagaan yang konkret. Namun, pada lapisan inilah banyak kasus kejahatan siber berhenti sebelum sempat memasuki ranah peradilan. Fenomena *underreporting* atau rendahnya angka pelaporan kejahatan siber terdokumentasi secara konsisten di hampir semua yurisdiksi yang diukur secara metodologis. Estimasi berbasis metode capture-recapture atas serangan ransomware di Belanda menemukan bahwa hanya sekitar 40 persen serangan terhadap perusahaan besar dan menengah yang dilaporkan ke kepolisian, sebuah angka yang justru dinilai lebih tinggi dibandingkan jenis kejahatan siber lainnya (Meurs et al., 2025). Pada tingkat individu, kondisinya jauh lebih mengkhawatirkan: survei representatif nasional terhadap dewasa muda mengungkapkan bahwa hanya 7,3 persen episode pelecehan berbasis teknologi yang dilaporkan ke platform, dan hanya 4,8 persen yang dilaporkan ke aparat penegak hukum, dengan hanya 29,8 persen responden yang menilai respons kepolisian membantu (Colburn et al., 2023). Analisis data pelaporan penipuan di Britania Raya lebih lanjut menunjukkan bahwa pelaporan yang tidak lengkap secara langsung menggerus relevansi data administratif bagi perumusan kebijakan pencegahan (Giro Correia, 2022). Tinjauan kritis atas riset penipuan identitas juga menegaskan minimnya bukti empiris mengenai dampak layanan bagi korban, sebuah kekosongan yang membuat upaya perbaikan sistem berjalan tanpa pijakan yang jelas (Irvin-Erickson, 2024). Kecenderungan serupa juga teramati pada kasus penipuan aset kripto (Holt & Cross, 2024).

Rendahnya tingkat pelaporan ini didorong oleh dua faktor psikososial utama: ketidakpercayaan institusional dan ketakutan akan viktimisasi sekunder. Sebagian besar korban enggan melapor karena skeptis bahwa laporan mereka akan ditanggapi secara serius. Analisis dua dekade data viktimisasi nasional di Amerika Serikat menunjukkan tren penurunan pemberitahuan kejahatan kepada polisi yang disertai dengan meningkatnya ketidakpercayaan terhadap daya tanggap kepolisian, sebuah fenomena yang merata di berbagai kelompok ras dan sosial ekonomi (Xie et al., 2023). Faktor lainnya adalah ketakutan akan disalahkan. Eksperimen viniet terhadap 108 petugas polisi di Britania Raya menemukan bahwa keterlambatan korban dalam melapor kasus penguntitan siber (*cyberstalking*) secara signifikan meningkatkan kecenderungan petugas untuk menyalahkan korban (*victim blaming*). Menariknya, petugas yang telah mengikuti pelatihan khusus mengenai kekerasan dalam pasangan intim hampir seluruhnya mengenali perbuatan tersebut sebagai tindak pidana, whereas di antara petugas tanpa pelatihan, sebagian besar menyatakan keraguan (Chatzisymeonidis & Pina, 2024). Temuan ini krusial karena menunjukkan bahwa sikap aparat bukanlah sifat bawaan, melainkan hasil dari kurikulum pelatihan yang dapat direformasi. Pada kasus sekstorsi, rasa malu dan ketakutan menjadi penghalang utama pencarian bantuan (Ray & Henry, 2024), dan dampak psikologisnya terbukti bertahan lama setelah insiden berakhir (O'Malley, 2023). Korban muda yang pelakunya adalah pasangan atau mantan pasangan bahkan memiliki probabilitas yang lebih kecil untuk mencari bantuan hukum maupun teknis (Mumford et al., 2022).

Konteks sosiokultural memperburuk dinamika ini, khususnya di negara-negara berpendapatan rendah dan menengah. Norma patriarkal secara signifikan membentuk pengalaman korban kekerasan seksual berbasis teknologi, mendorong mereka untuk bersandar pada dukungan keluarga informal alih-alih menempuh jalur hukum formal (Sheikh & Rogers, 2023). Studi kualitatif di Ghana merekam frustrasi mendalam korban yang menilai sistem peradilan sebagai institusi yang lamban dan tidak efektif (Mensah et al., 2023). Dalam konteks Indonesia, budaya patriarkal yang berpadu dengan lemahnya pemahaman aparat mengenai konsep persetujuan (*consent*) telah diidentifikasi sebagai pendorong utama viktimisasi sekunder terhadap perempuan korban kekerasan berbasis gender daring (Violin & Nafi, 2022). Stigma sosial yang melekat pada korban masih menjadi hambatan struktural yang menghambat akses mereka terhadap upaya hukum yang memadai (Purnama Pratiwi et al., 2025).

Selain faktor budaya, literasi digital muncul sebagai variabel kompleks yang hubungannya dengan viktimisasi tidak sesederhana asumsi kampanye kesadaran konvensional. Studi lintas seksi terhadap 864 lansia di Thailand Selatan menemukan bahwa literasi digital yang memadai memang berfungsi sebagai faktor protektif, sementara usia yang lebih tua dan tempat tinggal di daerah pedesaan meningkatkan kerentanan terhadap penipuan (Pituk et al., 2025). Namun, penelitian di Belgia mengungkap sebuah paradoks kognitif: individu yang merasa dirinya sudah cukup terinformasi tentang keamanan daring justru merasa kurang rentan dan, akibatnya, kurang terdorong untuk mengambil langkah pengamanan proaktif (De Kimpe et al., 2021). Studi serupa terhadap orang dewasa di Malaysia menemukan bahwa kepercayaan diri berlebihan (*overconfidence*) dan pengaruh sosial secara

signifikan memprediksi viktimisasi penipuan daring (Balakrishnan et al., 2025). Survei terhadap mahasiswa di Palestina juga menunjukkan bahwa 52,4 persen responden pernah menjadi korban kejahatan siber atau mengenal seseorang yang mengalaminya, disertai dengan rendahnya kesadaran mengenai penyebab dan langkah pencegahan yang tepat (Ahmead et al., 2024). Implikasi kebijakan dari temuan ini sangat spesifik: program literasi digital yang hanya berfokus pada penambahan pengetahuan teknis tanpa mengoreksi kalibrasi risiko (*risk calibration*) berpotensi menghasilkan efek yang berlawanan dengan tujuannya.

Kerentanan terhadap kejahatan siber juga terdistribusi secara tidak merata, menciptakan lapisan-lapisan marginalisasi baru. Faktor personal seperti hidup sendiri, jenis kelamin perempuan, dan status sosial ekonomi rendah berkorelasi dengan dampak emosional yang lebih berat, sementara usia lanjut berkaitan erat dengan menurunnya rasa aman (Borwell et al., 2025). Peretasan perangkat dan durasi kejahatan yang berkepanjangan semakin memperbesar dampak negatif pada kedua dimensi tersebut. Kelompok dengan gangguan kesehatan mental memiliki kerentanan tersendiri dan sering kali tidak menyadari risiko yang melekat pada perilaku daring mereka (Monteith et al., 2021). Anak-anak menghadapi hambatan unik: mereka memiliki kemampuan kognitif yang lebih rendah untuk menyadari bahwa mereka sedang menjadi korban, sehingga probabilitas pelaporan kepada otoritas menjadi semakin kecil (Choi & Lee, 2023). Bahkan perempuan yang terpapar indoktrinasi berbasis ideologi keagamaan semu melalui ruang siber memiliki hak untuk diperlakukan sebagai korban, meskipun sistem hukum cenderung secara keliru menempatkan mereka sebagai pelaku (Budiono et al., 2023). Akumulasi dampak yang tidak berhenti dalam ruang dan waktu inilah yang membuat viktimisasi daring terasa sangat invasif, sekaligus menjelaskan mengapa persepsi publik terhadap korban sering kali tidak sebanding dengan beratnya beban psikologis dan material yang mereka tanggung (Notté et al., 2021).

3.5. Pemulihan Hak Korban: Ketergantungan Struktural pada Kapasitas Finansial Pelaku

Perlindungan hukum yang tidak bermuara pada pemulihan hak korban merupakan perlindungan yang bersifat semu. Pada dimensi inilah kerangka hukum Indonesia menunjukkan kerapuhan paling mendasar, dan kerapuhan tersebut bersifat struktural—bukan insidental. Persoalan fundamentalnya terletak pada asumsi yang tertanam dalam rezim restitusi: bahwa pelaku akan tertangkap, terbukti bersalah secara hukum, dan memiliki aset yang memadai untuk membayar ganti rugi. Ketiga asumsi ini jarang terpenuhi secara simultan dalam kasus kejahatan siber. Penelitian doktrinal atas perundang-undangan dan putusan pengadilan di Indonesia menunjukkan bahwa hak korban atas kompensasi dan restitusi secara sistematis digantungkan pada pemidanaan pelaku, dan pelaku kerap memilih untuk menjalani pidana pengganti yang relatif singkat daripada memenuhi kewajiban pembayaran (Ali et al., 2022). Ketiadaan sanksi yang mengatur keterlambatan pembayaran semakin memperparah situasi, sehingga korban terpapar pada ketidakpastian yang berkepanjangan (Aprilianda & Fibriansyah, 2021). Bahkan dalam rezim tindak pidana kekerasan seksual—yang secara normatif merupakan rezim paling progresif—kompensasi negara diposisikan sebagai substitusi restitusi dan kehilangan maknanya sebagai kewajiban negara yang mandiri. Apabila aset pelaku tidak mencukupi, pengadilan cenderung menjatuhkan pidana pengganti ketimbang membebaskan kompensasi kepada negara (Purwadi et al., 2024). Prosedur yang rumit, minimnya pendampingan hukum, dan lemahnya koordinasi antara aparat penegak hukum dan lembaga perlindungan korban melengkapi rangkaian hambatan struktural ini (Indah & Dwiyatmi, 2024).

Bagi korban kejahatan siber, hambatan-hambatan struktural ini terakumulasi dan berlipat ganda. Pelaku sering kali beroperasi dari yurisdiksi asing, menggunakan identitas sintetis yang sulit dilacak, dan memindahkan hasil kejahatan melalui rantai rekening penampung serta aset kripto sebelum penyidikan dapat dimulai. Apabila restitusi hanya dapat ditagih kepada pelaku yang telah divonis bersalah, maka mayoritas korban kejahatan siber secara praktis berada di luar jangkauan mekanisme pemulihan yang ada. Analisis perbandingan kelembagaan menunjukkan bahwa Indonesia sebenarnya tergolong progresif dalam memberikan hak khusus atas kompensasi dan restitusi kepada kategori subjek tertentu (Arsawati et al., 2024). Namun, kemajuan normatif ini tidak diterjemahkan menjadi mekanisme operasional yang dapat dijalankan tanpa bergantung pada nasib pelaku. Diagnosis fungsionalisasi memberikan penjelasan struktural atas fenomena ini: kerangka perlindungan korban disusun mengikuti logika kebutuhan prosedural negara, sehingga korban hanya bernilai sepanjang ia berguna bagi kelancaran proses peradilan (Pangaribuan, 2026).

Dimensi kerugian yang harus dipulihkan juga jauh lebih luas daripada yang diakui oleh hukum positif. Bukti empiris menunjukkan bahwa dampak kejahatan siber merambah kesejahteraan emosional, rasa aman, dan citra diri korban. Korban yang kerugian finansialnya tidak diganti mengalami dampak emosional yang

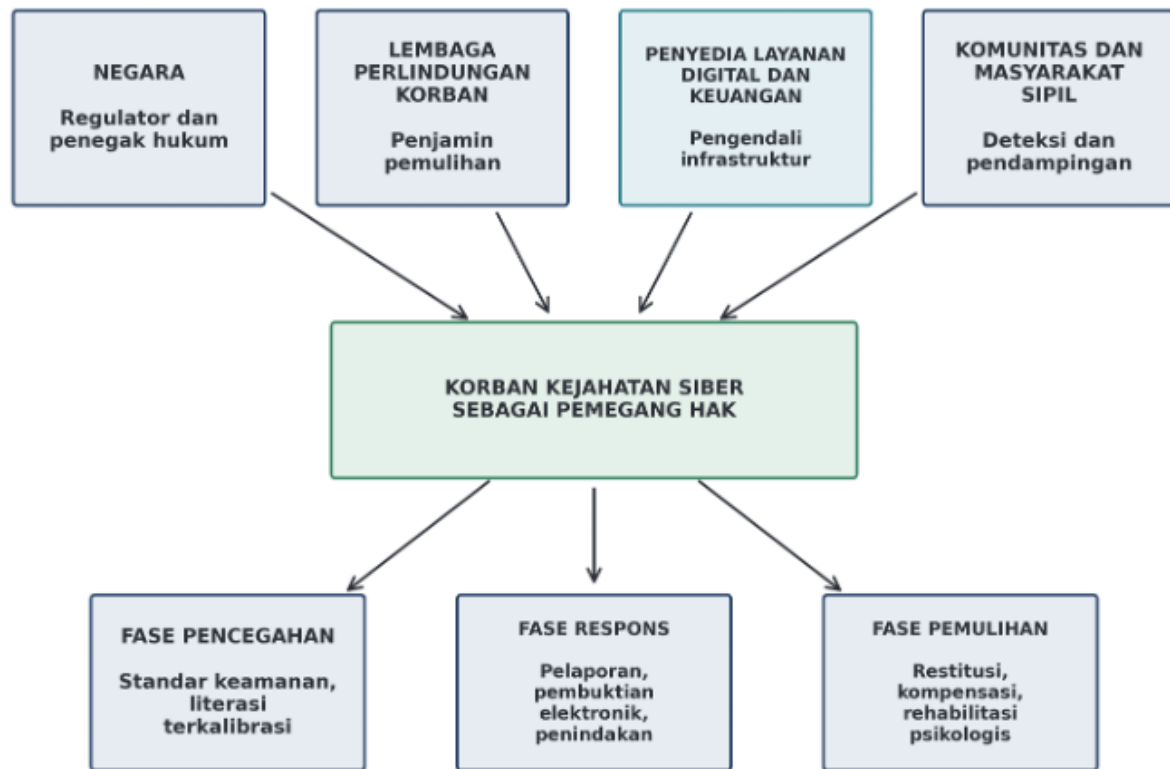
secara signifikan lebih berat dibandingkan mereka yang mendapat kompensasi (Borwell et al., 2021). Penipuan daring menimbulkan kecemasan kronis, rasa malu, hilangnya kepercayaan diri dalam urusan keuangan, hingga keretakan relasi sosial (Kassem, 2023). Pada korban lanjut usia, durasi penyalahgunaan data dan waktu yang dihabiskan untuk menyelesaikan masalah berkorelasi positif dengan tingkat tekanan emosional yang dialami (DeLiema et al., 2021). Dengan demikian, rezim restitusi yang hanya mengakui kerugian materiil secara inheren akan selalu tertinggal dari realitas kerugian multidimensi yang dialami korban.

Menghadapi keterbatasan ini, eksplorasi terhadap mekanisme alternatif menjadi keniscayaan. Praktik keadilan restoratif (*restorative justice*) menunjukkan dampak psikologis positif yang bertahan lama bagi korban yang berpartisipasi, termasuk dalam mengurangi gejala pascatrauma dan memperbaiki persepsi mereka terhadap pelaku (Nascimento et al., 2022). Gagasan panel korban-pelaku (*victim-offender panels*) diajukan secara khusus untuk konteks siber: pertemuan terstruktur antara sekelompok korban dan sekelompok pelaku terpidana memberikan ruang bagi korban untuk menyuarakan kerugian yang dialami dan bagi pelaku untuk menumbuhkan rasa penyesalan, dengan potensi menekan angka residivisme dalam kerangka *reintegrative shaming* (Robalo & Abdul Rahim, 2023). Namun, penerapan keadilan restoratif di Indonesia memiliki catatan kritis yang serius. Kajian atas praktiknya menemukan bahwa penyelesaian prosedural sering kali diutamakan di atas penyembuhan substantif korban: tidak ada asesmen psikologis wajib, keterlibatan tenaga kesehatan jiwa sangat terbatas, pemantauan pascamediasi lemah, dan faktor sosiokultural seperti praktik menyalahkan korban (*victim blaming*) serta campur tangan pihak ketiga menggerus prinsip kesukarelaan (Azisa et al., 2025). Tanpa reformasi mendasar pada aspek-aspek ini, keadilan restoratif berisiko terdegradasi menjadi jalan pintas untuk menutup perkara, bukan sebagai jalur pemulihan yang bermakna.

Dua gagasan alternatif lain layak dipertimbangkan secara serius. Pertama, memperkuat partisipasi korban dalam proses peradilan melalui instrumen pernyataan dampak korban (*victim impact statement*). Analisis normatif dan komparatif atas instrumen ini dalam sistem peradilan anak menunjukkan bahwa mekanisme yang sederhana dan berbiaya rendah ini dapat memperkaya pertimbangan hakim, meningkatkan kepuasan korban, dan memperkuat legitimasi pengadilan (Aprilianda et al., 2025). Instrumen serupa dapat diadaptasi bagi korban kejahatan siber dewasa, terutama untuk mendokumentasikan kerugian nonmateriil yang selama ini tidak terekam dalam berkas perkara. Kedua, membangun respons berlapis (*layered response*) yang tidak menyandarkan seluruh beban pemulihan pada sistem peradilan pidana. Studi multiyurisdiksi atas kekerasan seksual berbasis citra mengusulkan respons berjenjang yang dipimpin oleh organisasi keselamatan daring (*online safety organizations*) yang didanai oleh pemerintah dan industri, sehingga korban dapat merebut kembali kendali atas situasi mereka baik di dalam maupun di luar jalur pidana (Rackley et al., 2021). Pendekatan ini mengakui realitas empiris yang telah terbukti: sebagian besar korban tidak akan pernah memasuki sistem peradilan pidana, dan kebijakan yang hanya menyiapkan mekanisme pemulihan melalui jalur pidana berarti membiarkan mayoritas korban tanpa akses terhadap layanan pemulihan. Perlu pula dicatat secara kritis bahwa kebijakan yang dibingkai sebagai keadilan restoratif di ranah informasi dan transaksi elektronik selama ini lebih didorong oleh kebutuhan mengurangi kelebihan kapasitas lembaga pemasyarakatan ketimbang oleh komitmen untuk memulihkan hak korban (Triasari et al., 2023).

3.6. Model Perlindungan Hukum Terintegrasi: Empat Pilar, Tiga Fase

Dari analisis pada tiga lapisan sistem hukum di atas, penelitian ini merumuskan model perlindungan hukum terintegrasi bagi korban kejahatan siber di Indonesia. Model ini disusun di atas dua sumbu. Sumbu pertama adalah pilar aktor: negara sebagai pembentuk dan penegak norma, lembaga perlindungan korban sebagai penjamin pemulihan, penyedia layanan digital dan keuangan sebagai pengendali infrastruktur tempat kejahatan berlangsung, dan komunitas beserta masyarakat sipil sebagai simpul deteksi dini dan pendampingan. Sumbu kedua adalah fase perlindungan: pencegahan, respons, dan pemulihan. Gambar 2 memvisualkan susunan tersebut.



Gambar 2. Model perlindungan hukum terintegrasi bagi korban kejahatan siber. Sumber: hasil olahan penulis (2026)

Pilar pertama, penguatan negara, menuntut tiga langkah yang saling menopang. Pengesahan undang-undang keamanan dan ketahanan siber akan memberi dasar bagi koordinasi kelembagaan yang selama ini tersandera ego sektoral dan ketidakpastian mandat (Aji, 2025), sekaligus menetapkan standar keamanan infrastruktur digital dan kewajiban pelaporan insiden (Ramli et al., 2026). Pembentukan otoritas pengawas perlindungan data pribadi yang independen dan bertanggung jawab langsung kepada Presiden merupakan prasyarat bagi penegakan sanksi administratif yang selama ini tidak berjalan (Aisy et al., 2025, Yuspin et al., 2024). Penerbitan peraturan pelaksana hukum acara pidana yang mengatur autentikasi bukti elektronik, rantai penguasaan barang bukti, dan kualifikasi ahli forensik digital menjadi kebutuhan mendesak agar pengakuan normatif atas bukti elektronik tidak berhenti sebagai kemajuan tekstual. Kerangka validasi bertingkat yang membedakan level teknologi, metode, dan penerapan menyediakan cetak biru yang dapat langsung diadaptasi (Stoykova & Franke, 2023). Penguatan kapasitas forensik tidak harus menunggu anggaran besar, karena perangkat sumber terbuka yang divalidasi secara benar terbukti menghasilkan bukti yang layak diterima pengadilan (Ismail & Akram Zainol Ariffin, 2025) dan sertifikasi ahli dapat diperluas melalui kemitraan dengan perguruan tinggi (Setiawan & Hartiwiningsih, 2025). Reformasi pengaturan peradilan elektronik pada tingkat legislatif melengkapi agenda ini (Saputra et al., 2023).

Pilar kedua, lembaga perlindungan korban, memerlukan pergeseran mandat yang mendasar. Selama restitusi digantungkan pada pemidanaan pelaku, sebagian besar korban kejahatan siber tidak akan pernah menerima pemulihan. Model ini mengusulkan pemisahan tegas antara restitusi sebagai kewajiban pelaku dan kompensasi sebagai kewajiban negara yang berdiri sendiri, dengan pendanaan yang tidak bergantung pada kemampuan bayar pelaku. Persoalan itu telah lama diidentifikasi sebagai cacat regulasi utama (Ali et al., 2022, Purwadi et al., 2024). Sanksi atas keterlambatan pembayaran restitusi perlu dirumuskan untuk menutup celah yang selama ini melahirkan viktimisasi sekunder (Aprilianda & Fibriansyah, 2021). Perluasan cakupan tindak pidana yang memberi hak atas kompensasi hingga mencakup kejahatan siber bernilai kerugian signifikan merupakan langkah berikutnya, mengingat kerangka Indonesia sebenarnya sudah mengenal hak khusus bagi kategori subjek tertentu (Arsawati et al., 2024). Pemulihan juga harus mencakup dimensi nonmateriil melalui asesmen psikologis dan

pendampingan yang terlembaga, bukan bergantung pada inisiatif kasuistik ([Azisa et al., 2025](#)), serta membuka kanal partisipasi korban dalam persidangan melalui instrumen sejenis pernyataan dampak korban ([Aprilianda et al., 2025](#)).

Pilar ketiga, penyedia layanan digital dan keuangan, merupakan bagian yang paling belum tergarap dalam kerangka Indonesia. Model ini mengusulkan pergeseran dari kepatuhan administratif menuju kewajiban kehati-hatian yang dapat dituntut oleh pengguna yang dirugikan, mengikuti argumen bahwa platform membentuk ruang sosial melalui arsitektur dan algoritmanya sehingga bertanggung jawab atas bahaya yang lahir dari ruang tersebut ([Price, 2021](#)). Elemen konkretnya mencakup kewajiban notifikasi pelanggaran data kepada subjek data dalam tenggat tegas, mekanisme penghapusan cepat untuk konten intim nonkonsensual, kewajiban penahanan sementara dana pada rekening yang dilaporkan sebagai penampung hasil penipuan, dan transparansi berkala mengenai penanganan laporan pengguna. Perumusannya harus menjaga keseimbangan agar beban pemantauan tidak berbalik menjadi sensor berlebih ([Frosio & Geiger, 2023](#), [Machado & Aguiar, 2023](#)), dan harmonisasi lintas yurisdiksi diperlukan karena inkonsistensi kerangka merupakan hambatan utama akuntabilitas perantara ([Sahak et al., 2025](#)). Pengalaman kerangka Eropa yang memadukan lapisan administratif preventif dengan lapisan pidana menunjukkan bahwa keduanya dapat berjalan beriringan asalkan titik singgungnya dirumuskan jelas ([Bartoli, 2025](#)).

Pilar keempat, komunitas dan masyarakat sipil, berfungsi sebagai simpul deteksi dan pendampingan. Program literasi digital perlu dirancang untuk mengoreksi kalibrasi risiko, bukan sekadar menambah pengetahuan, mengingat temuan bahwa merasa terinformasi justru menurunkan kewaspadaan ([De Kimpe et al., 2021](#)) dan bahwa kepercayaan diri berlebih memprediksi viktimisasi ([Balakrishnan et al., 2025](#)). Sasarannya perlu dibedakan menurut kerentanan, dengan perhatian khusus pada kelompok lanjut usia dan wilayah dengan akses terbatas ([Pituk et al., 2025](#)). Pendampingan berbasis komunitas menutup jarak bagi korban yang tidak akan pernah menempuh jalur formal, sebagaimana diusulkan dalam respons berjenjang yang dipimpin organisasi keselamatan daring ([Rackley et al., 2021](#)), dan ruang dialog terstruktur antara korban dan pelaku dapat dipertimbangkan sebagai pelengkap, bukan pengganti, jalur pidana ([Robalo & Abdul Rahim, 2023](#)).

Model ini juga menuntut dimensi eksternal. Akses terhadap Konvensi Budapest beserta Protokol Keduanya akan memangkas hambatan waktu dalam pertukaran bukti lintas negara yang selama ini bukan sekadar memperlambat melainkan kerap membuat penyidikan mustahil ([Casino et al., 2022b](#), [Spiezia, 2022](#)). Kerja sama regional perlu diperdalam melampaui operasi bersama sesaat menuju pembangunan kapasitas yang merata, mengingat ketimpangan kemampuan antarnegara anggota membatasi hasil kolaborasi ([Sundram, 2024](#)) dan riset keamanan siber kawasan belum terkonsolidasi menjadi kerangka kebijakan bersama ([Ali et al., 2025](#)). Pendekatan regulasi responsif berlapis yang menggabungkan pembangunan kapasitas pelindung calon korban, pelumpuhan jaringan kurir uang, dan penindakan terhadap sindikat menawarkan kerangka operasional yang telah diuji secara empiris di kawasan ini ([Sun et al., 2025](#)). Tabel 2 menerjemahkan model tersebut menjadi agenda yang dapat dioperasionalkan beserta indikator keberhasilannya.

Tabel 2. Agenda operasionalisasi model perlindungan hukum terintegrasi bagi korban kejahatan siber

Pilar	Agenda Prioritas	Aktor Penanggung Jawab	Indikator Keberhasilan
Negara	Pengesahan undang-undang keamanan dan ketahanan siber serta peraturan pelaksana pembuktian elektronik	Dewan Perwakilan Rakyat, Pemerintah, Mahkamah Agung	Terbitnya undang-undang dan peraturan pelaksana; proporsi laporan yang naik ke tahap penyidikan
Negara	Pembentukan otoritas pengawas perlindungan data pribadi yang independen	Presiden	Jumlah sanksi administratif yang dijatuhkan per tahun
Lembaga Perlindungan Korban	Pemisahan kompensasi negara dari restitusi pelaku dan sanksi atas keterlambatan pembayaran	Dewan Perwakilan Rakyat, LPSK, Kementerian Keuangan	Rasio restitusi dan kompensasi yang dibayarkan terhadap yang diputuskan
Lembaga Perlindungan Korban	Asesmen psikologis dan pendampingan melekat pada penanganan perkara siber	LPSK, Kepolisian, Kejaksaan	Persentase korban yang menerima pendampingan psikologis
Penyedia Layanan Digital dan Keuangan	Kewajiban notifikasi pelanggaran data dan penghapusan cepat konten intim nonkonsensual	Regulator sektor digital, penyelenggara sistem elektronik	Waktu tanggap rata-rata notifikasi dan penghapusan konten
Penyedia Layanan Digital dan Keuangan	Kewajiban penahanan sementara dana pada rekening yang dilaporkan sebagai penampung hasil penipuan	Otoritas Jasa Keuangan, perbankan, penyelenggara sistem pembayaran	Nilai dana yang berhasil ditahan dan dikembalikan kepada korban
Komunitas dan Masyarakat Sipil	Literasi digital yang mengoreksi kalibrasi risiko, bukan sekadar menambah pengetahuan	Kementerian bidang digital, perguruan tinggi, organisasi masyarakat sipil	Perubahan skor kalibrasi risiko pada survei berkala
Komunitas dan Masyarakat Sipil	Pendampingan korban di luar jalur pidana	Organisasi keselamatan daring, lembaga bantuan hukum	Jumlah korban terlayani dan tingkat kepercayaan korban terhadap aparat

Sumber: hasil olahan penulis (2026), disintesis dari (Aisy et al., 2025, Price, 2021, Rackley et al., 2021, Sun et al., 2025)

Indikator pada Tabel 2 sengaja dipilih agar dapat diukur tanpa menunggu perubahan undang-undang. Proporsi laporan yang mencapai tahap penyidikan, rasio restitusi yang benar-benar dibayarkan terhadap yang diputuskan, waktu tanggap penghapusan konten, dan tingkat kepercayaan korban terhadap aparat merupakan besaran yang dapat dipantau secara berkala. Basis datanya pun sudah sebagian tersedia, meskipun kualitas pencatatan perlu diperbaiki lebih dahulu karena pelaporan yang tidak lengkap secara langsung menggerus kegunaan data administratif bagi kebijakan pencegahan (Giro Correia, 2022). Pemantauan berkala terhadap indikator-indikator ini akan memberi umpan balik yang selama ini tidak dimiliki pembuat kebijakan, sekaligus menjadi bahan bagi riset lanjutan yang lebih terarah (Zhao & Cheng, 2024).

Ada satu catatan penutup yang perlu disampaikan dengan jujur. Model ini disusun dari analisis normatif dan sintesis bukti empiris yang dikumpulkan peneliti lain di yurisdiksi berbeda. Sebagian proposisinya—terutama mengenai sikap aparat Indonesia terhadap korban kejahatan siber dan pengalaman korban dalam menempuh mekanisme pemulihan—belum diuji dengan data lapangan Indonesia. Pengujian itu justru menjadi agenda paling mendesak, dan rancangan penelitian yang diuraikan pada bagian metode disiapkan untuk keperluan tersebut. Kerangka transformasi digital yang terfragmentasi dan reaktif, sebagaimana didiagnosis dalam kajian atas fondasi hukumnya (Anggono et al., 2025), hanya dapat diperbaiki bila perumusan kebijakan berpijak pada bukti tentang apa yang benar-benar dialami korban, bukan pada asumsi tentang apa yang seharusnya mereka alami. Kepercayaan konsumen terhadap ekonomi digital, pada akhirnya, dibangun dari pengalaman nyata bahwa negara hadir ketika sesuatu berjalan salah (Prastyanti & Sharma, 2024). Tanpa itu, penguatan

regulasi hanya akan menambah pasal tanpa menambah keadilan, sebuah risiko yang juga membayangi upaya menyesuaikan instrumen hukum internasional dengan teknologi kecerdasan buatan yang terus berkembang (Velasco, 2022).

4. KESIMPULAN

Arsitektur normatif perlindungan korban kejahatan siber di Indonesia tampak lengkap secara tekstual, namun mengalami kegagalan sistemik pada rantai pemulihan. Melalui lensa sistem hukum, penelitian ini menemukan bahwa kegagalan tersebut bersifat multidimensi dan saling memperkuat. Secara substansial, norma masih bias pada pengendalian konten dan pemidanaan pelaku, sementara hak subjek data sulit ditegakkan. Secara struktural, penegakan hukum terhambat oleh defisit kapasitas forensik digital, ketiadaan standar pembuktian elektronik yang baku, dan tumpang tindih kewenangan antarlembaga. Secara kultural, rendahnya pelaporan dan praktik viktimisasi sekunder oleh aparat membuat sebagian besar kasus tidak pernah mencapai tahap peradilan. Pengakuan hak korban dalam KUHP dan KUHP terbaru, meski merupakan pergeseran paradigmatis, belum diimbangi oleh regulasi turunan yang operasional.

Kontribusi utama penelitian ini terletak pada pergeseran pendekatan dari analisis sektoral menuju pembacaan holistik atas lima instrumen hukum utama sebagai satu matriks yang koheren, yang secara presisi memetakan titik terputusnya hak korban. Secara praktis, penelitian ini menawarkan model perlindungan terintegrasi berbasis empat pilar aktor dan tiga fase. Kebaruan (*novelty*) model ini terletak pada penempatan penyedia layanan digital dan keuangan bukan sekadar sebagai subjek yang mematuhi regulasi administratif, melainkan sebagai pemikul kewajiban kehati-hatian (*duty of care*) yang dapat dituntut secara hukum oleh korban, setara dengan peran aparat penegak hukum.

Berdasarkan temuan tersebut, reformasi hukum harus bergerak melampaui amendemen pasal menuju perbaikan sistemik. Rekomendasi strategis penelitian ini mencakup tiga agenda utama: (1) Reformasi Pemulihan: memisahkan mekanisme kompensasi negara dari restitusi pelaku untuk menjamin kepastian, serta memperluas cakupan tindak pidana yang berhak atas kompensasi; (2) Penguatan Kelembagaan: percepatan pembentukan otoritas pengawas data pribadi yang independen dan penerbitan aturan pembuktian elektronik tanpa penundaan; dan (3) Regulasi Platform: internalisasi kewajiban notifikasi pelanggaran data, mekanisme penghapusan cepat konten intim nonkonsensual, dan kewajiban penahanan dana darurat pada rekening yang terindikasi sebagai penampung hasil penipuan.

Keterbatasan penelitian ini perlu diakui secara transparan. Analisis yang disajikan masih bertumpu pada konstruksi normatif dan sintesis data empiris sekunder dari yurisdiksi komparatif. Proposisi mengenai respons aparat dan pengalaman korban di Indonesia belum diuji secara langsung dengan data primer. Oleh karena itu, agenda penelitian masa depan yang paling mendesak adalah pengujian empiris terhadap model yang diusulkan, khususnya melalui pengumpulan data lapangan dari penyidik, penuntut, dan korban, serta validasi indikator kinerja seperti rasio realisasi restitusi dan proporsi laporan yang berhasil naik ke tahap penyidikan. Pengujian ini krusial untuk mengubah model teoretis menjadi kebijakan berbasis bukti (*evidence-based policy*) yang efektif.

DEKLARASI

Pendanaan

Penulis tidak menerima bantuan finansial dalam bentuk apa pun untuk pelaksanaan penelitian, penyusunan, dan/atau publikasi artikel ini.

Konflik Kepentingan

Penulis menyatakan tidak memiliki benturan kepentingan finansial maupun hubungan personal yang dapat memengaruhi hasil penelitian yang dilaporkan dalam artikel ini.

Ketersediaan Data dan Bahan Hukum

Seluruh bahan hukum dan sumber sekunder yang dianalisis dalam penelitian ini telah tercantum lengkap di dalam naskah dan daftar pustaka.

Pernyataan Penggunaan AI

Penulis menggunakan Google Gemini sebagai alat bantu pada tahap pemetaan literatur dan penyuntingan

kebahasaan. Penggunaan tersebut terbatas pada efisiensi teknis dan tidak melibatkan proses analisis substantif. Seluruh interpretasi hukum, argumentasi, dan kesimpulan dirumuskan, diverifikasi, dan dipertanggungjawabkan sepenuhnya oleh penulis. Penulis menegaskan bahwa kecerdasan buatan tidak berperan dalam pengambilan keputusan intelektual maupun penarikan kesimpulan penelitian.

DAFTAR PUSTAKA

- Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: A cross sectional study. *Crime Science*, 13(1). <https://doi.org/10.1186/s40163-024-00230-w>
- Aisy, F. R., Maskur, M. A., & Amiruddin, A. M. A. (2025). Establishing Indonesia's personal data protection agency: Comparative administration sanctions enforcement from Ireland, Australia, and Singapore. *Journal of Indonesian Legal Studies*, 10(1), 431-482. <https://doi.org/10.15294/jils.v10i1.13755>
- Aji, M. P. (2025). Cybersecurity politics in building cyber sovereignty in Indonesia through strengthening the role of the national cyber and crypto agency. *Society*, 13(2), 1056-1071. <https://doi.org/10.33019/society.v13i2.960>
- Ali, A. S., Zaaba, Z. F., Singh, M. M., Anuar, N. B., & Shariff, M. R. B. M. (2025). Advancing cybersecurity in ASEAN: Current trends, emerging challenges, and opportunities for enhanced resilience. *International Journal of Information Security*, 24(5). <https://doi.org/10.1007/s10207-025-01111-2>
- Ali, M., Mulyono, A., Sanjaya, W., & Wibowo, A. (2022). Compensation and restitution for victims of crime in Indonesia: Regulatory flaws, judicial response, and proposed solution. *Cogent Social Sciences*, 8(1). <https://doi.org/10.1080/23311886.2022.2069910>
- Anggono, B. D., Wahanisa, R., Sari A.P, A. O. V. P., & Adiyatma, S. E. (2025). Interrogating the legal foundations of digital transformation: Balancing economic growth and social welfare in the era of disruption. *Volkgeist: Jurnal Ilmu Hukum dan Konstitusi*, 191-211. <https://doi.org/10.24090/volkgeist.v8i1.12211>
- Aprilianda, N., & Fibriansyah, R. I. (2021). Implications of legal loophole concerning liability over delay in restitution payment by criminal offender. *Jurnal Media Hukum*, 28(1), 47-56. <https://doi.org/10.18196/jmh.v28i1.10411>
- Aprilianda, N., Maharani, F., A. Kadir, N., Ferdian, A., & Solehuddin, S. (2025). Re-conceptualizing child victim rights: A normative and comparative analysis of victim impact statement in Indonesia's juvenile justice system. *Jambura Law Review*, 7(2), 442-467. <https://doi.org/10.33756/jlr.v7i2.30132>
- Ariawan, A. (2025). Regulatory barriers to consumer protection in digital marketplaces. *Journal of Human Rights, Culture and Legal System*, 5(3), 806-832. <https://doi.org/10.53955/jhcls.v5i3.782>
- Arsawati, N. N. J., Putri, L. P. Y. K., Wulandari, N. G. A. A. M. T., Tajuddin, H. H. A., & Withnall, E. G. (2024). Comparative analysis of witness protection law in Indonesia, Malaysia, and Australia. *Journal of Indonesian Legal Studies*, 9(2). <https://doi.org/10.15294/jils.v9i2.1498>
- Azisa, N., Muin, A. M., Munandar, M. A., Mukhlis, M. M., & Rahman, A. A. (2025). Psychological recovery of crime victims within contemporary restorative justice: An Islamic legal perspective. *MILRev: Metro Islamic Law Review*, 4(2), 1098-1127. <https://doi.org/10.32332/milrev.v4i2.11184>
- Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLOS ONE*, 20(1), e0317232. <https://doi.org/10.1371/journal.pone.0317232>
- Bartoli, L. (2025). Cybersecurity and the fight against cybercrime: Partners or competitors? *European Journal of Risk Regulation*, 16(2), 498-513. <https://doi.org/10.1017/err.2025.31>
- Bekkers, L., Leukfeldt, R., & Kleemans, E. (2025). Police investigations into financial-economic cybercriminal networks: The experiences and perceptions of Dutch law enforcement. *European Journal on Criminal Policy and Research*, 32(2), 305-324. <https://doi.org/10.1007/s10610-025-09615-2>

- Borwell, J., Jansen, J., & Stol, W. (2021). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review*, 40(4), 933-954. <https://doi.org/10.1177/0894439320983828>
- Borwell, J., Jansen, J., & Stol, W. (2024). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology*, 31(1), 156-181. <https://doi.org/10.1177/02697580241282782>
- Borwell, J., Jansen, J., & Stol, W. (2025). The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors. *European Journal of Criminology*, 22(4), 603-624. <https://doi.org/10.1177/14773708241312506>
- Budiono, A., Absori, A., Wardiono, K., Yuspin, W., & Gulyamov, S. S. (2023). Cyber indoctrination victims in Indonesia and Uzbekistan: Victim protection and indoctrination in practice. *Journal of Human Rights, Culture and Legal System*, 3(3), 441-475. <https://doi.org/10.53955/jhcls.v3i3.127>
- Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022a). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, 10, 25464-25493. <https://doi.org/10.1109/access.2022.3154059>
- Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022b). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, 8(1). <https://doi.org/10.1093/cybsec/tyac014>
- Chatzisyneonidis, S., & Pina, A. (2024). Exploring police attitudes on victims' delayed reporting and victim blame in technology-facilitated IPV. *Crime Science*, 13(1). <https://doi.org/10.1186/s40163-024-00213-x>
- Choi, K.-S., & Lee, H. (2023). The trend of online child sexual abuse and exploitations: A profile of online sexual offenders and criminal justice response. *Journal of Child Sexual Abuse*, 33(6), 804-823. <https://doi.org/10.1080/10538712.2023.2214540>
- Colburn, D. A., Finkelhor, D., & Turner, H. A. (2023). Help-seeking from websites and police in the aftermath of technology-facilitated victimization. *Journal of Interpersonal Violence*, 38(21-22), 11642-11665. <https://doi.org/10.1177/08862605231186156>
- Council of Europe. (2001). *Convention on Cybercrime* (European Treaty Series No. 185). Council of Europe.
- De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, 41(8), 1796-1808. <https://doi.org/10.1080/0144929x.2021.1905066>
- DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adults. *Innovation in Aging*, 5(4). <https://doi.org/10.1093/geroni/igab043>
- Enggarsasi, U., Sa'diyah, N. K., & Martio, P. A. (2024). Legal safeguards for victims of data dissemination crimes and cybercrime protection. *Jurnal Hukum*, 40(2), 258. <https://doi.org/10.26532/jh.v40i2.39974>
- Feka, M., Pujiyono, Sularto, R. B., & Pareke, J. (2025). Navigating the legal minefield: The impact of articles 27a and 27b of Indonesia's EIT Law on freedom of expression and the path to legal reform. *Journal of Law and Legal Reform*, 6(1), 265-304. <https://doi.org/10.15294/jllr.v6i1.19116>
- Franceschini, I., Li, L., & Bo, M. (2023). Compound capitalism: A political economy of Southeast Asia's online scam operations. *Critical Asian Studies*, 55(4), 575-603. <https://doi.org/10.1080/14672715.2023.2268104>
- Frosio, G., & Geiger, C. (2023). Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *European Law Journal*, 29(1-2), 31-77. <https://doi.org/10.1111/eulj.12475>
- Giro Correia, S. (2022). Making the most of cybercrime and fraud crime report data: A case study of UK action fraud. *International Journal of Population Data Science*, 7(1). <https://doi.org/10.23889/ijpds.v7i1.1721>

- Grant, S., & Buil-Gil, D. (2025). The effect of true crime docuseries on romance fraud reporting to the police. *Crime Science*, 14(1). <https://doi.org/10.1186/s40163-025-00244-y>
- Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice*, 46(6), 837-842. <https://doi.org/10.1007/s12103-021-09652-7>
- Holt, T. J., & Cross, C. (2024). Assessing the correlates of cryptofraud victimization reporting. *Deviant Behavior*, 47(2), 313-324. <https://doi.org/10.1080/01639625.2024.2435907>
- Indah, C. M., & Dwiyatmi, S. H. (2024). Advancing access to justice for female victims of sexual violence through restitution. *Jurnal Hukum*, 40(1), 171. <https://doi.org/10.26532/jh.v40i1.37794>
- Irvin-Erickson, Y. (2024). Identity fraud victimization: A critical review of the literature of the past two decades. *Crime Science*, 13(1). <https://doi.org/10.1186/s40163-024-00202-0>
- Ismail, I., & Akram Zainol Ariffin, K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *Plos One*, 20(9), e0331683. <https://doi.org/10.1371/journal.pone.0331683>
- Jaelani, A. K., & Luthviati, R. D. (2021). The crime of damage after the Constitutional Court's decision number 76/puu-xv/2017. *Journal of Human Rights, Culture and Legal System*, 1(1). <https://doi.org/10.53955/jhcls.v1i1.5>
- Kassem, R. (2023). How fraud impacts individuals' wellbeing – academic insights and gaps. *Journal of Financial Crime*, 31(5), 1261-1268. <https://doi.org/10.1108/jfc-08-2023-0215>
- Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Gale Vergara, R. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, 11, 971. <https://doi.org/10.12688/f1000research.123098.1>
- Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, 362, 112133. <https://doi.org/10.1016/j.forsciint.2024.112133>
- Laia, W. D., Anggustin, M., & Sihotang, L. (2025). Application of criminal law in online gambling case. *International Journal of Law, Crime and Justice*, 2(1), 108-121. <https://doi.org/10.62951/ijlcj.v2i1.440>
- Lee, C. S. (2021). Online fraud victimization in China: A case study of Baidu Tieba. *Victims & Offenders*, 16(3), 343-362. <https://doi.org/10.1080/15564886.2020.1838372>
- Luong, H. T., & Ngo, H. M. (2024). Understanding the nature of the transnational scam-related fraud: Challenges and solutions from Vietnam's perspective. *Laws*, 13(6), 70. <https://doi.org/10.3390/laws13060070>
- Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2023). Cybercriminal networks in the UK and beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, 27(3), 364-387. <https://doi.org/10.1007/s12117-022-09476-9>
- Machado, C. C. V., & Aguiar, T. H. (2023). Emerging regulations on content moderation and misinformation policies of online media platforms: Accommodating the duty of care into intermediary liability models. *Business and Human Rights Journal*, 8(2), 244-251. <https://doi.org/10.1017/bhj.2023.25>
- Mania, K. (2022). 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. <https://doi.org/10.1177/15248380221143772>
- Manitra, R. R. M., Prabandari, A. P., Jibril, A. M., & Hossain, A. (2026). A proposal for decriminalisation of online defamation in Indonesia: Towards a human rights-based approach. *Cogent Social Sciences*, 12(1). <https://doi.org/10.1080/23311886.2026.2613959>
- Manullang, S. O. (2022). The legality of devious cyber practices: Readiness of Indonesia's cyber laws. *Society*, 10(2), 489-502. <https://doi.org/10.33019/society.v10i2.482>

- Marwan, A., Garduño, D. O.-C., & Bonfigli, F. (2022). Detection of digital law issues and implication for good governance policy in Indonesia. *Bestuur*, 10(1), 22. <https://doi.org/10.20961/bestuur.v10i1.59143>
- Masyhar, A., & Emovwodo, S. O. (2023). Techno-prevention in counterterrorism: Between countering crime and human rights protection. *Journal of Human Rights, Culture and Legal System*, 3(3), 625-655. <https://doi.org/10.53955/jhcls.v3i3.176>
- Mensah, R. O., Mensah, P., & Opoku, D. (2023). Experiences and perceptions of cybercrime victims in Ghana: The perspective of digital consumers of agricultural produce. *Cogent Education*, 10(2). <https://doi.org/10.1080/2331186x.2023.2285623>
- Meurs, T., Junger, M., Cruyff, M., & van der Heijden, P. G. M. (2025). Estimating the number of ransomware attacks. *Journal of Quantitative Criminology*, 42(2), 227-243. <https://doi.org/10.1007/s10940-025-09625-7>
- Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, 6, 100296. <https://doi.org/10.1016/j.fsisyn.2022.100296>
- Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, 23(4). <https://doi.org/10.1007/s11920-021-01228-w>
- Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy*, 4(3), 731-761. <https://doi.org/10.3390/jcp4030034>
- Mumford, E. A., Rothman, E. F., Maitra, P., & Sheridan-Johnson, J. (2022). U.s. Young adults' professional help-seeking in response to technology-facilitated abuse. *Journal of Interpersonal Violence*, 38(11-12), 7063-7088. <https://doi.org/10.1177/08862605221140042>
- Nascimento, A. M., Andrade, J., & de Castro Rodrigues, A. (2022). The psychological impact of restorative justice practices on victims of crimes—a systematic review. *Trauma, Violence, & Abuse*, 24(3), 1929-1947. <https://doi.org/10.1177/15248380221082085>
- Natamiharja, R., Sabatira, F., Banjarani, D. R., Davey, O. M., & Setiawan, I. (2022). Balancing two conflicting perspectives on wiretapping act: Rights to privacy and law enforcement. *Al-Risalah: Forum Kajian Hukum dan Sosial Kemasyarakatan*, 22(1), 18-30. <https://doi.org/10.30631/alrisalah.v22i1.1226>
- Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, 27(3), 272-294. <https://doi.org/10.1177/02697580211010692>
- O'Malley, R. L. (2023). Short-term and long-term impacts of financial sextortion on victim's mental well-being. *Journal of Interpersonal Violence*, 38(13-14), 8563-8592. <https://doi.org/10.1177/08862605231156416>
- Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological impact of hacking victimization. *Sage Open*, 11(4). <https://doi.org/10.1177/21582440211061556>
- Pangaribuan, A. (2026). Victim protection in Indonesia: Rhetoric, reality, and the functionalisation thesis. *International Review of Victimology*. <https://doi.org/10.1177/02697580261441319>
- Panjaitan, H., Girsang, J., Djanegara, M. S., & Fahim, M. H. K. (2025). Strengthening consumer protection in digital transactions: A legal perspective on click-wrap agreements under the consumer protection law. *Jurnal Hukum*, 41(3), 666. <https://doi.org/10.26532/jh.v41i3.47262>
- Pituk, P., Chutipattana, N., Laor, P., Sukdee, T., Kittikun, J., Jitwiratnukool, W., Fajriyah, R., & Saisanan Na Ayudhaya, W. (2025). Digital media victimization among older adults in upper-southern Thailand. *Informatics*, 12(1), 24. <https://doi.org/10.3390/informatics12010024>
- Prastyanti, R. A., & Sharma, R. (2024). Establishing consumer trust through data protection law as a competitive advantage in Indonesia and India. *Journal of Human Rights, Culture and Legal System*, 4(2), 354-390. <https://doi.org/10.53955/jhcls.v4i2.200>

- Price, L. (2021). Platform responsibility for online harms: Towards a duty of care for online hazards. *Journal of Media Law*, 13(2), 238-261. <https://doi.org/10.1080/17577632.2021.2022331>
- Purnama Pratiwi, P. F., Aziz, A. S., Nurdin, F. S., Gunarto, & Abdelaali, M. (2025). Assessing legal protection effectiveness for women facing digital sexual violence. *Journal of Human Rights, Culture and Legal System*, 5(3), 922-948. <https://doi.org/10.53955/jhcls.v5i3.795>
- Purwadi, H., Lukitasari, D., Mayastuti, A., Abd Aziz, H., & Cahyaningtyas, I. (2024). Regulatory framework on compensation for the restoration of victims of sexual violence. *Law Reform*, 20(2), 383-407. <https://doi.org/10.14710/lr.v20i2.58181>
- Rackley, E., McGlynn, C., Johnson, K., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). Seeking justice and redress for victim-survivors of image-based sexual abuse. *Feminist Legal Studies*, 29(3), 293-322. <https://doi.org/10.1007/s10691-021-09460-8>
- Raharjo, A., Bintoro, R. W., Tri Utami, N. A., & Suzuki, M. (2022). The legal policy of criminal justice bureaucracy cybercrime. *Bestuur*, 10(2), 105. <https://doi.org/10.20961/bestuur.v10i2.64498>
- Rahman, F. (2025). Safeguarding personal data in the public sector: Unveiling the impact of the new personal data protection act in Indonesia. *UUM Journal of Legal Studies*, 16(1), 1-18. <https://doi.org/10.32890/uumjls2025.16.1.1>
- Ramli, A. M., Suseno, S., Mayana, R. F., Rajamanickam, R., & Rohmana, R. D. (2026). The urgency of regulating artificial intelligence in relation to cybersecurity and cyber resilience. *Cogent Social Sciences*, 12(1). <https://doi.org/10.1080/23311886.2026.2632977>
- Ray, A., & Henry, N. (2024). Sextortion: A scoping review. *Trauma, Violence, & Abuse*, 26(1), 138-155. <https://doi.org/10.1177/15248380241277271>
- Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.
- Republik Indonesia. (2014). *Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban*. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 293.
- Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.
- Republik Indonesia. (2018). *Peraturan Pemerintah Nomor 7 Tahun 2018 tentang Pemberian Kompensasi, Restitusi, dan Bantuan kepada Saksi dan Korban*. Lembaran Negara Republik Indonesia Tahun 2018 Nomor 21.
- Republik Indonesia. (2022a). *Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 120.
- Republik Indonesia. (2022b). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
- Republik Indonesia. (2023). *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.
- Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1.
- Republik Indonesia. (2025). *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*. Lembaran Negara Republik Indonesia Tahun 2025 Nomor 188.
- Robalo, T. L. A. S., & Abdul Rahim, R. B. B. (2023). Cyber victimisation, restorative justice and victim-offender panels. *Asian Journal of Criminology*, 18(1), 61-74. <https://doi.org/10.1007/s11417-023-09396-9>

- Sahak, S., Rajamanickam, R., & Hassan, M. S. (2025). Liability of internet intermediaries and legal challenges: A comprehensive systematic review. *Quality & Quantity*, 60(1), 2435-2457. <https://doi.org/10.1007/s11135-025-02344-y>
- Saputra, R., Setiodjati, J. P., & Barkhuizen, J. (2023). Under-legislation in electronic trials and renewing criminal law enforcement in Indonesia (comparison with United States). *Journal of Indonesian Legal Studies*, 8(1), 243-288. <https://doi.org/10.15294/jils.v8i1.67632>
- Setiawan, E., & Hartiwiningsih, H. (2025). Optimizing the use of digital forensics and information technology in proving criminal acts of electronic document forgery in Indonesia. *International Journal of Law, Crime and Justice*, 2(2), 72-86. <https://doi.org/10.62951/ijlcj.v2i2.587>
- Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review*, 10(1), 1. <https://doi.org/10.20956/halrev.v10i1.5016>
- Sheikh, M. M. R., & Rogers, M. M. (2023). Technology-facilitated sexual violence and abuse in low and middle-income countries: A scoping review. *Trauma, Violence, & Abuse*, 25(2), 1614-1629. <https://doi.org/10.1177/15248380231191189>
- Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: Welcoming Protocol II to the Budapest Convention on cybercrime. *ERA Forum*, 23(1), 101-108. <https://doi.org/10.1007/s12027-022-00707-8>
- Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, 45, 301554. <https://doi.org/10.1016/j.fsidi.2023.301554>
- Sudarwanto, A. S., & Kharisma, D. B. B. (2021). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, 29(4), 1443-1457. <https://doi.org/10.1108/jfc-09-2021-0193>
- Sun, J., Gu, S., & Su, R. (2025). Ai-empowered responsive regulation for preventing future crimes: An empirical inquiry into the regulatory pyramid to combat future crimes in China and Southeast Asia. *Asian Journal of Criminology*, 21(1). <https://doi.org/10.1007/s11417-025-09477-x>
- Sundram, P. (2024). ASEAN cooperation to combat transnational crime: Progress, perils, and prospects. *Frontiers in Political Science*, 6. <https://doi.org/10.3389/fpos.2024.1304828>
- Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Aurellia Nathania Tiarma, B. (2025). Cybercrime in the new Criminal Code in Indonesia. *Cogent Social Sciences*, 11(1). <https://doi.org/10.1080/23311886.2024.2439543>
- Triasari, D., Hanum, W. N., & Firmandiaz, V. (2023). Mapping restorative justice in information and electronic transaction criminal regulation. *Journal of Human Rights, Culture and Legal System*, 3(1), 1-16. <https://doi.org/10.53955/jhcls.v3i1.75>
- Triyanti, N., Handayani, I. G. A. K. R., & Karjoko, L. (2025). Legal gaps in personal data protection: Reforming Indonesia's population administration law. *Hasanuddin Law Review*, 11(1), 132. <https://doi.org/10.20956/halrev.v11i1.6177>
- Velasco, C. (2022). Cybercrime and artificial intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, 23(1), 109-126. <https://doi.org/10.1007/s12027-022-00702-z>
- Violin, G., & Nafi, Y. K. (2022). Protection of online gender-based violence victims: A feminist legal analysis. *The Indonesian Journal of Socio-Legal Studies*, 1(2). <https://doi.org/10.54828/ijsls.2021v1n2.6>
- Wibowo, A., Alawiyah, W., & Azriadi (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, 10(1). <https://doi.org/10.1080/23311886.2024.2306751>

- Xie, M., Ortiz Solis, V., & Chauhan, P. (2023). Declining trends in crime reporting and victims' trust of police in the United States and major metropolitan areas in the 21st century. *Journal of Contemporary Criminal Justice*, 40(1), 138-171. <https://doi.org/10.1177/10439862231190212>
- Yuspin, W., Rajput, T., Basu Bal, A., Wardiono, K., & Absori, A. (2024). The regulations of the supervisory officer personal data protection-based accountability principle. *Bestuur*, 12(1), 49. <https://doi.org/10.20961/bestuur.v12i1.89742>
- Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal data protection law in digital banking governance in Indonesia. *StudiaIuridica Lublinensia*, 32(1), 99-130. <https://doi.org/10.17951/sil.2023.32.1.99-130>
- Zaltina, P., & Nurtjahyo, L. I. (2024). Right to be forgotten as a legal protection for the victims of electronic sexual violence cases. *The Indonesian Journal of Socio-Legal Studies*, 3(2). <https://doi.org/10.54828/ijsls.2024v3n2.4>
- Zhao, Y., & Cheng, L. (2024). A bibliometric study of research trends in cross-border cybercrime. *International Journal of Legal Discourse*, 9(1), 1-31. <https://doi.org/10.1515/ijld-2024-2001>