Jurnal Hukum, Administrasi Publik dan Negara
Volume. 3, Nomor. 4 Juli 2026
e-ISSN: 3063-7864; p-ISSN: 3063-7872, Hal. 22-32
DOI: https://doi.org/10.62383/hukum.v3i4.1109
Tersedia: https://ejournal.appisi.or.id/index.php/hukum

Dampak Psikologis dan Sosial Serta Perlindungan Korban Kejahatan Siber dalam Perspektif Viktimologi

Kadek Dwi Ayu Lestari[1*], Ni Ketut Sari Adnyani[2], I Putu Dwika Ariestu[3]
[1-3]Ilmu Hukum, Universitas Pendidikan Ganesha, Indonesia
**Penulis Korespondensi: dwi.ayu.lestari.2@student.undiksha.ac.id*

Abstract*. Rapid advancements in information and communication technology have fueled a rise in cybercrime in Indonesia. These crimes not only result in material losses but also have psychological and social impacts on victims. This study aims to analyze the psychological and social effects experienced by victims of cybercrime and to examine this phenomenon from a victimological perspective. The method used is normative legal research with a legislative and conceptual approach. Data were collected through a literature review covering legislation, books, and scientific journals related to victimology and cybercrime. The results of the study indicate that victims of cybercrime often experience psychological impacts such as anxiety, fear, stress, trauma, and a decline in self-confidence. Additionally, they face social impacts including feelings of shame, reduced social interaction, and stigma from their surroundings. From a victimology perspective, it is crucial for victims of cybercrime to receive greater attention through legal protection, social support, and psychological recovery efforts. Therefore, more comprehensive measures are needed from the government and society to provide protection and recovery for victims of cybercrime in Indonesia.*

Keywords*: Cybercrime; Psychological Impact; Social Impact; Victim Protection; Victimology.*

Abstrak. Perkembangan pesat dalam teknologi informasi dan komunikasi telah memicu peningkatan kejahatan siber di Indonesia. Kejahatan ini tidak hanya menyebabkan kerugian materiil, tetapi juga berdampak psikologis dan sosial pada korban. Penelitian ini bertujuan untuk menganalisis efek psikologis dan sosial yang dialami korban kejahatan siber serta mengkaji fenomena ini dari sudut pandang viktimologi. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual. Data dikumpulkan melalui studi pustaka yang mencakup peraturan perundang-undangan, buku, dan jurnal ilmiah terkait viktimologi dan kejahatan siber. Hasil penelitian menunjukkan bahwa korban kejahatan siber sering mengalami dampak psikologis berupa kecemasan, ketakutan, stres, trauma, serta penurunan rasa percaya diri. Selain itu, mereka juga menghadapi dampak sosial yang meliputi rasa malu, berkurangnya interaksi sosial, dan stigma dari lingkungan sekitar. Dalam perspektif viktimologi, sangat penting bagi korban kejahatan siber untuk mendapatkan perhatian lebih melalui perlindungan hukum, dukungan sosial, dan upaya pemulihan psikologis. Oleh karena itu, diperlukan langkah-langkah yang lebih komprehensif dari pemerintah dan masyarakat untuk memberikan perlindungan dan pemulihan bagi korban kejahatan siber di Indonesia.

Kata Kunci: Dampak Psikologis; Dampak Sosial; Kejahatan Siber; Perlindungan Korban; Viktimologi.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengubah berbagai aspek kehidupan masyarakat, di mana aktivitas yang dulunya dilakukan secara langsung kini dapat diakses melalui perangkat digital seperti *smartphone*, laptop, dan jaringan internet. Kemudahan akses informasi dan komunikasi tanpa batas jarak dan waktu ini membawa manfaat besar, namun di sisi lain juga memunculkan dampak negatif berupa penyalahgunaan teknologi yang mengarah pada kejahatan siber. Kejahatan siber terus berkembang seiring meningkatnya penggunaan teknologi digital dalam kegiatan seperti *email*, perbankan *online*, dan *e-commerce*, yang memberikan peluang bagi pelaku untuk melakukan tindakan ilegal melalui jaringan global, sehingga kejahatan ini tidak terbatas pada satu wilayah tetapi dapat melampaui batas negara dan menyebabkan kerugian serta dampak serius bagi para

Naskah Masuk: 18 April 2026; Revisi: 19 Mei 2026; Diterima: 30 Juni 2026; Terbit: 04 Juli 2026

korban (Widianingrum, 2024). Munculnya kejahatan siber dipengaruhi oleh celah keamanan sistem yang dimanfaatkan pelaku, yang dapat muncul dalam berbagai bentuk seperti peretasan, pencurian data pribadi, penipuan daring, hingga pengubahan data digital yang merugikan individu maupun organisasi. Kejahatan ini sering dilakukan dengan memanfaatkan kelemahan jaringan internet, kurangnya perlindungan sistem, rendahnya kesadaran pengguna akan perlindungan data pribadi, serta sifat anonimitas dunia maya yang memudahkan pelaku menyembunyikan identitas dan menghindari pengawasan aparat penegak hukum. Perkembangan teknik dan metode pelaku yang semakin kompleks menunjukkan bahwa kejahatan siber tidak hanya bertambah dalam jumlah, tetapi juga dalam kualitas dan variasi cara operasinya, sehingga semakin sulit untuk diidentifikasi dan diatasi (Kafiar, 2026).

Di tengah kemajuan kejahatan siber, pengguna teknologi digital berada pada posisi rentan terhadap berbagai serangan seperti pencurian identitas, penipuan daring, peretasan akun, dan penyalahgunaan informasi pribadi yang dapat mengakibatkan kerugian finansial serta tekanan mental seperti rasa takut, kecemasan, stres, bahkan masalah dalam interaksi sosial akibat hilangnya kepercayaan terhadap dunia maya dan orang lain. Fenomena ini menunjukkan bahwa kejahatan siber tidak hanya berdampak pada aspek keamanan teknologi, tetapi juga menyebabkan dampak serius pada kesehatan psikologis dan sosial para korban (Barus, 2026). Berdasarkan berbagai akibat yang timbul, diperlukan strategi yang tidak hanya berfokus pada pelaku kriminal tetapi juga memberikan perhatian lebih pada korban. Kajian viktimologi menjadi krusial karena menyajikan perspektif yang menjadikan korban sebagai titik fokus untuk memahami tindakan kriminal, termasuk dalam konteks kejahatan siber. Viktimologi tidak hanya menyoroti kerugian yang dialami korban, tetapi juga menyelidiki pengaruh psikologis dan sosial seperti trauma, rasa ketidakamanan, serta penurunan rasa percaya diri dan interaksi sosial.

Dengan pendekatan ini, dapat teridentifikasi kebutuhan korban terkait perlindungan, pemulihan, dan pemenuhan hak-hak mereka selama proses penanganan kejahatan, sehingga mendorong lembaga penegak hukum agar lebih responsif dan berfokus pada kepentingan korban untuk memberikan keadilan yang lebih komprehensif (Barus, 2026). Berdasarkan uraian tersebut, rumusan masalah dalam penelitian ini adalah: (1) Bagaimana bentuk kejahatan siber yang berkembang di masyarakat? dan (2) Bagaimana dampak dan perlindungan terhadap korban dalam perspektif viktimologi?. Penelitian ini bertujuan untuk menganalisis bentuk kejahatan siber yang berkembang di masyarakat serta mengkaji dampak dan perlindungan terhadap korban dalam perspektif viktimologi. Manfaat penelitian ini diharapkan dapat memberikan kontribusi secara teoritis dalam pengembangan ilmu viktimologi serta secara

praktis menjadi bahan pertimbangan bagi aparat penegak hukum dalam meningkatkan perlindungan terhadap korban kejahatan siber.

2. KAJIAN TEORITIS

Perspektif Viktimologi dalam Kejahatan Siber

Kejahatan siber atau *cybercrime* didefinisikan sebagai tindak ilegal yang dilakukan melalui perangkat digital dan jaringan internet, yang dapat menargetkan sistem komputer, data pribadi, hingga infrastruktur digital suatu negara. Sifat kejahatan ini yang lintas batas dan sulit dideteksi menjadikannya tantangan global yang serius dalam penegakan hukum modern, karena perkembangan teknologi digital yang pesat tidak selalu diimbangi dengan sistem hukum yang adaptif, sehingga menciptakan celah yang dimanfaatkan oleh pelaku kejahatan untuk melancarkan aksinya. Kejahatan siber hadir dalam berbagai bentuk tindakan melanggar hukum, antara lain peretasan sistem (*hacking*), pencurian identitas, penipuan daring (*online fraud*), pemerasan digital (*sextortion*), *doxing* atau penyebaran data pribadi secara ilegal, hingga penyebaran konten pornografi dan ujaran kebencian. Modus operandi pelaku terus berkembang seiring dengan kemajuan teknologi, menandakan peningkatan tidak hanya dalam kuantitas tetapi juga kompleksitas dan variasi cara kejahatan, sehingga membutuhkan pemahaman yang mendalam dari berbagai sudut pandang keilmuan, termasuk viktimologi

Selanjutnya Viktimologi merupakan cabang ilmu kriminologi yang menjadikan korban sebagai titik fokus untuk memahami tindakan kriminal, termasuk dalam konteks kejahatan siber, di mana pendekatan ini tidak hanya menyoroti kerugian yang dialami korban tetapi juga menyelidiki pengaruh psikologis dan sosial yang dihadapi, seperti trauma, rasa ketidakamanan, serta penurunan rasa percaya diri dan interaksi sosial (Ahmad, 2025). Dalam perspektif viktimologi, korban kejahatan siber sering dikategorikan sebagai *non-participating victims*, di mana mereka tidak terlibat langsung dalam kejadian, melainkan menjadi sasaran akibat kelalaian pihak ketiga seperti penyelenggara sistem elektronik atau rendahnya kesadaran pengguna akan pentingnya perlindungan data pribadi, sehingga tipologi ini penting untuk memahami bahwa korban sering kali tidak memiliki andil dalam terjadinya kejahatan dan karenanya sistem perlindungan hukum perlu memberikan perhatian khusus (wibowo, 2025). Salah satu konsep penting dalam viktimologi kontemporer adalah viktimisasi berlapis (*multiple victimization*), yakni kondisi ketika seseorang menjadi korban baik di dunia fisik maupun dunia digital secara bersamaan atau berkelanjutan, yang menjadi semakin relevan seiring dengan meningkatnya perundungan siber (cyberbullying) yang sering kali merupakan kelanjutan dari perundungan di dunia nyata. Viktimisasi berlapis berdampak lebih berat bagi korban karena

mereka kehilangan ruang aman di dua dunia sekaligus dunia fisik yang dapat mereka lihat dan dunia maya yang sulit mereka kendalikan dan dalam kajian viktimologi, kondisi ini disebut sebagai *secondary victimization*, yaitu situasi ketika korban kembali mengalami luka emosional akibat eksposur berulang terhadap materi yang merugikan diri mereka sendiri.

Kerentanan korban dalam kejahatan siber tidak hanya ditentukan oleh faktor pribadi, tetapi juga struktur sosial, lingkungan, dan teknologi yang memfasilitasi kejahatan, di mana beberapa faktor yang meningkatkan kerentanan individu menjadi korban antara lain rendahnya literasi digital yang menyebabkan banyak pengguna internet belum mampu membedakan informasi asli dan penipuan serta belum memahami pentingnya menjaga data sensitif seperti OTP, PIN, atau kata sandi (Sembiring, 2026)Selain itu, fenomena FOMO (*Fear of Missing Out*) atau dorongan untuk selalu mengikuti tren dan mendapatkan validasi sosial membuat banyak orang mudah terpengaruh informasi yang belum tentu benar, sehingga rentan terhadap rekayasa sosial, dan hal ini diperparah dengan kelemahan sistem keamanan pada platform digital serta sifat anonimitas dunia maya yang memungkinkan pengguna menyembunyikan identitas dan memudahkan pelaku menghindari pengawasan aparat penegak hukum (Dani, 2025). Faktor-faktor kerentanan ini menunjukkan bahwa kejahatan siber tidak dapat dipahami semata-mata sebagai persoalan teknis, melainkan juga menyangkut aspek sosial, psikologis, dan struktural yang membutuhkan pendekatan viktimologi yang komprehensif untuk merumuskan strategi pencegahan dan perlindungan yang efektif.

Perlindungan Korban Kejahatan Siber dalam Perspektif Viktimologi

Di Indonesia, regulasi yang mengatur kejahatan siber secara garis besar tertuang dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui UU Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban, serta Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Perlindungan hukum terhadap korban kejahatan siber diatur melalui Pasal 27 ayat (1), (3), (4), Pasal 28 ayat (2), dan Pasal 29 UU ITE dengan sanksi pidana 4 hingga 12 tahun penjara, sementara untuk kasus kekerasan seksual berbasis elektronik, korban berhak mendapatkan pemulihan, penurunan konten (*take down*), hingga restitusi atau ganti rugi dari pelaku (Barus, 2026). Namun demikian, meskipun landasan konstitusional dan kerangka normatif telah tersedia, perlindungan hukum terhadap korban kejahatan siber di Indonesia masih belum memadai, baik secara normatif maupun institusional, karena konstruksi regulasi masih

dominan berorientasi pada pelaku (*offender-oriented*), sementara dimensi perlindungan dan pemulihan korban belum menjadi pusat desain hukum pidana siber

Beberapa kelemahan perlindungan hukum yang teridentifikasi mencakup ketidakjelasan norma karena tidak adanya definisi khusus untuk berbagai bentuk kejahatan siber seperti perundungan siber yang menyebabkan multitafsir dalam penegakan hukum, keterbatasan kapasitas aparat penegak hukum yang belum seluruhnya memiliki pemahaman dan kapasitas yang cukup untuk menangani kasus siber secara profesional dan empatik, serta kesulitan pembuktian terutama dalam atribusi identitas pelaku di ruang digital dan pembuktian kausalitas yang menjadi tantangan serius. Selain itu, minimnya mekanisme pemulihan yang komprehensif bagi korban, baik dari sisi psikologis, sosial, maupun restitusi, menjadi hambatan besar dalam upaya perlindungan korban, sehingga banyak korban kejahatan siber yang tidak mendapatkan keadilan dan pemulihan yang layak setelah mengalami tindak kejahatan (Utami, 2026). Kelemahan-kelemahan ini menunjukkan bahwa sistem perlindungan hukum yang ada masih memerlukan reformasi mendasar untuk dapat merespons kompleksitas kejahatan siber dan dampaknya terhadap korban.

Berdasarkan pendekatan viktimologi, diperlukan pergeseran paradigma dari hukum pidana yang berorientasi pada penghukuman pelaku menuju model restoratif yang memprioritaskan pemulihan korban, dengan beberapa rekomendasi yang dapat diimplementasikan secara konkret. Pertama, reformulasi kebijakan melalui revisi UU ITE harus menekankan prinsip perlindungan korban dan penghapusan pasal-pasal multitafsir yang berpotensi menyasar korban, sehingga regulasi tidak justru menjadi alat yang menambah penderitaan korban. Kedua, penguatan lembaga perlindungan dengan memperkuat peran Lembaga Perlindungan Saksi dan Korban (LPSK) yang diberikan mandat khusus untuk kasus siber, termasuk penyediaan program konseling, bantuan hukum, dan pengawasan pasca-insiden yang berkelanjutan. Ketiga, peningkatan kapasitas aparat penegak hukum melalui pelatihan forensik digital dan pendekatan berbasis hak asasi manusia, sehingga aparat mampu menangani kasus kejahatan siber dengan profesionalisme dan kepekaan terhadap kondisi korban. Keempat, penyediaan sistem layanan korban seperti *hotline* nasional untuk kejahatan siber, platform pengaduan digital yang mudah diakses, serta kampanye literasi digital tentang hak-hak korban yang masif dan berkelanjutan. Terakhir, penerapan prinsip *non-revictimization* yang memastikan setiap tahap proses hukum tidak menambah luka psikologis baru bagi korban, sehingga korban merasa aman dan didukung sepanjang proses peradilan (Pramana, 2026).

3. METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian hukum normatif, yaitu penelitian yang berfokus pada kajian terhadap norma-norma hukum yang berlaku. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan hukum yang berkaitan dengan kejahatan siber dan perlindungan korban, sedangkan pendekatan konseptual dilakukan dengan mengkaji konsep-konsep viktimologi yang berkembang dalam literatur ilmiah. Subjek dalam penelitian ini tidak berupa individu secara langsung, melainkan berupa bahan hukum yang terdiri dari bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan kejahatan siber dan perlindungan korban. Bahan hukum sekunder berupa buku, jurnal ilmiah, serta hasil penelitian yang relevan dengan topik viktimologi dan kejahatan siber. Adapun bahan hukum tersier berupa kamus hukum dan sumber lain yang mendukung pemahaman terhadap istilah-istilah yang digunakan.

Teknik pengumpulan data yang digunakan adalah studi kepustakaan (*library research*), yaitu dengan cara mengumpulkan dan menelaah berbagai literatur yang relevan, seperti peraturan perundang-undangan, buku, jurnal ilmiah, serta sumber lain yang berkaitan dengan penelitian ini. Teknik analisis data dalam penelitian ini dilakukan secara normatif, yaitu dengan cara mengkaji dan menginterpretasikan bahan hukum yang telah dikumpulkan secara sistematis. Data dianalisis dengan menggunakan metode deskriptif-analitis, yaitu menggambarkan secara jelas mengenai fenomena kejahatan siber serta dampaknya terhadap korban, kemudian dianalisis berdasarkan perspektif viktimologi untuk memperoleh kesimpulan yang komprehensif.

4. HASIL DAN PEMBAHASAN

Bentuk Kejahatan Siber yang Berkembang di Masyarakat

Kejahatan siber yang berkembang di masyarakat saat ini menunjukkan spektrum yang sangat luas dan terus mengalami perluasan seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Bentuk-bentuk kejahatan ini tidak hanya terbatas pada satu jenis tindakan, melainkan mencakup berbagai aktivitas ilegal yang memanfaatkan sistem komputer dan jaringan internet sebagai sarana utama, mulai dari manipulasi data, spionase, sabotase, provokasi, pencucian uang, peretasan (*hacking*), pornografi, prostitusi *online*, pencurian perangkat lunak, hingga perusakan perangkat keras yang menunjukkan kompleksitas kejahatan di dunia maya (Kafiar, 2026). Dalam praktiknya, kejahatan yang sering terjadi di masyarakat

antara lain pencurian kartu kredit (*carding*), peretasan situs web, penyadapan data seperti *email*, serta manipulasi data melalui perintah yang tidak sah dalam suatu sistem. Kejahatan siber juga dapat diklasifikasikan berdasarkan jenis aktivitasnya, seperti *unauthorized access*, *illegal contents*, penyebaran virus, *data forgery*, *cyber espionage*, *cyber sabotage and extortion*, *cyberstalking*, hingga *cyber terrorism* yang dapat mengancam keamanan negara (Pratiwi, 2022).

Perkembangan terkini menunjukkan bahwa modus kejahatan siber semakin canggih dengan memanfaatkan kecerdasan buatan atau *artificial intelligence* (AI). Serangan *phishing* yang dipersonalisasi secara hiper menggunakan *Large Language Models* (LLM) menjadi salah satu ancaman utama, di mana pelaku memanfaatkan data publik dari media sosial untuk menyusun narasi yang sangat meyakinkan sehingga korban hampir tidak bisa membedakan antara pesan resmi dan penipuan. Selain itu, teknologi *deepfake* telah mencapai tahap di mana manipulasi video dan suara terjadi secara *real-time*, sering digunakan untuk meniru suara atau wajah atasan (*CEO Fraud*) guna menginstruksikan transfer dana ke rekening pelaku. *Ransomware* juga berevolusi menjadi *triple extortion*, di mana pelaku tidak hanya mengunci sistem, tetapi juga mengancam membocorkan data sensitif ke publik dan melakukan serangan DDoS ke infrastruktur korban jika tebusan tidak dibayar, dengan target utama sektor infrastruktur kritis dan layanan kesehatan (Ahmad, 2025).

Data empiris menunjukkan peningkatan signifikan kasus kejahatan siber di Indonesia. Polda Metro Jaya mencatat sebanyak 2.597 laporan polisi terkait tindak pidana siber dengan kerugian mencapai Rp24,3 miliar sepanjang Januari hingga Agustus 2025, dengan bentuk penipuan daring yang paling dominan adalah *online scam*, *phishing*, dan pinjaman *online* ilegal, serta modus yang semakin canggih seperti penipuan kerja paruh waktu, investasi kripto fiktif (*pig butchering scam*), dan pemerasan seksual (*sextortion*) . Kejahatan ini pun tidak lagi berskala lokal, melainkan terorganisir lintas negara yang melibatkan jaringan internasional dengan pelaku dari Indonesia, Malaysia, dan Kamboja, di mana para pelaku memanfaatkan teknologi terbaru mulai dari aplikasi palsu di *Playstore* hingga manipulasi wajah dengan *deepfake* (Pah, 2025). Bentuk lain yang juga marak adalah penyebaran ujaran kebencian (*cyberhate*) yang dilatarbelakangi tingginya penetrasi pengguna media sosial dan pemanfaatan isu yang didominasi konten kebencian politik, agama, dan rasisme, yang seringkali berakar pada bias SARA dan polarisasi politik (Sembiring, 2026). Kehadiran Badan Siber dan Sandi Negara (BSSN) dan unit khusus di Polri menjadi langkah pemerintah dalam menangani peningkatan kasus ini, namun kesadaran masyarakat mengenai keamanan teknologi informasi dinilai masih rendah. Sebagai tindakan mitigasi, diperlukan edukasi tentang pentingnya

keamanan informasi kepada masyarakat, penguatan regulasi kebijakan keamanan siber, implementasi pendekatan *zero trust*, serta kolaborasi antar pemangku kepentingan yang melibatkan pemerintah, akademisi, swasta, media, dan komunitas (Afifah, 2025).

Dampak dan Perlindungan terhadap Korban dalam Perspektif Viktimologi

Perlindungan hukum bagi korban kejahatan siber di Indonesia masih belum optimal. Hal ini terlihat dari adanya kelemahan dalam mekanisme pemulihan korban serta keterbatasan kerja sama internasional dalam penanganan kejahatan siber yang bersifat lintas negara. Meskipun telah terdapat regulasi seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, implementasinya dinilai belum sepenuhnya memenuhi standar internasional dan aspek pemulihan korban sering kali kurang mendapatkan perhatian . Dalam praktiknya, korban kebocoran data sering dikategorikan sebagai *non-participating victims*, di mana mereka tidak terlibat langsung dalam kejadian, melainkan menjadi sasaran akibat kelalaian pihak ketiga seperti penyelenggara sistem elektronik (Barus, 2026). Korban kejahatan siber tidak hanya menghadapi keterbatasan dalam aspek perlindungan hukum, tetapi juga mengalami berbagai dampak yang signifikan dalam kehidupan mereka. Dalam konteks e-commerce, pengguna sering menjadi korban berbagai jenis kejahatan siber seperti penipuan *online*dan pencurian identitas yang menimbulkan kerugian finansial maupun dampak psikologis berupa trauma dan menurunnya tingkat kepercayaan diri.

Perlindungan hukum bagi pengguna *e-commerce* menghadapi tantangan kompleks seiring pesatnya pertumbuhan transaksi digital, di mana implementasi regulasi masih terhambat oleh rendahnya literasi digital masyarakat, lemahnya koordinasi antarlembaga, serta kerumitan yurisdiksi pelaku kejahatan lintas negara yang berbeda. Dalam perspektif viktimologi, pendekatan ini menjadi penting untuk memahami tingkat kerentanan korban serta faktor-faktor yang dapat meningkatkan risiko seseorang menjadi korban kejahatan siber. Penelitian menunjukkan bahwa korban seringkali rentan karena rendahnya literasi digital, tingginya kepercayaan pada pelaku, dan kurangnya verifikasi informasi, yang mengakibatkan kerugian finansial dan psikologis (Pratiwi, 2022). Teori viktimisasi menjelaskan bahwa korban memiliki tingkat keterlibatan yang berbeda dalam suatu peristiwa kejahatan, mulai dari korban yang sepenuhnya tidak bersalah hingga korban yang secara tidak langsung berkontribusi terhadap terjadinya tindak pidana. Perlindungan hukum terhadap korban juga diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen serta Undang-Undang Informasi dan Transaksi Elektronik, namun implementasinya masih menghadapi berbagai

kendala seperti rendahnya literasi digital masyarakat dan lemahnya penegakan hukum terhadap kejahatan siber yang bersifat lintas negara.

Sistem perlindungan hukum saat ini masih lebih berfokus pada penghukuman pelaku daripada pemulihan hak-hak korban, sehingga diperlukan pergeseran paradigma dari hukum pidana yang berorientasi pada penghukuman pelaku menuju model restoratif yang memprioritaskan pemulihan korban (Audrian, 2026). Pendekatan viktimologi menekankan pemulihan holistik yang tidak hanya bersifat finansial, tetapi juga restoratif untuk mengembalikan kesejahteraan psikis dan sosial korban . Pemerintah disarankan untuk memperkuat peran Lembaga Perlindungan Saksi dan Korban (LPSK) dengan mandat khusus untuk kasus siber, termasuk program konseling, bantuan hukum, dan pengawasan pasca-insiden guna menciptakan ekosistem perlindungan yang lebih adaptif terhadap dinamika ancaman digital. Untuk meningkatkan perlindungan korban, diperlukan kolaborasi antar lembaga dalam meningkatkan literasi digital masyarakat, penguatan regulasi dengan mempertegas sanksi pelanggaran dan mekanisme pemulihan korban, serta strategi integratif berupa kampanye nasional literasi digital, penguatan kolaborasi antar *stakeholder* untuk mengadopsi teknologi enkripsi dan *two-factor authentication*, serta reformasi regulasi yang responsif terhadap dinamika kejahatan siber (Mufid, 2026). Dengan pendekatan holistik ini, diharapkan tercipta ekosistem digital yang aman, adil, dan berkelanjutan, sehingga korban kejahatan siber tidak hanya mendapatkan keadilan prosedural tetapi juga pemulihan yang bermakna bagi kehidupan mereka.

5. KESIMPULAN DAN SARAN

Kejahatan siber di Indonesia telah berkembang menjadi fenomena yang sangat kompleks dengan spektrum yang luas, mencakup berbagai bentuk seperti penipuan daring, peretasan, pencurian identitas, ransomware, penyebaran hoax, hingga kejahatan berbasis kecerdasan buatan dan *deepfake* yang semakin canggih. Data empiris menunjukkan peningkatan signifikan kasus kejahatan siber dengan kerugian finansial yang sangat besar, yang tidak hanya menyasar individu tetapi juga sektor bisnis dan pemerintahan, serta melibatkan jaringan pelaku yang terorganisir lintas negara.

Dampak yang dialami korban tidak terbatas pada kerugian materi, melainkan juga mencakup trauma psikologis, kecemasan, depresi, isolasi sosial, dan penurunan kepercayaan diri yang mempengaruhi kualitas hidup mereka secara keseluruhan. Dalam perspektif viktimologi, korban kejahatan siber sering kali berada dalam posisi rentan akibat rendahnya literasi digital, kelemahan sistem keamanan, dan sifat anonimitas dunia maya, sehingga

membutuhkan perhatian khusus dalam upaya perlindungan dan pemulihan. Berdasarkan simpulan tersebut, diperlukan peningkatan literasi digital masyarakat agar mampu memahami risiko serta melindungi diri dari kejahatan siber. Selain itu, penguatan sistem keamanan teknologi informasi dan penegakan hukum yang lebih efektif perlu terus ditingkatkan. Kerja sama antara pemerintah, aparat penegak hukum, serta berbagai pihak terkait, baik di tingkat nasional maupun internasional, juga perlu diperkuat guna menciptakan perlindungan yang lebih komprehensif bagi korban dan mewujudkan ekosistem digital yang aman dan terpercaya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Ibu Dr. Ni Ketut Sari Adnyani S.Pd., M.Hum. selaku dosen pengampu Mata Kuliah Viktimologi atas bimbingan dan arahan dalam penulisan artikel ini. Serta penulis ucapkan terimakasih kepada Bapak I Putu Dwika Ariestu selaku dosen tim dari dosen pengampu Mata Kuliah Viktimologi

DAFTAR REFERENSI

Afifah, E. F. (2025). Keamanan siber dalam perbankan serta tantangan dan solusi di era digital. *Jurnal Multidisiplin Ilmu Akademik, 2*(1), 33–42. https://doi.org/10.63545/jaim.v1.i2.157

Ahmad, M. R. (2025). Perlindungan hukum pengguna e-commerce: Perspektif viktimologi dalam menghadapi kejahatan siber. *Bookchapter Hukum dan Lingkungan, 1*, 967–989.

Audrian, R. P. (2026). Perlindungan dan pemulihan hak korban tindak pidana: Studi viktimologi dalam sistem peradilan pidana di Indonesia. *Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan, 2*(3), 795–797. https://doi.org/10.58466/axfent61

Barus, A. D. (2026). Perlindungan hukum terhadap korban kejahatan siber dalam perspektif viktimologi: Studi terhadap kebocoran data pribadi di Indonesia. *Fatih: Journal of Contemporary Research, 3*(1).

Dani, R. (2025, September 13). Menelaah konstruksi norma hukum dalam upaya perlindungan korban terhadap kejahatan siber global. *Tribunnews*. https://www.tribunnews.com/nasional/7728173/menelaah-konstruksi-norma-hukum-dalam-upaya-perlindungan-korban-terhadap-kejahatan-siber-global

Kafiar, G. S. (2026). Phishing dan upaya perlindungan hukum di Indonesia sebagai ancaman kejahatan siber. *Jembatan Hukum: Kajian Ilmu Hukum, Sosial dan Administrasi Negara, 3*(1), 126–134. https://doi.org/10.62383/jembatan.v3i1.2959

Mufid, S. F. (2026). Keamanan digital di era transformasi teknologi: Peran literasi dan perilaku dalam perlindungan diri. *Qolamuna: Keislaman, Pendidikan, Literasi dan Humaniora, 3*(1), 251–261.

Pah, C. E. (2025). Sosialisasi kejahatan siber dan perlindungan data pribadi untuk mencegah penipuan berbasis online terhadap masyarakat. *Mitra Mahajana: Jurnal Pengabdian Masyarakat, 6*(1), 24–33. https://doi.org/10.37478/mahajana.v6i1.4908

Pramana, I. B. (2026, Maret 24). FOMO dan rendahnya literasi digital penyebab tingginya korban kejahatan siber. *RRI*. https://rri.co.id/denpasar/hiburan/2281384/fomo-dan-rendahnya-literasi-digital-penyebab-tingginya-korban-kejahatan-siber

Pratiwi, B. (2022). Kajian konsep *modalities of constraint* terhadap pencegahan konten *hate speech* sebagai cybercrime di Indonesia. *Jurnal Panorama Hukum, 7*(2), 147–160. https://doi.org/10.21067/jph.v7i2.7635

Raharjo, T. (2024). Penatausahaan aset tanah daerah hasil pemekaran Kabupaten Jayapura. *Journal of Political Issues, 5*(2), 134–145. https://doi.org/10.33019/jpi.v5i2.159

Romanza, R. (2023). *Implementasi kebijakan penyerahan aset dari pemerintahan Kabupaten Kerinci kepada Pemerintah Kota Sungai Penuh Provinsi Jambi*. Program Studi Politik Pemerintahan.

Salwa, Z. (2025). Dampak kebijakan desentralisasi terhadap otonomi daerah dalam kerangka hukum tata negara. *INNOVATIVE: Journal of Social Science Research, 5*(4), 639–649.

Sari, D. P. (2025). *Relevansi rencana pemekaran Kecamatan Kota Lama Ponorogo perspektif Maṣlaḥah Mursalah dan teori desentralisasi*. IAIN Ponorogo.

Sembiring, T. F. (2026). *Aspek perlindungan yuridis korban perundungan siber dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik*. Universitas Islam Sumatera Utara.

Utami, F. R. (2026). Eksploitasi siber dan pertanggungjawaban negara di Asia Tenggara: Tinjauan viktimologis dalam kerangka hukum internasional. *Jurnal Untirta, 4*(1).

Wibowo, L. R. (2025, Juni 13). Perlindungan hukum terhadap korban kejahatan siber: Sudahkah memadai? *Radar Magelang*. https://radarmagelang.jawapos.com/artikel-ilmiah/2506130002/perlindungan-hukum-terhadap-korban-kejahatan-siber-sudahkah-memadai

Widianingrum, A. R. (2024). Analisis implementasi kebijakan hukum terhadap penanganan kejahatan siber di era digital. *Journal Iuris Scientia, 2*(2), 90–102. https://doi.org/10.62263/jis.v2i2.40