Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 3 Number 6, 2025
DOI: https://doi.org/10.61104/alz.v3i6.2802

Perlindungan Hukum Terhadap Korban Kejahatan Siber di Indonesia Dalam Perspektif Hukum Internasional

Annisa Khaidir[1], Mahendra Putra Kurnia[2], Rika Erawaty[3]
Fakultas Hukum, Universitas Mulawarman, Samarinda, Indonesia[1-3]
Email Korespondensi: khaidirannisa2@gmail.com

Article received: 15 September 2025, Review process: 25 September 2025
Article Accepted: 10 Oktober 2025, Article published: 16 Desember 2025

ABSTRACT
This study aims to analyze the implementation of legal protection in Indonesia for victims of cybercrime based on national regulations and international legal principles, and to identify the obstacles faced by the national legal system in providing legal protection according to international standards. The research method used is doctrinal research with a historical and comparative approach to national legal instruments such as Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and the 2001 Budapest Convention. The results of the study indicate that legal protection for victims of cybercrime in Indonesia is not optimal due to weak victim recovery mechanisms, incomplete derivative regulations, and limited international cooperation due to the non-ratification of the Budapest Convention. Therefore, it is necessary to harmonize national regulations with international legal principles to strengthen the protection system for victims of cybercrime in Indonesia.
Keywords: *Legal Protection, Cybercrime, International Law*

ABSTRAK
Penelitian ini bertujuan untuk menganalisis penerapan perlindungan hukum di Indonesia terhadap korban kejahatan siber berdasarkan regulasi nasional dan prinsip-prinsip hukum internasional, serta mengidentifikasi kendala yang dihadapi sistem hukum nasional dalam memberikan perlindungan hukum sesuai standar internasional. Metode penelitian yang digunakan adalah penelitian doktrinal dengan pendekatan historis dan perbandingan terhadap instrumen hukum nasional seperti Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, dan Konvensi Budapest 2001. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap korban kejahatan siber di Indonesia belum optimal karena lemahnya mekanisme pemulihan korban, belum lengkapnya aturan turunan, serta terbatasnya kerja sama internasional akibat belum diratifikasinya Konvensi Budapest. Oleh karena itu, diperlukan harmonisasi regulasi nasional dengan prinsip-prinsip hukum internasional untuk memperkuat sistem perlindungan korban kejahatan siber di Indonesia.
Kata Kunci: Perlindungan Hukum, Kejahatan Siber, Hukum Internasional

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi signifikan dalam kehidupan manusia, memfasilitasi komunikasi global, transaksi elektronik, dan pertukaran informasi secara instan. Namun, kemajuan ini juga melahirkan ancaman baru berupa kejahatan siber *(cybercrime)*, yang semakin kompleks dan sulit dikendalikan. Kejahatan siber tidak hanya menimbulkan kerugian finansial, tetapi juga melanggar privasi, merusak reputasi, dan bahkan mengancam keamanan nasional. Menurut laporan *World Economic Forum* (2023), lanskap keamanan siber global pada tahun 2025 diperkirakan akan semakin kompleks, dengan peningkatan serangan yang melibatkan kecerdasan buatan dan teknologi canggih (World Economic Forum, 2023).

Di Indonesia, fenomena kejahatan siber mengalami peningkatan yang signifikan seiring dengan masifnya penggunaan internet dan media sosial. Data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa pada tahun 2024, jumlah pengguna internet di Indonesia mencapai 221 juta orang, menjadikannya negara dengan pengguna internet terbesar ke-4 di dunia (APJII, 2023). Namun, pertumbuhan ini diiringi oleh lonjakan kasus kejahatan siber, seperti peretasan, pencurian data, penyebaran malware, phishing, dan ransomware. Laporan Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada paruh kedua tahun 2023, terjadi lebih dari 685 juta serangan siber, dengan rata-rata 13 juta serangan per hari. Pada enam bulan pertama tahun 2024, serangan siber mencapai 2,4 miliar kasus, menunjukkan tingkat ancaman yang sangat tinggi terhadap keamanan siber di Indonesia (Badan Siber dan Sandi Negara, 2024).

Korban kejahatan siber tidak hanya menanggung kerugian materiil, tetapi juga dampak psikologis dan sosial yang serius. Kondisi ini dapat menimbulkan viktimisasi sekunder, di mana korban mengalami penderitaan lanjutan akibat proses hukum yang berbelit, sikap aparat penegak hukum yang kurang empati, atau stigma sosial. Contoh nyata adalah kasus serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS 2) pada Juni 2024, yang dilakukan oleh kelompok peretas internasional Brain Cipher (varian LockBit 3.0). Serangan ini melumpuhkan sistem data milik Kementerian Komunikasi dan Informatika, mempengaruhi lebih dari 282 instansi pemerintah dan daerah, termasuk Direktorat Jenderal Imigrasi. Para pelaku menuntut tebusan sebesar US$ 8 juta, namun pemerintah menolak membayar, sehingga sebagian besar data tidak dapat dipulihkan dan diduga diperjualbelikan di *dark web*. Kasus ini menegaskan lemahnya perlindungan hukum bagi korban kejahatan siber di Indonesia, di mana korban institusi dan masyarakat tidak memperoleh pemulihan yang memadai (Akinyemi, O., Sulaiman, R., & Abosata, N. 2023).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang Nomor 19 Tahun 2016) merupakan dasar utama dalam mengatur tindak pidana siber di Indonesia. UU ITE berperan sebagai *lex specialis* yang mengatur berbagai bentuk penipuan dan kejahatan siber melalui media sosial dan platform digital. Namun, implementasinya sering kali menimbulkan paradoks, di mana, UU ITE lebih menitikberatkan pada aspek pidana terhadap pelaku, tanpa

memberikan aturan yang jelas mengenai pemulihan dan kompensasi bagi korban. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) diharapkan menjadi tonggak penting dalam melindungi data pribadi masyarakat di era digital. UU PDP mengadopsi prinsip-prinsip seperti *lawfulness, fairness*, dan *purpose limitation*, yang sejalan dengan *General Data Protection Regulation* (GDPR) Uni Eropa. Namun, efektivitasnya masih diragukan karena belum adanya lembaga pengawas independen yang sepenuhnya beroperasi, serta keterbatasan mekanisme penegakan sanksi. Pada kasus kebocoran data BPJS Kesehatan tahun 2021, yang menyangkut data 279 juta peserta, korban tidak memperoleh kompensasi yang layak, meskipun data pribadi mereka diperdagangkan secara ilegal.

Dari perspektif hukum internasional, berbagai upaya telah dilakukan untuk menangani kejahatan siber, seperti pengesahan *Budapest Convention on Cybercrime 2001* oleh *Council of Europe.* Konvensi ini menetapkan standar global dalam pemberantasan kejahatan siber dan kerja sama antarnegara. Namun, Indonesia hingga saat ini belum meratifikasi konvensi tersebut, sehingga kerja sama internasional dalam pemberantasan kejahatan siber menjadi terbatas. Ketiadaan keterikatan Indonesia pada instrumen internasional seperti *Budapest Convention* menyebabkan hambatan dalam proses ekstradisi, pengumpulan bukti digital lintas negara, dan koordinasi dengan lembaga penegak hukum internasional. Prinsip-prinsip hukum internasional menempatkan korban sebagai subjek hukum yang harus mendapatkan pemulihan dan perlindungan secara maksimal (Putra, D. K, 2021). *United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power* (1985) menegaskan hak korban atas perlindungan, kompensasi, dan rehabilitasi. Namun, dalam konteks nasional, perlindungan korban kejahatan siber di Indonesia masih berfokus pada aspek pidana terhadap pelaku, sementara aspek pemulihan korban sering kali diabaikan. Tidak ada sistem terpadu yang memastikan korban mendapatkan keadilan secara komprehensif, baik melalui bantuan hukum, ganti rugi, maupun perlindungan psikologis.

Perbandingan dengan praktik internasional menunjukkan bahwa negara-negara yang telah meratifikasi *Budapest Convention* umumnya memiliki mekanisme yang lebih efektif dalam melindungi korban kejahatan siber. Negara-negara tersebut membangun sistem kerja sama lintas negara, mengadopsi teknologi forensik digital modern, serta menyediakan layanan pendampingan khusus bagi korban. Sebagai contoh, Amerika Serikat melalui *Computer Fraud and Abuse Act* (CFAA) dan *Patriot Act* menyediakan jalur kompensasi cepat bagi korban, sementara Australia melalui *Cybercrime Legislation Amendment Act* 2012 menekankan pada *victim-centered justice* (Europol, 2023) Korban kejahatan siber memiliki karakteristik unik, sering tidak sadar menjadi korban karena serangan berlangsung diam- diam. Kerugian meliputi finansial, hilangnya data pribadi, rusaknya reputasi, dan dampak psikologis. Korban dapat berupa individu, korporasi, atau negara. Teori viktimologi modern menekankan hak korban atas pemulihan dan partisipasi hukum sesuai prinsip internasional.

Artikel ini bertujuan untuk menganalisis penerapan perlindungan hukum terhadap korban kejahatan siber di Indonesia berdasarkan regulasi nasional dan prinsip-prinsip hukum internasional, serta mengidentifikasi kendala yang dihadapi

sistem hukum Indonesia dalam memberikan perlindungan tersebut sesuai standar internasional. Dengan menggunakan metode penelitian doktrinal, artikel ini mengkaji berbagai sumber hukum relevan untuk memberikan pemahaman mendalam tentang isu ini.

METODE

Penelitian ini menggunakan pendekatan doktrinal (normatif) dengan jenis penelitian deskriptif-analitis. Bahan hukum primer mencakup peraturan perundang-undangan nasional seperti Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, dan UU No. 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban, serta instrumen internasional seperti *Budapest Convention* 2001 dan *Declaration of Basic Principles of Justice for Victms Of Crime and Abuse of Power* 1985. Pendekatan historis digunakan untuk menelusuri perkembangan regulasi *cyber law* di Indonesia, sedangkan perbandingan digunakan untuk menilai kesesuaian sistem hukum nasional dengan praktik negara lain yang telah mengadopsi Konvensi Budapest.

HASIL DAN PEMBAHASAN

Penerapan Perlindungan Hukum Terhadap Korban Kejahatan Siber di Indonesia Berdasarkan Regulasi Nasional dan Prinsip-Prinsip Hukum Internasional

Perkembangan teknologi informasi yang sangat cepat telah mengubah hampir seluruh aspek kehidupan manusia, termasuk sistem ekonomi, politik, sosial, dan hukum. Digitalisasi yang diharapkan meningkatkan efisiensi dan transparansi, pada kenyataannya juga membuka peluang bagi munculnya berbagai bentuk kejahatan siber (*cybercrime*). Fenomena ini menimbulkan konsekuensi hukum baru, terutama terkait perlindungan terhadap korban yang menjadi pihak paling dirugikan oleh aktivitas kriminal digital.Kejahatan siber memiliki karakteristik unik, yakni bersifat *borderless*, anonim, dan menggunakan sistem elektronik sebagai sarana utama (Barda Nawawi Arief, 2008). Dalam konteks Indonesia, kejahatan ini meliputi peretasan (*hacking*), penipuan daring (*online fraud*), penyebaran data pribadi, penyebaran konten asusila, serta ujaran kebencian berbasis siber. Korban dari kejahatan tersebut tidak hanya mengalami kerugian material, tetapi juga penderitaan psikologis dan sosial yang sulit diukur secara ekonomis.

Perlindungan hukum terhadap korban kejahatan siber menjadi bagian penting dari prinsip negara hukum (*rechtstaat*), sebagaimana diatur dalam Pasal 1 ayat (3) Undang- Undang Dasar Negara Republik Indonesia Tahun 1945. Negara berkewajiban menjamin hak setiap warga negara untuk memperoleh rasa aman, keadilan, dan perlindungan dari segala bentuk kejahatan, termasuk yang terjadi di ruang siber. Dalam konteks inilah sistem hukum Indonesia dituntut untuk beradaptasi terhadap perkembangan teknologi. Regulasi utama yang menjadi dasar hukum terhadap kejahatan siber di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Undang-Undang ini mengatur

berbagai perbuatan hukum yang dilarang di dunia digital serta memberikan mekanisme hukum bagi korban untuk mengajukan pengaduan, pemulihan, dan penegakan hukum. Selain UU ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Undang-Undang Nomor 27 Tahun 2022) memberikan dasar hukum baru bagi perlindungan korban pelanggaran data pribadi. UU PDP memperkuat hak korban atas privasi dan keamanan data digital dengan memberikan hak untuk memperoleh pemberitahuan pelanggaran data, hak untuk menghapus data pribadi, dan hak untuk menuntut ganti rugi apabila datanya disalahgunakan (M. Arsyad Sanusi, 2004).

Dalam perspektif sistem perlindungan korban, Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban (Undang-Undang Nomor 31 Tahun 2014) memiliki relevansi penting. Melalui Lembaga Perlindungan Saksi dan Korban (LPSK), negara menyediakan mekanisme pemberian kompensasi, restitusi, bantuan medis, dan bantuan hukum. Namun, mekanisme tersebut masih belum spesifik mengatur perlindungan terhadap korban kejahatan siber, yang membutuhkan pendekatan berbeda dibanding korban kejahatan konvensional. Perlindungan hukum terhadap korban memiliki dua dimensi utama, yaitu preventif dan represif. Perlindungan preventif mencakup edukasi masyarakat, penguatan keamanan siber, dan sistem deteksi dini terhadap potensi kejahatan digital. Sedangkan perlindungan represif berkaitan dengan penegakan hukum setelah kejahatan terjadi, termasuk pemberian ganti rugi dan pemulihan kondisi korban kejahatan siber di Indonesia. Namun dalam penerapannya, banyak korban kejahatan siber mengalami kesulitan dalam memperoleh akses keadilan. Beberapa di antaranya tidak mengetahui prosedur pelaporan atau tidak memiliki bukti digital yang cukup kuat. Selain itu, prosedur hukum yang panjang dan birokratis sering kali membuat korban enggan melapor, sehingga tingkat *reporting* kasus siber masih sangat rendah di Indonesia.

Secara teoritis, perlindungan korban kejahatan berkaitan dengan teori *victimology,* yang memandang korban bukan sekadar objek dalam sistem peradilan pidana, tetapi juga subjek hukum yang memiliki hak. Dalam konteks hukum pidana modern, korban berhak atas partisipasi dalam proses hukum, pemulihan kerugian, dan perlindungan dari ancaman lanjutan. Prinsip inilah yang seharusnya menjadi dasar bagi kebijakan hukum Indonesia. Dalam hukum internasional, perlindungan korban didasarkan pada *Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power 1985*. Deklarasi ini menegaskan bahwa korban kejahatan siber berhak mendapatkan informasi, keadilan, restitusi, kompensasi, dan bantuan hukum tanpa diskriminasi. Indonesia sebagai anggota PBB berkewajiban untuk mengimplementasikan prinsip-prinsip tersebut ke dalam sistem hukumnya. Selain itu, *Budapest Convention on Cybercrime (2001)* merupakan instrumen hukum internasional paling penting dalam pemberantasan kejahatan siber. Konvensi ini menekankan kerja sama antarnegara dalam investigasi dan perlindungan korban lintas batas. Meskipun Indonesia belum meratifikasinya, prinsip-prinsip dalam konvensi tersebut seperti *protection of privacy* dan *access to justice* dapat diadopsi dalam hukum nasional melalui pendekatan harmonisasi lunak (*soft law*).

Dalam konteks ASEAN, Indonesia terlibat dalam *ASEAN Cybersecurity Cooperation Strategy 2021–2025* yang menekankan perlindungan hak digital dan keamanan data pengguna. Strategi regional ini menunjukkan pengakuan atas pentingnya perlindungan korban kejahatan siber di Asia Tenggara. Oleh karena itu, integrasi kebijakan nasional dengan komitmen regional menjadi langkah penting untuk memperkuat efektivitas perlindungan. Dari sisi kelembagaan, perlindungan korban kejahatan siber menuntut kerja sama antara lembaga penegak hukum dan regulator digital. LPSK, BSSN, Kominfo, dan Kepolisian juga harus memiliki sistem terpadu untuk mendeteksi, menindak, dan memulihkan korban. Integrasi data dan koordinasi antar lembaga masih menjadi tantangan yang sangat besar besar yang tentunya secara maksimal dan tentunya hal ini harus diselesaikan oleh pemerintah Indonesia. Bentuk perlindungan hukum juga mencakup pemulihan psikologis bagi korban, terutama dalam kasus pelecehan atau kekerasan berbasis gender online (KBGO) (LPSK, 2022). Dalam hal ini, kolaborasi dengan Kementerian Pemberdayaan Perempuan dan Perlindungan Anak serta lembaga swadaya masyarakat menjadi bagian dari sistem perlindungan korban secara menyeluruh.

Dalam praktik global, negara seperti Inggris, Korea Selatan, dan Jepang telah mengembangkan *Cyber Victim Support Unit* yang menyediakan layanan bantuan hukum, psikologis, dan teknis. Unit ini berfungsi memberikan pendampingan langsung kepada korban kejahatan digital. Model ini dapat menjadi referensi bagi Indonesia untuk memperkuat kelembagaan perlindungan korban kejahatan siber. Perlindungan hukum korban kejahatan siber di Indonesia juga harus mencakup aspek tanggung jawab penyelenggara sistem elektronik (U.S. Department of Justice, 2020). UU PDP mewajibkan penyelenggara melindungi data pengguna dan melaporkan kebocoran data, dengan sanksi administratif dan pidana sebagai perlindungan tidak langsung bagi korban kejahatan siber. Selain regulasi, literasi hukum digital masyarakat harus ditingkatkan melalui kampanye keamanan siber. Perlindungan khusus perlu diberikan pada korban rentan seperti anak- anak, perempuan, dan difabel digital, terutama dalam kasus eksploitasi seksual anak online sesuai UU Perlindungan Anak No. 35 Tahun 2014. Perlindungan hukum harus bersifat inklusif.

Penguatan aspek *due process of law* juga krusial. Aparat penegak hukum harus menjamin proses hukum yang adil, transparan, dan tidak memihak, baik bagi pelaku maupun korban. Prinsip *fair trial* dan *access to justice* harus menjadi pedoman dalam setiap penanganan kasus kejahatan siber di Indonesia yang kasusnya setiap tahun bertambah. Dengan demikian, penerapan perlindungan hukum terhadap korban kejahatan siber di Indonesia masih memerlukan penguatan regulasi, kelembagaan, dan kerja sama internasional. Integrasi hukum nasional dengan prinsip-prinsip internasional menjadi kunci agar korban memperoleh perlindungan yang efektif, berkeadilan, dan sesuai dengan standar hukum global.

Kendala Sistem Hukum Indonesia dan Upaya Mengatasi dalam Memberikan Perlindungan Hukum Bagi Korban Kejahatan Siber Sesuai Standar Hukum Internasional

Meskipun Indonesia telah memiliki sejumlah regulasi yang mengatur kejahatan siber dan perlindungan data pribadi, pelaksanaannya masih menghadapi kendala serius baik dari sisi substansi hukum, struktur kelembagaan, maupun budaya hukum masyarakat. Tantangan tersebut menjadikan perlindungan korban kejahatan siber belum berjalan optimal sesuai standar hukum internasional yang menekankan hak korban atas keadilan dan pemulihan yang efektif bagi korban kejahatan siber di Indonesia. Dari segi substansi hukum, peraturan perundang-undangan yang ada masih bersifat sektoral dan belum terintegrasi secara sistemik. UU ITE, UU PDP, dan UU Perlindungan Saksi dan Korban masing-masing mengatur aspek yang berbeda tanpa mekanisme koordinasi yang jelas antar perangkat hukum tersebut. Akibatnya, muncul kekosongan norma dalam hal perlindungan korban secara komprehensif, terutama dalam aspek kompensasi dan rehabilitasi pascakejahatan siber.

Kendala utama dalam substansi hukum terletak pada belum adanya *lex specialis* yang secara khusus mengatur perlindungan korban kejahatan siber. UU ITE cenderung berorientasi pada pelaku dengan menekankan unsur pidana, sementara hak-hak korban seperti hak untuk didengar, hak atas informasi, dan hak atas restitusi belum mendapat perhatian memadai. Kondisi ini tidak sejalan dengan prinsip-prinsip hukum internasional yang menekankan kesetaraan antara perlindungan terhadap pelaku dan korban kejahatan siber, bukan hanya fokus pada pemidanaan pelaku. Ketentuan dalam UU PDP memang memberikan kemajuan, tetapi implementasinya masih menghadapi kendala structural (L. Prasetyo, 2023). Belum ada lembaga independen yang secara efektif menjalankan fungsi pengawasan terhadap pelanggaran data pribadi. Padahal, *General Data Protection Regulation* (GDPR) di Uni Eropa menunjukkan pentingnya lembaga pengawas independen seperti *Data Protection Authority* untuk menjamin pemulihan korban kebocoran data.

Dari aspek struktur hukum, kelembagaan penegak hukum di Indonesia masih bekerja secara terpisah dan belum terkoordinasi dalam menangani kasus kejahatan siber. Polri, Kejaksaan, Kominfo, BSSN, dan LPSK memiliki kewenangan masing- masing, namun tidak diatur mekanisme koordinasi antar lembaga yang jelas dalam hal perlindungan korban. Akibatnya, proses hukum sering berjalan parsial dan berlarut- larut. Sebagai contoh, dalam kasus kebocoran data, Kementerian Kominfo berperan sebagai regulator, namun tidak memiliki kewenangan penegakan hukum pidana. Di sisi lain, kepolisian memiliki kewenangan penyidikan, namun sering kali terkendala dalam memperoleh data teknis yang dikuasai penyelenggara sistem elektronik. Kondisi ini menimbulkan *jurisdictional gap* yang berdampak langsung terhadap pemenuhan hak korban (Polda Jambi, 2024).

Kendala berikutnya adalah keterbatasan sumber daya manusia di bidang hukum dan teknologi informasi. Banyak aparat penegak hukum yang belum memiliki keahlian dalam *digital forensics* dan *cyber investigation*. Dalam kasus kejahatan siber yang kompleks, seperti *phishing*, *malware*, dan *ransomware*, bukti digital memerlukan penanganan teknis tinggi agar dapat dijadikan alat bukti yang sah di pengadilan. Selain itu, fasilitas dan infrastruktur pendukung penyidikan kejahatan siber masih terbatas. Hanya beberapa lembaga seperti Bareskrim Polri dan

BSSN yang memiliki laboratorium forensik digital berstandar internasional. Ketimpangan sarana antar wilayah menyebabkan banyak kasus siber di daerah tidak tertangani secara profesional, sehingga korban kehilangan kesempatan mendapatkan pemulihan hukum.

Dari segi budaya hukum, rendahnya kesadaran masyarakat terhadap pentingnya keamanan digital menjadi kendala serius. Banyak korban kejahatan siber tidak melapor karena merasa malu, takut, atau tidak mengetahui mekanisme hukum yang tersedia. Rendahnya tingkat literasi digital menyebabkan masyarakat cenderung pasif dan membiarkan kejahatan siber terus terjadi tanpa proses hukum. Fenomena *victim blaming* dalam masyarakat juga menjadi faktor penghambat perlindungan korban. Korban sering dianggap bersalah karena dianggap lalai menjaga data pribadinya. Sikap ini bertentangan dengan asas perlindungan korban dalam hukum pidana modern, yang menekankan bahwa korban tidak boleh dipersalahkan atas kejahatan yang menimpanya.

Dalam konteks hukum internasional, Indonesia juga menghadapi kendala karena belum menjadi pihak dari *Budapest Convention on Cybercrime*. Ketidakikutsertaan ini menyebabkan keterbatasan kerja sama internasional dalam penegakan hukum, terutama dalam hal pertukaran informasi, ekstradisi, dan *mutual legal assistance (MLA)* (Kharbanda, V. 2019). Padahal, kejahatan siber bersifat lintas batas, sehingga penanganannya harus memerlukan kerja sama antar global. Selain aspek substansi dan struktur, masalah waktu dan prosedur penegakan hukum juga menjadi kendala. Proses penyelidikan dan penyidikan kasus siber sering kali memakan waktu lama, sementara kerugian korban dapat meningkat secara eksponensial. Ketidakpastian hukum dalam beberapa pasal UU ITE juga menjadi faktor yang memperlemah posisi korban. Misalnya, tidak adanya pengaturan yang jelas tentang tanggung jawab *intermediary* (penyelenggara platform) atas kerugian yang dialami korban akibat kelalaian pengawasan konten atau pelanggaran keamanan sistem elektronik.

Untuk mengatasi berbagai kendala tersebut, diperlukan reformasi hukum yang bersifat struktural dan substansial. Pertama, perlu adanya penyusunan *Rancangan Undang-Undang Perlindungan Korban Kejahatan Siber* sebagai *lex specialis* yang mengatur hak-hak korban secara rinci. Undang-undang ini harus mencakup hak atas pemulihan, kompensasi, rehabilitasi, dan jaminan keamanan digital. Kedua, pemerintah perlu memperkuat kapasitas lembaga penegak hukum melalui pelatihan berkelanjutan di bidang *cyber law* dan *digital evidence management*. Aparat harus dibekali kemampuan teknis dalam mengamankan bukti digital, menganalisis jejak siber, dan bekerja sama dengan lembaga internasional seperti INTERPOL dan ASEAN. Ketiga, penting dibentuknya lembaga khusus bernama *National Cyber Victim Protection Agency* yang bertugas memberikan bantuan langsung kepada korban kejahatan siber. Lembaga ini dapat berfungsi layaknya *victim support office* di negara- negara Eropa, menyediakan bantuan hukum gratis, pendampingan psikologis, restitudi, dan juga tentunya koordinasi dengan aparat penegak hukum yang berwajib. Selain penguatan kelembagaan, perlu juga reformasi prosedural untuk mempercepat proses hukum korban kejahatan siber diIndonesia. Mekanisme pelaporan daring terintegrasi dapat diimplementasikan, sehingga korban bisa

melapor melalui satu portal nasional tanpa harus mendatangi berbagai instansi secara terpisah. Penerapan teknologi hukum juga dapat mempercepat proses perlindungan. Sistem *case tracking* berbasis digital memungkinkan korban memantau perkembangan kasus secara transparan, sehingga mengurangi potensi maladministrasi dan meningkatkan kepercayaan publik terhadap sistem peradilan (Daly, K. 2007).

Dari sisi pendidikan dan literasi, pemerintah perlu menjalankan program literasi digital nasional yang fokus pada hak-hak hukum korban kejahatan siber. Edukasi publik harus menekankan tanggung jawab bersama antara negara, masyarakat, dan sektor swasta dalam menjaga keamanan digital dan menegakkan hak korban. Kerja sama internasional juga harus diperkuat. Indonesia dapat memperluas partisipasinya dalam *ASEAN Cybercrime Framework Agreement* dan menjajaki ratifikasi *Budapest Convention*. Kerja sama ini akan meningkatkan kapasitas penegakan hukum lintas batas dan mempercepat proses pemulihan korban di tingkat global. Dari perspektif hak asasi manusia, setiap korban kejahatan siber memiliki hak untuk memperoleh keadilan sebagaimana diatur dalam *Article 8 Universal Declaration of Human Rights* dan *Article 2(3) ICCPR*. Oleh karena itu, negara wajib menjamin mekanisme hukum yang efektif bagi korban untuk memperoleh perlindungan hukum korban harus mengedepankan prinsip non-discrimination dan gender sensitivity, terutama karena perempuan sering menjadi korban kekerasan berbasis gender online (KBGO). Penanganan harus sensitif terhadap kondisi sosial dan psikologis korban untuk menghindari trauma sekunder. Selain pidana, pendekatan keperdataan melalui gugatan kelompok (class action) penting, terutama dalam kasus kebocoran data massal. Sistem hukum harus adaptif terhadap perkembangan teknologi tanpa mengabaikan prinsip keadilan dan HAM, mencerminkan "*rule of law in the digital age.*" Selain reformasi hukum formal, pendekatan sosial dan etis juga dibutuhkan dengan membangun budaya empati dan tanggung jawab sosial di ruang digital, menjadikan etika digital dan penegakan hukum sebagai pondasi perlindungan korban yang berkelanjutan (R. Nugroho, 2020).

Upaya penguatan sistem hukum Indonesia juga harus melibatkan sektor swasta, terutama penyedia platform digital. Negara dapat mewajibkan mereka untuk membentuk unit *Cyber Incident Response Team (CIRT)* internal yang bekerja sama dengan aparat penegak hukum dalam memberikan perlindungan awal bagi korban (Wall, D. S. 2007). Dalam konteks globalisasi digital, Indonesia perlu mengembangkan kebijakan hukum siber yang selaras dengan prinsip-prinsip internasional namun tetap berakar pada nilai- nilai Pancasila dan keadilan sosial. Pendekatan *glocalization global principle, local adaptation* dapat menjadi strategi efektif untuk membangun sistem hukum siber yang berkeadilan. Evaluasi berkala terhadap efektivitas regulasi juga penting dilakukan. Pemerintah perlu membentuk *Cyber Law Review Committee* yang bertugas menilai kinerja penegakan hukum dan perlindungan korban setiap dua tahun sekali. Mekanisme ini memastikan hukum nasional selalu relevan dengan perkembangan kejahatan siber yang cepat berubah.

Dengan langkah-langkah tersebut, Indonesia dapat memperkuat fondasi perlindungan hukum bagi korban kejahatan siber sekaligus memenuhi komitmen

internasionalnya dalam menjamin hak asasi manusia di ruang digital. Hukum nasional harus menjadi instrumen keadilan yang adaptif, inklusif, dan berorientasi pada korban. Secara keseluruhan, kendala sistem hukum Indonesia dalam melindungi korban kejahatan siber bukanlah persoalan yang tidak dapat diatasi. Melalui pembaruan regulasi, peningkatan kapasitas kelembagaan, serta kerja sama internasional yang solid, Indonesia berpotensi menjadi negara yang tidak hanya mampu menindak pelaku kejahatan siber, tetapi juga memberikan perlindungan maksimal kepada setiap korban secara bermartabat dan berkeadilan.

SIMPULAN

Perlindungan hukum terhadap korban kejahatan siber di Indonesia masih belum optimal karena lemahnya sistem pemulihan dan keterbatasan kerja sama internasional. Meskipun Indonesia memiliki kerangka hukum seperti Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Saksi dan Korban, implementasinya belum sesuai dengan standar hukum internasional seperti yang diatur dalam Konvensi Budapest dan Deklarasi PBB 1985. Diperlukan harmonisasi regulasi nasional dengan prinsip hukum internasional serta peningkatan kapasitas aparat dan lembaga perlindungan korban agar perlindungan hukum di era digital dapat tercapai secara efektif.

DAFTAR RUJUKAN

Akinyemi, O., Sulaiman, R., & Abosata, N. (2023). *Analysis of the LockBit 3.0 and its infiltration into Advanced's infrastructure crippling NHS services*. arXiv.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2023). *Laporan Survei Internet Indonesia 2023*.

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan Keamanan Siber Indonesia 2024*. Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, (Jakarta: Kencana, 2008), hlm. 56.

Council of Europe, *Budapest Convention on Cybercrime* (2001).

Daly, K. (2007). *Victims of crime: Rights, powers, and justice*. New York, NY: Springer. *Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power 1985*

Europol, "*Internet Organized Crime Threat Assessment (IOCTA) 2023. General Data Protection Regulation* (GDPR).

Kharbanda, V. (2019, April 29). *International cooperation in cybercrime: The Budapest Convention*. Centre for Internet and Society.

L. Prasetyo, "Evaluasi Perlindungan Data Pribadi dalam Undang-Undang No. 27 Tahun 2022,"*Jurnal Ilmu Hukum*, Vol. 12, No. 1, 2023, hlm. 45-52.

LPSK, *Peran Lembaga Perlindungan Saksi dan Korban dalam Memberikan Perlindungan dan Pemulihan bagi Korban Tindak Pidana* (Jakarta: LPSK, 2022), hlm. 12–13.

M. Arsyad Sanusi, *Teknologi Informasi dan Hukum E-Commerce*, (Jakarta: PT Dian Rakyat, 2004), hlm. 78–80.

Polri (Polda Jambi). (2024, April 19). *Polda Jambi perkuat keahlian personel digital forensik siber*. ANTARA

Putra, D. K. (2021). *Implementasi Prinsip-prinsip Hukum Internasional dalam Perlindungan Korban Kejahatan Siber di Indonesia*. Jurnal Hukum Internasional, 17(3), 101-120.

R. Nugroho, *Cybercrime Law and Policy in Indonesia* (Springer 2020).

U.S. Department of Justice. (2020). *Cybercrime enforcement in the United States: Annual report*.

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang tentang Perlindungan Saksi dan Korban.

UNICEF Indonesia, "Perlindungan Anak dari Kejahatan Siber," UNICEF,

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge, UK: Polity Press.

World Economic Forum, "Global Cybersecurity Outlook 2025," *World Economic Forum Publications*, 2023.

