JURNAL ANALISIS HUKUM DAN KEBIJAKAN
Vol 7, No 2, Tahun 2026
https://ejurnals.com/ojs/index.php/jahk

PERLINDUNGAN HUKUM BAGI KORBAN KEJAHATAN SIBER DI INDONESIA

Lasyohana Situmorang[1]

[1]Universitas Pamulang

lasyohanas@gmail.com

ABSTRACT; *The massive development of information technology has opened up new opportunities for the emergence of various forms of digital-based crime known as cybercrime. Indonesia, as one of the countries with the largest internet users in Southeast Asia, has faced a significant surge in cybercrime cases over the past decade. This phenomenon raises important questions about the extent to which the Indonesian legal system is able to provide adequate protection for victims. This study aims to comprehensively analyze the forms of cybercrime and their impact on victims, examine the legal framework governing the protection of cybercrime victims in Indonesia, examine the mechanisms for protecting and restoring victims' rights, and identify obstacles and challenges faced in their implementation. The method used is normative legal research with statutory, conceptual, and comparative approaches. The results of the study indicate that although Indonesia has legal instruments such as Law Number 1 of 2024 concerning the Second Amendment to the Information Technology Law, protection for cybercrime victims remains partial and reactive. The mechanisms for restoring victims' rights are not optimal due to limited law enforcement capacity, minimal public digital education, and weak inter-institutional coordination. This article recommends the creation of a comprehensive cybercrime victim protection law, strengthening victim recovery institutions, and developing a more robust international cooperation framework.*

Keywords: *Cybercrime, Victim Protection, Cyber Law, Indonesia, Rights Restoration.*

ABSTRAK; Perkembangan teknologi informasi yang masif telah membuka peluang baru bagi munculnya berbagai bentuk kejahatan berbasis digital yang dikenal sebagai kejahatan siber. Indonesia, sebagai salah satu negara dengan pengguna internet terbesar di Asia Tenggara, telah menghadapi lonjakan signifikan kasus kejahatan siber selama dekade terakhir. Fenomena ini menimbulkan pertanyaan penting tentang sejauh mana sistem hukum Indonesia mampu memberikan perlindungan yang memadai bagi korban. Studi ini bertujuan untuk menganalisis secara komprehensif bentuk-bentuk kejahatan siber dan dampaknya terhadap korban, meneliti kerangka hukum yang mengatur perlindungan korban kejahatan siber di Indonesia, meneliti mekanisme perlindungan dan pemulihan hak-hak korban, dan mengidentifikasi hambatan dan tantangan yang dihadapi dalam implementasinya. Metode yang digunakan adalah penelitian hukum normatif

dengan pendekatan statutori, konseptual, dan komparatif. Hasil penelitian menunjukkan bahwa meskipun Indonesia memiliki instrumen hukum seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Undang-Undang Teknologi Informasi, perlindungan bagi korban kejahatan siber masih bersifat parsial dan reaktif. Mekanisme pemulihan hak-hak korban belum optimal karena keterbatasan kapasitas penegak hukum, minimnya pendidikan digital publik, dan lemahnya koordinasi antarlembaga. Artikel ini merekomendasikan pembentukan undang-undang perlindungan korban kejahatan siber yang komprehensif, penguatan lembaga pemulihan korban, dan pengembangan kerangka kerja kerja sama internasional yang lebih solid.

Kata Kunci: Kejahatan Siber, Perlindungan Korban, Hukum Siber, Indonesia, Pemulihan Hak.

PENDAHULUAN

Indonesia berada di persimpangan antara kemajuan teknologi digital yang mengesankan dan ancaman kejahatan siber yang semakin kompleks. Menurut data yang dikumpulkan oleh Badan Siber dan Kriptografi Nasional (BSSN), pada tahun 2022 saja, lebih dari 370 juta serangan siber tercatat menargetkan berbagai sektor strategis, mulai dari perbankan dan pemerintahan hingga infrastruktur publik (BSSN, 2023). Angka-angka ini bukan sekadar statistik; di baliknya terdapat ribuan korban individu—mengalami kerugian finansial, kerusakan reputasi, trauma psikologis, dan bahkan ancaman terhadap nyawa.

Munculnya kejahatan siber sebagai fenomena hukum tidak sepenuhnya diantisipasi oleh sistem hukum Indonesia, yang dibangun di atas paradigma kejahatan konvensional. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU TIK), yang kemudian diubah oleh Undang-Undang Nomor 19 Tahun 2016 dan yang terbaru oleh Undang-Undang Nomor 1 Tahun 2024, memang berupaya mengisi celah hukum ini. Namun, para ahli hukum percaya bahwa peraturan yang ada lebih berfokus pada penuntutan pelaku daripada pemulihan hak-hak korban (Siahaan, 2021). Orientasi retributif ini menciptakan kesenjangan yang signifikan dalam perlindungan bagi mereka yang paling dirugikan.

Dari perspektif akademis, penelitian tentang kejahatan siber di Indonesia telah berkembang pesat, tetapi sebagian besar masih berfokus pada aspek kriminal material, kriminologi digital, dan analisis pasal-pasal dalam Undang-Undang Teknologi Informasi

dan Komunikasi (ITE). Studi yang secara khusus meneliti dimensi perlindungan korban termasuk mekanisme pemulihan hak, kompensasi, dan dukungan psikososial dalam konteks kejahatan siber masih relatif terbatas (Mahardika & Putri, 2022).

Kesenjangan penelitian ini mendorong studi yang lebih mendalam dan holistik. Lebih spesifiknya, penelitian ini dirumuskan untuk menjawab empat pertanyaan utama: Pertama, bentuk-bentuk kejahatan siber apa yang lazim di Indonesia, dan bagaimana dampaknya terhadap korban? Kedua, bagaimana kerangka hukum Indonesia mengatur perlindungan korban kejahatan siber? Ketiga, mekanisme apa yang tersedia untuk melindungi dan memulihkan hak-hak korban? Keempat, hambatan dan tantangan apa yang dihadapi dalam menerapkan perlindungan tersebut? Dengan menjawab pertanyaan-pertanyaan ini, artikel ini diharapkan dapat memberikan kontribusi akademis yang berarti serta rekomendasi kebijakan yang dapat diimplementasikan secara praktis.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yang didefinisikan oleh Soekanto dan Mamudji (2015) sebagai penelitian yang menempatkan hukum sebagai sistem norma yang terstruktur secara hierarkis dan saling berinteraksi. Karakteristik utama dari pendekatan ini adalah ketergantungannya pada analisis materi hukum, bukan data empiris di lapangan. Metode ini dipilih berdasarkan pertimbangan bahwa masalah perlindungan korban kejahatan siber di Indonesia pada dasarnya adalah masalah normatif yang berkaitan dengan apa yang harus diatur, bagaimana peraturan yang ada diinterpretasikan, dan arah reformasi hukum.

Tiga pendekatan digunakan secara terintegrasi dalam penelitian ini. Pertama, pendekatan undang-undang, yang melibatkan tinjauan komprehensif terhadap semua peraturan hukum yang relevan, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU PPK) dan amandemennya, KUHP, UU Perlindungan Konsumen, UU Perlindungan Data Pribadi (UU PDP Nomor 27 Tahun 2022), berbagai peraturan pemerintah terkait, dan konvensi internasional yang diratifikasi oleh Indonesia. Kedua, pendekatan konseptual digunakan untuk membangun kerangka analitis teoretis dengan merujuk pada doktrin hukum yang dikembangkan dalam literatur akademis, khususnya di bidang viktimologi, hukum siber komparatif, dan keadilan restoratif. Ketiga, pendekatan komparatif menempatkan sistem hukum Indonesia dalam perspektif

komparatif dengan negara-negara yang dianggap lebih maju dalam memberikan perlindungan bagi korban kejahatan siber, seperti negara-negara anggota Uni Eropa dan Korea Selatan.

Materi hukum yang digunakan untuk analisis diklasifikasikan menjadi tiga kategori. Materi hukum primer meliputi undang-undang dan peraturan, keputusan pengadilan yang relevan, dan instrumen internasional. Materi hukum sekunder terdiri dari artikel jurnal ilmiah, buku teks hukum, laporan dari lembaga pemerintah dan LSM, dan hasil penelitian akademis yang relevan. Materi hukum tersier meliputi kamus hukum dan ensiklopedia. Semua materi hukum dianalisis menggunakan teknik interpretasi sistematis, teleologis, dan komparatif untuk menghasilkan kesimpulan yang koheren dan ilmiah.

HASIL DAN PEMBAHASAN

1. Bentuk-Bentuk Kejahatan Siber dan Dampaknya terhadap Korban

Lanskap kejahatan siber di Indonesia mencerminkan tren global sekaligus memiliki karakteristik lokal yang berbeda. Menurut data dari Direktorat Kejahatan Siber Badan Investigasi Kriminal Kepolisian Nasional Indonesia (Bareskrim Polri), beberapa modus kejahatan paling dominan dan memiliki dampak paling signifikan terhadap masyarakat (Bareskrim Polri, 2023). Penipuan daring menduduki peringkat teratas, dengan jumlah laporan meningkat setiap tahunnya.

Metode ini mencakup berbagai varian, mulai dari penipuan belanja daring yang menjanjikan produk tetapi gagal mengirimkan, hingga skema investasi berbasis aplikasi digital yang curang yang telah memengaruhi ratusan ribu korban.

Data dari Otoritas Jasa Keuangan (OJK) (2023) menunjukkan bahwa kerugian akibat penipuan investasi digital sepanjang tahun 2022 mencapai lebih dari Rp 10 triliun, dengan korban tersebar di seluruh provinsi. Yang membuat metode ini lebih berbahaya adalah kemampuannya untuk terus berkembang seiring tren teknologi, seperti memanfaatkan platform media sosial, aplikasi pesan instan, dan teknologi kecerdasan buatan untuk menciptakan persona palsu yang meyakinkan. Pencurian identitas dan pelanggaran data adalah bentuk kedua dari kejahatan siber, dengan dampak yang seringkali jangka panjang dan melampaui sekadar kerugian finansial. Kebocoran data di berbagai platform digital utama di Indonesia—termasuk pelanggaran data BPJS

Kesehatan tahun 2021 yang mengungkap data lebih dari 279 juta penduduk—menunjukkan kerentanan ekosistem digital nasional (Putra & Ramadan, 2022).

Data yang dicuri kemudian dapat disalahgunakan untuk berbagai tujuan kriminal, mulai dari pembukaan kredit tanpa izin dan penjualan data di dark web hingga penggunaan identitas korban sebagai instrumen untuk kejahatan lainnya. Korban pencurian identitas sering kali menghadapi proses pemulihan yang panjang, harus membuktikan bahwa tindakan yang dilakukan atas nama mereka dilakukan oleh pihak lain. Kekerasan berbasis gender daring (KDRT) dan pelecehan di ruang digital merupakan bentuk kejahatan siber yang dampaknya tidak dapat diukur hanya dalam hal keuangan. Komisi Nasional Anti Kekerasan Terhadap Perempuan (Komnas Perempuan) (2022) mencatat peningkatan sebesar 241% dalam kasus kekerasan berbasis gender daring antara tahun 2019 dan 2022, termasuk kasus berbagi gambar intim tanpa persetujuan (NCII), penguntitan siber, dan pelecehan siber.

Dampak psikologis yang diderita korban mayoritas di antaranya adalah Perempuan sangat serius, termasuk depresi klinis, gangguan stres pascatrauma (PTSD), dan dalam kasus ekstrem, melukai diri sendiri. Dimensi ini menunjukkan bahwa kejahatan siber bukan hanya masalah teknologi atau hukum, tetapi juga masalah kesetaraan gender dan kesehatan mental masyarakat. Ransomware dan serangan siber terhadap infrastruktur kritis merupakan ancaman yang dampaknya dapat menjangkau semua lapisan masyarakat secara bersamaan. Serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024, meskipun melampaui periode studi sebelumnya, menjadi pengingat yang jelas tentang kerentanan infrastruktur digital Indonesia. Dalam kategori ini, korban bukan hanya individu, tetapi juga lembaga negara dan masyarakat luas yang layanan publiknya bergantung pada sistem digital yang dikompromikan (Wahyudi dkk., 2023).

Phishing dan rekayasa sosial adalah bentuk kejahatan yang mengeksploitasi kelemahan manusia, bukan kelemahan sistem teknis. Pelaku memanipulasi korban agar secara sukarela menyerahkan informasi sensitif atau mentransfer dana dengan berpura-pura sebagai individu yang dapat dipercaya—seperti karyawan bank, petugas pajak, atau kerabat dalam keadaan darurat. Teknik-teknik ini semakin canggih, menggunakan kloning suara berbasis AI dan manipulasi video waktu nyata yang sulit dibedakan dari

komunikasi nyata (Kriswanto & Andriansyah, 2022). Dampak kejahatan siber terhadap korban bersifat multidimensional.

Secara finansial, kerugian langsung dapat mencapai ratusan juta hingga miliaran rupiah, terutama dalam kasus penipuan investasi dan pembobolan rekening bank. Namun, yang sering diabaikan adalah dampak tidak langsung, seperti biaya pemulihan, hilangnya produktivitas, dan penyusutan aset digital. Secara psikologis, Surip dkk. (2021) menemukan dalam penelitian mereka bahwa korban kejahatan siber mengalami tingkat kecemasan dan depresi yang sebanding dengan korban kejahatan konvensional serius, dengan tambahan dimensi rasa malu dan stigma sosial yang seringkali menghalangi mereka untuk melapor kepada pihak berwenang. Secara sosial, kejahatan siber dapat menghancurkan reputasi, merusak hubungan keluarga, dan mengisolasi korban dari jaringan sosial mereka.

2. Regulasi Hukum untuk Perlindungan Korban Kejahatan Siber di Indonesia

Kerangka hukum untuk melindungi korban kejahatan siber di Indonesia tersebar di berbagai instrumen hukum yang saling melengkapi, namun belum membentuk sistem yang benar-benar terintegrasi. Analisis instrumen hukum ini mengungkapkan baik pencapaian maupun kesenjangan yang masih perlu diatasi. UU Nomor 1 Tahun 2024 tentang Perubahan Kedua UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU TIK) merupakan landasan utama untuk mengatur kejahatan siber di Indonesia. Amandemen terbaru ini membawa beberapa perbaikan penting, termasuk penambahan ketentuan tentang perlindungan anak di ruang digital, penguatan sanksi atas penyalahgunaan data pribadi, dan klarifikasi ketentuan yang sebelumnya dianggap terbuka untuk berbagai interpretasi.

Namun, dari perspektif perlindungan korban, UU TIK pada dasarnya masih terbatas: peraturannya masih didominasi oleh ketentuan pidana yang berfokus pada penghukuman pelaku, sementara mekanisme restitusi dan kompensasi bagi korban masih kurang proporsional (Siahaan, 2021). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PPN) merupakan terobosan legislatif yang telah lama ditunggu dan signifikan. Sebelum undang-undang ini, perlindungan data pribadi tersebar di berbagai peraturan sektoral yang tidak konsisten. UU PPN mengadopsi pendekatan yang terinspirasi oleh Peraturan Perlindungan Data Umum (GDPR) Uni Eropa, yang

mewajibkan pengontrol dan pengolah data untuk menerapkan standar keamanan teknis dan organisasi yang memadai, dan memberikan hak kepada subjek data untuk mengakses, memperbaiki, dan bahkan menghapus data pribadi mereka.

Relevansinya terhadap perlindungan korban kejahatan siber sangat signifikan: dalam kasus pelanggaran data, UU PPN memberikan dasar hukum bagi korban untuk meminta pertanggungjawaban pengontrol data dan berpotensi mendapatkan kompensasi atas kerugian yang diderita (Fauzia, 2021). Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban, sebagaimana diubah oleh Undang-Undang Nomor 31 Tahun 2014 (UU PSK), pada prinsipnya, memberikan kerangka kerja umum bagi korban kejahatan. Lembaga Perlindungan Saksi dan Korban (LPSK), yang dibentuk berdasarkan undang-undang ini, diamanatkan untuk memberikan perlindungan fisik, bantuan hukum, rehabilitasi psikologis, dan restitusi kepada korban kejahatan. Masalahnya adalah bahwa Undang-Undang LPSK tidak secara eksplisit menyebutkan korban kejahatan siber sebagai kategori yang menerima perlindungan khusus, sehingga akses mereka ke layanan LPSK seringkali bergantung pada interpretasi petugas dan belum diinstitusionalisasi secara sistematis. (Prasetyo& Wibowo, 2021).

KUHP baru UU Nomor 1 Tahun 2023, yang akan mulai berlaku pada tahun 2026 memberikan kontribusi signifikan dengan memperluas hukuman pidana untuk mencakup berbagai bentuk kejahatan berbasis teknologi. Namun, fokusnya tetap pada hukuman, bukan pemulihan korban. Sementara itu, KUHP, yang mengatur prosedur pidana, belum cukup mengakomodasi spesifik proses pembuktian dalam kasus kejahatan siber, termasuk standar untuk penerimaan bukti forensik digital. Secara internasional, Indonesia belum meratifikasi Konvensi Budapest tentang Kejahatan Siber, perjanjian internasional paling komprehensif di bidang ini. Ketidakhadiran ini membatasi kemampuan Indonesia untuk berpartisipasi dalam kerangka kerja kerja sama internasional yang ditetapkan oleh konvensi tersebut, termasuk akses ke mekanisme bantuan hukum timbal balik (MLA), yang lebih efektif dalam mengejar pelaku kejahatan siber lintas batas (Wahyudi dkk., 2023). Status Indonesia sebagai negara non-pihak menciptakan kesenjangan serius dalam menangani kejahatan siber transnasional.

Secara keseluruhan, kerangka hukum Indonesia untuk melindungi korban kejahatan siber ditandai dengan fragmentasi regulasi, penekanan yang kuat pada penuntutan

daripada ganti rugi, dan kelemahan dalam kerja sama internasional. Situasi ini menunjukkan bahwa sistem hukum Indonesia berada dalam fase transisi—telah mulai bergerak menuju perlindungan korban yang lebih besar, tetapi belum mencapai kohesi dan kelengkapan yang diperlukan.

3. Mechanism for Protection and Restoration of Victims' Rights

Mekanisme perlindungan dan pemulihan hak-hak korban kejahatan siber di Indonesia dapat dianalisis melalui tiga saluran utama: sistem peradilan pidana, litigasi perdata, dan mekanisme non-litigasi. Sistem peradilan pidana merupakan mekanisme yang paling umum digunakan oleh korban kejahatan siber. Proses ini dimulai dengan pelaporan kepada unit siber kepolisian—yang ditangani di tingkat pusat oleh Direktorat Kejahatan Siber (Ditipidsiber) Badan Kriminal (Bareskrim Polri), sedangkan di tingkat regional ditangani oleh unit-unit di Polda dan Polres.

Dalam kerangka ini, korban bertindak sebagai pelapor atau saksi, dan hak-hak mereka sebagai korban secara teoritis dilindungi melalui ketentuan-ketentuan dalam KUHP (Kitab Hukum Acara Pidana), yang mengatur hak atas informasi tentang perkembangan kasus, hak atas restitusi yang dapat diminta dari hakim dalam putusan, dan hak atas kompensasi yang ditanggung oleh negara dalam kondisi tertentu melalui LPSK (Lembaga Penanggulangan Hukum). Namun, dalam praktiknya, Mahardika dan Putri (2022) menemukan bahwa pemberian restitusi dalam kasus kejahatan siber masih sangat jarang, sebagian karena hakim tidak memiliki pedoman yang jelas tentang cara menghitung kerugian non-materiil dalam kejahatan digital. Litigasi perdata memberikan alternatif bagi korban yang ingin mencari kompensasi langsung dari pelaku atau pihak ketiga yang bertanggung jawab. Dasar hukumnya adalah Pasal 1365 KUHP tentang perbuatan melawan hukum (onrechtmatigedaad), yang dapat digunakan untuk meminta pertanggungjawaban baik pelaku kejahatan siber maupun platform digital atas kelalaian dalam mengamankan data pengguna. Gugatan perdata berdasarkan

Undang-Undang Privasi dan Perlindungan Data (PDP) memberikan dasar yang lebih spesifik, khususnya terhadap pengontrol data yang gagal mencegah kebocoran data pribadi. Namun, litigasi perdata menghadirkan hambatan praktis yang signifikan: biaya litigasi yang tinggi, kesulitan dalam mengidentifikasi dan melacak pelaku, yang seringkali anonim, dan proses pengadilan yang Panjang yang dapat berlangsung selama

bertahun-tahun sementara kerugian korban terus berlanjut (Fauzia, 2021). Mekanisme non-litigasi mencakup berbagai saluran alternatif yang semakin penting. LPSK (Lembaga Sosial Berskala Waskita Karya) menyediakan layanan komprehensif bagi korban yang memenuhi syarat, termasuk perlindungan fisik dan psikologis, bantuan medis, perwakilan hukum, dan fasilitasi restitusi. Ombudsman Indonesia dapat menerima pengaduan terkait malpraktik dalam pelayanan publik yang berkaitan dengan insiden siber.

Otoritas Jasa Keuangan (OJK) memiliki mekanisme pengaduan dan perlindungan konsumen khusus untuk kasus kejahatan siber di sektor keuangan, termasuk mekanisme pemblokiran akun yang digunakan dalam penipuan. Kementerian Komunikasi dan Informatika (Kemenkominfo) memiliki kewenangan untuk memblokir konten dan situs web yang digunakan dalam kejahatan siber, meskipun efektivitasnya dalam menegakkan hak korban masih terbatas (Putra & Ramadhan, 2022). Perlindungan khusus bagi korban kekerasan berbasis gender (KDRT) telah mendapat perhatian khusus melalui kehadiran Komisi Nasional Anti Kekerasan

Terhadap Perempuan (Komnas Perempuan) dan unit khusus untuk menangani KDRT berbasis gender di berbagai lembaga negara. Undang-Undang Pidana Kekerasan Seksual (TPKS) Nomor 12 Tahun 2022 memberikan terobosan signifikan dengan mengkriminalisasi penyebaran konten intim tanpa persetujuan dan menetapkan hak-hak korban yang lebih komprehensif, termasuk hak atas dukungan psikologis dan hak anonimitas di media (Komnas Perempuan, 2022). Hal ini merupakan salah satu kemajuan legislatif paling signifikan dalam melindungi korban KDRT berbasis gender di Indonesia.

Analisis perbandingan dengan praktik di negara lain menunjukkan bahwa jalan yang harus ditempuh Indonesia masih panjang. Korea Selatan, misalnya, telah menetapkan sistem kompensasi korban kejahatan siber yang terintegrasi dengan sistem jaminan sosial nasionalnya, sehingga korban tidak perlu lagi menunggu putusan pidana untuk menerima bantuan keuangan awal (Leukfeldt dkk., 2022). Negara-negara anggota Uni Eropa, melalui GDPR, telah menerapkan sistem denda administratif, dengan sebagian dari hasil denda dialokasikan untuk merehabilitasi korban pelanggaran data. Model-model ini layak dipertimbangkan sebagai referensi untuk reformasi hukum di Indonesia.

4. Obstacles and Challenges in Protecting Cybercrime Victims

Mengidentifikasi hambatan dan tantangan dalam melindungi korban kejahatan siber di Indonesia memerlukan analisis yang melampaui teks hukum dan peraturan. Hambatan yang ada bersifat multidimensional, meliputi kapasitas kelembagaan, literasi digital, koordinasi antar lembaga, dan dimensi geopolitik-internasional. Dalam hal kapasitas kelembagaan penegakan hukum, kesenjangan antara volume kasus dan kapasitas penanganan masih sangat mencolok. Jumlah penyidik dengan keahlian forensik digital masih sangat terbatas, terutama di tingkat kepolisian dan kepolisian daerah di luar Jawa. Prasetyo dan Wibowo (2021) mencatat bahwa di beberapa daerah, laporan kasus kejahatan siber bahkan ditolak karena kurangnya penyidik yang mampu menangani kasus tersebut. Situasi ini menciptakan "zona mati" dalam sistem perlindungan korban, di mana korban di daerah terpencil hampir tidak memiliki akses ke mekanisme perlindungan dibandingkan dengan korban di kota-kota besar.

Masalah pembuktian dalam kasus kejahatan siber juga menimbulkan tantangan hukum prosedural yang signifikan. Bukti digital—seperti log server, catatan transaksi digital, metadata file, dan tangkapan layar—memiliki karakteristik yang berbeda dari bukti konvensional: mudah dimanipulasi, mudah dihapus, dan sering disimpan di server yang berlokasi di yurisdiksi asing. Kitab Undang-Undang Hukum Acara Pidana (KUHP) yang ada tidak memberikan panduan yang memadai tentang standar pengumpulan, penyimpanan, dan penyajian bukti digital di pengadilan. Akibatnya, banyak kasus ditolak pada tahap penuntutan karena masalah dengan penerimaan bukti, sehingga korban tidak mendapatkan keadilan (Wahyudi dkk., 2023).

Rendahnya tingkat pelaporan oleh korban merupakan fenomena yang dikenal dalam kriminologi sebagai "angka gelap kejahatan"—kesenjangan antara kejahatan aktual dan kejahatan yang dilaporkan kepada pihak berwenang. Dalam konteks kejahatan siber, fenomena ini bahkan lebih parah daripada kejahatan konvensional. Survei yang dilakukan oleh Badan Nasional Kejahatan Siber dan Kejahatan Siber (BSSN) (2023) menunjukkan bahwa hanya sekitar 12–15% korban kejahatan siber yang melaporkan kasus mereka. Berbagai faktor berkontribusi pada rendahnya tingkat pelaporan ini: kurangnya kepercayaan korban bahwa laporan mereka akan ditindaklanjuti secara efektif, rasa malu, terutama dalam kasus kekerasan berbasis gender (OGBV), ketidakpahaman terhadap

prosedur pelaporan, dan persepsi bahwa kerugian yang diderita terlalu kecil untuk ditindaklanjuti melalui proses hukum yang panjang. Dimensi transnasional kejahatan siber menciptakan tantangan yurisdiksi yang sangat kompleks.

Para pelaku kejahatan siber sering beroperasi dari negara lain, menggunakan server yang berlokasi di yurisdiksi pihak ketiga, dan melancarkan serangan melalui jaringan komputer yang membentang di berbagai benua. Dalam situasi seperti itu, kemampuan Indonesia untuk menuntut pelaku, menyita aset, dan memulihkan kerugian korban sangat bergantung pada mekanisme kerja sama internasional. Namun, seperti yang disebutkan, Indonesia belum meratifikasi Konvensi Budapest, dan perjanjian bilateral MLA yang ada tidak mencakup semua negara tempat operasi kejahatan siber berbasis (Mahardika & Putri, 2022).

Literasi digital publik yang rendah merupakan tantangan struktural yang memperburuk kerentanan terhadap kejahatan siber dan menyulitkan korban untuk mengakses mekanisme perlindungan yang ada. Data dari Kementerian Komunikasi dan Informatika (Kominfo) (2022) menunjukkan bahwa indeks literasi digital Indonesia tetap berada di angka 3,54 pada skala 5, dengan perbedaan yang signifikan antara kelompok usia muda dan tua, serta antara daerah perkotaan dan pedesaan. Korban dengan literasi digital rendah seringkali tidak menyadari bahwa mereka telah menjadi korban kejahatan, tidak mengetahui saluran pelaporan yang tersedia, dan tidak memahami hak-hak hukum mereka.

Fragmentasi kelembagaan dalam menangani kejahatan siber juga merupakan hambatan serius. Saat ini, setidaknya delapan lembaga pemerintah memiliki kewenangan yang tumpang tindih dengan kejahatan siber, mulai dari Kepolisian Nasional (Polri), Kejaksaan Agung (Kemenkominfo), Badan Nasional Perlindungan Perempuan (BSSN), Otoritas Jasa Keuangan (OJK), Badan Perlindungan Saksi dan Korban (LPSK), Komisi Nasional Kekerasan Terhadap Perempuan (Komnas Perempuan), hingga Badan Nasional Perlindungan Perempuan (BPKN). Fragmentasi ini menciptakan risiko tumpang tindih kewenangan, kesenjangan koordinasi, dan kebingungan di antara korban tentang lembaga mana yang harus dihubungi untuk mengajukan pengaduan.

Tidak adanya satu lembaga tunggal yang berfungsi sebagai "titik masuk" bagi korban kejahatan siber mempersulit akses keadilan, terutama bagi korban yang rentan.

(Surip dkk.,2021). Dari perspektif ekonomi politik, alokasi anggaran untuk pengembangan kapasitas siber Indonesia masih jauh dari memadai dibandingkan dengan skala ancaman yang dihadapinya. Penelitian oleh Leukfeldt dkk. (2022) menunjukkan korelasi yang kuat antara jumlah investasi negara dalam kapasitas siber dan efektivitas perlindungan korban. Indonesia perlu meningkatkan secara signifikan anggarannya untuk pelatihan penyelidik siber, pengembangan infrastruktur forensik digital, dan program dukungan korban jika ingin membangun sistem perlindungan yang benar-benar efektif.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan analisis komprehensif yang dilakukan, studi ini menghasilkan beberapa kesimpulan utama. Pertama, kejahatan siber di Indonesia telah berkembang menjadi ancaman multidimensi, yang dampaknya meluas melampaui aspek finansial hingga psikologis, sosial, dan bahkan politik. Keragaman sifat kejahatan ini, mulai dari penipuan daring dan pencurian identitas hingga kekerasan berbasis gender di ruang digital, hingga serangan ransomware, mencerminkan kemampuan adaptasi kejahatan ini terhadap perkembangan teknologi yang terus berubah.

Kedua, kerangka hukum Indonesia untuk melindungi korban kejahatan siber masih terfragmentasi dan belum membentuk sistem yang terpadu dan kohesif. Meskipun terdapat beberapa instrumen penting, seperti Undang-Undang Teknologi Informasi dan Komunikasi (ITE) yang telah dua kali diubah, Undang-Undang Perlindungan Data Pribadi (PDP), dan Undang-Undang Keamanan Publik (TPKS), peraturan-peraturan ini masih lebih berfokus pada penuntutan pelaku daripada rehabilitasi dan pemberdayaan korban.

Ketiga, mekanisme yang tersedia untuk perlindungan dan pemulihan hak-hak korban, baik melalui jalur pidana, perdata, atau non-litigasi, belum berfungsi secara optimal. Hambatan struktural, seperti keterbatasan kapasitas penegakan hukum, kesulitan dalam memperoleh bukti digital, tingkat pelaporan yang rendah, dan fragmentasi kelembagaan, secara kolektif menciptakan situasi di mana sebagian besar korban kejahatan siber tidak mendapatkan keadilan dan ganti rugi yang layak mereka terima.

Keempat, tantangan kejahatan siber transnasional, yang diperburuk oleh tidak diratifikasinya Konvensi Budapest dan kerangka kerja sama internasional yang terbatas,

menciptakan titik buta yang serius dalam kemampuan Indonesia untuk melindungi warganya dari kejahatan siber lintas batas.

Saran

Berdasarkan kesimpulan di atas, studi ini mengusulkan beberapa rekomendasi kebijakan praktis dan dapat segera ditindaklanjuti. Pertama, Indonesia perlu segera menyusun undang-undang yang komprehensif dan spesifik tentang perlindungan korban kejahatan siber, yang secara eksplisit mengatur hak-hak korban, mekanisme kompensasi, prosedur pemulihan, dan standar layanan dukungan korban. Undang-undang ini idealnya harus mengadopsi pendekatan "berpusat pada korban" yang menempatkan pemulihan korban sebagai prioritas utama sistem peradilan.

Kedua, pemerintah perlu memperkuat kapasitas kelembagaan lembaga penegak hukum di seluruh Indonesia, termasuk meningkatkan jumlah dan kualitas penyelidik forensik digital, berinvestasi dalam infrastruktur laboratorium digital, dan mengembangkan pedoman teknis yang komprehensif untuk bukti digital. Kesenjangan kapasitas antara pemerintah pusat dan daerah harus diatasi sebagai prioritas kebijakan.

Ketiga, pembentukan lembaga tunggal yang berfungsi sebagai "pusat layanan terpadu" bagi korban kejahatan siber perlu segera dipertimbangkan. Lembaga ini dapat

berbentuk Pusat Perlindungan Korban Kejahatan Siber Nasional yang mengintegrasikan layanan pelaporan, bantuan hukum, dukungan psikologis, bantuan keuangan awal, dan pemantauan tindak lanjut kasus.

Keempat, proses ratifikasi Konvensi Budapest harus dipercepat dengan mempertimbangkan opsi aksesi dengan reservasi terkait pasal-pasal yang berpotensi bertentangan dengan kepentingan nasional. Secara bersamaan, Indonesia perlu secara aktif memperluas jaringan perjanjian MLA bilateralnya, khususnya dengan negara-negara yang berfungsi sebagai basis operasi bagi kelompok kejahatan siber yang menargetkan Indonesia. Kelima, program literasi digital nasional perlu ditingkatkan secara signifikan, dengan fokus khusus pada pendidikan tentang keamanan siber, pengenalan metode kejahatan siber, dan pemahaman hak-hak korban dan prosedur pelaporan. Program ini harus dirancang dengan mempertimbangkan beragam karakteristik demografis dan geografis penduduk Indonesia.

DAFTAR PUSTAKA

Gosita, A. (1993). Masalah Korban Kejahatan. Jakarta: AkademikaPressindo.

Hamzah, A. (2005). Hukum Acara Pidana Indonesia (edisirevisi). Jakarta: Sinar Grafika.

Maskun. (2013). Kejahatan Siber (Cyber Crime): SuatuPengantar Jakarta: Kencana Prenadamedia Group.

Soekanto, S., &Mamudji, S. (2015). Penelitian Hukum Normatif: SuatuTinjauan Singkat. Jakarta: RajaGrafindo Persada.

Wahid, A., & Irfan, M. (2001). Perlindunganterhadap Korban KekerasanSeksual: Advokasiatas Hak Asasi Perempuan. Bandung: Refika Aditama.

Zehr, H. (2002). The Little Book of Restorative Justice. Intercourse: Good Books

Fauzia, A. (2021). Perlindungan Data Pribadisebagai Bagian dari Hak AsasiManusiaatasPrivasi di Indonesia. JurnalKonstitusi, 18(4), 796–817. https://doi.org/10.31078/jk1845

Kriswanto, A., & Andriansyah, M. (2022). Evolusi Modus Cybercrime di Era KecerdasanBuatan: Tantangan Hukum dan Regulasi. Jurnal Hukum Ius Quia Iustum, 29(2), 310–335. https://doi.org/10.20885/iustum.vol29.iss2.art4

Leukfeldt, E. R., Kleemans, E. R., &Stol, W. P. (2022). Cybercrime, Victims, and the State: A Comparative Analysis of National Responses. International Journal of Cybersecurity, 14(3), 88–112. https://doi.org/10.1080/19439684.2022.2041893

Mahardika, R., & Putri, A. R. (2022). ProblematikaMekanismeRestitusibagi Korban Kejahatan Siber Finansial di Indonesia. Jurnal Hukum dan Peradilan, 11(1), 45–68. https://doi.org/10.25216/jhp.11.1.2022.45-68

Prasetyo, B., & Wibowo, A. (2021). ImplementasiUndang-Undang ITE dalamPerlindungan Korban Kejahatan Siber: Studi pada Lima Polda di Indonesia. Masalah-Masalah Hukum, 50(2), 195–210. https://doi.org/10.14710/mmh.50.2.2021.195-210

Putra, M. H., & Ramadhan, F. (2022). Kebocoran Data Pribadi di Indonesia: AnalisisYuridis dan Implikasi bagiPerlindungan Korban. JurnalIlmu Hukum TambunBungai, 7(1), 67–

90. https://doi.org/10.37304/jihtb.v7i1.3892

Siahaan, R. (2021). OrientasiPerlindungan Korban dalamUndang-UndangInformasi dan Transaksi Elektronik: Kajian Kritis. Jurnal Hukum dan Pembangunan, 51(3), 674–695. https://doi.org/10.21143/jhp.vol51.no3.3115

Surip, N., Nuraini, S., & Hartono, B. (2021). DampakPsikologis Cybercrime terhadap Korban:
PerspektifViktimologi dan Kesehatan Mental. JurnalPsikologi dan Kesehatan, 9(2), 112–128. https://doi.org/10.35814/jpk.v9i2.2241

Wahyudi, A., Pratama, D. I., & Santoso, T. (2023). KerentananInfrastruktur Digital Indonesia
terhadapAncaman Ransomware: Analisis Hukum dan Kebijakan. JurnalKeamanan Nasional, 9(1), 1–22. https://doi.org/10.31599/jkn.v9i1.1823

Undang-UndangNomor 11 Tahun 2008 tentangInformasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58).

Undang-UndangNomor 19 Tahun 2016 tentangPerubahan Atas Undang- Undang Nomor 11 Tahun 2008 tentangInformasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251).

Undang-UndangNomor 1 Tahun 2024 tentangPerubahanKedua Atas Undang- Undang Nomor 11 Tahun 2008 tentangInformasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1).

Undang-UndangNomor 27 Tahun 2022 tentangPerlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196).

Undang-UndangNomor 12 Tahun 2022 tentang TindakP idana Kekerasan Seksual (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 120).

Undang-UndangNomor 31 Tahun 2014 tentangPerlindungan Saksi dan Korban (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 293).

Undang-UndangNomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1)..