ULIL ALBAB : Jurnal Ilmiah Multidisiplin
Vol.5, No.9, Agustus 2026

Perlindungan Korban Kejahatan Siber dalam Perspektif Kriminologi dan Viktimologi

Ruliyanando Gondo Suhandito[1], Bagas Intan Sanjaya[2], Budhi Rahmadi[3], Muhammad Rafi Ardian Syahputra[4], Noor Rohmat[5]
[1]Universitas Widya Mataram, Indonesia
[2]Universitas Widya Mataram, Indonesia
[3]Universitas Widya Mataram, Indonesia
[4]Universitas Widya Mataram, Indonesia
[5]Universitas Widya Mataram, Indonesia
E-mail: suhanditoruliyanando21@gmail.com[1], bagasintansanjaya@gmail.com[2], budhirahmadi94@gmail.com[3], rafiardian17@gmail.com[4], noorrohmatnotaris@gmail.com[5]

Article History:
Received: 03 Juli 2026
Revised: 18 Juli 2026
Accepted: 01 Agustus 2026

Keywords: *Kriminologi; Viktimologi; Cybercrime; Perlindungan Korban; Hukum Pidana.*

Abstrak: *Perkembangan teknologi informasi telah memberikan dampak signifikan terhadap perubahan pola kejahatan dari bentuk konvensional menuju kejahatan berbasis digital atau kejahatan siber (cybercrime). Fenomena ini tidak hanya meningkatkan kompleksitas tindak pidana, tetapi juga memperluas jumlah dan karakteristik korban yang mengalami kerugian ekonomi, psikologis, maupun sosial. Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap korban kejahatan siber berdasarkan perspektif kriminologi dan viktimologi serta mengidentifikasi faktor-faktor yang memengaruhi tingginya angka viktimisasi di ruang digital. Penelitian menggunakan metode penelitian hukum normatif dengan pendekatan peraturan perundang-undangan, konseptual, dan studi kepustakaan. Data dianalisis secara kualitatif melalui interpretasi terhadap berbagai regulasi nasional dan literatur ilmiah mengenai kriminologi, viktimologi, dan cybercrime. Hasil penelitian menunjukkan bahwa meningkatnya penggunaan teknologi belum diimbangi dengan sistem perlindungan korban yang komprehensif. Perspektif kriminologi mampu menjelaskan faktor penyebab terjadinya cybercrime, sedangkan viktimologi memberikan pemahaman mengenai karakteristik korban, tingkat kerentanan, serta bentuk perlindungan yang seharusnya diberikan negara. Oleh karena itu, penguatan regulasi, peningkatan literasi digital masyarakat, serta optimalisasi mekanisme perlindungan korban menjadi langkah penting dalam mewujudkan sistem peradilan pidana yang berorientasi pada keadilan bagi korban.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era digital telah membawa perubahan yang sangat besar dalam berbagai aspek kehidupan masyarakat. Internet telah menjadi bagian yang tidak terpisahkan dari aktivitas ekonomi, pendidikan, pemerintahan, perdagangan, hingga interaksi sosial. Kemudahan akses informasi dan komunikasi tersebut memberikan berbagai manfaat bagi masyarakat, namun di sisi lain juga membuka peluang lahirnya berbagai bentuk tindak pidana baru yang memanfaatkan teknologi digital sebagai sarana melakukan kejahatan. Perubahan karakteristik kejahatan dari kejahatan konvensional menuju kejahatan berbasis teknologi menimbulkan tantangan baru bagi sistem hukum pidana, khususnya dalam memberikan perlindungan terhadap korban kejahatan. Kejahatan siber (cybercrime) berkembang dengan sangat cepat seiring meningkatnya jumlah pengguna internet di Indonesia. Modus operandi pelaku juga semakin kompleks, mulai dari penipuan daring (online fraud), pencurian identitas, penyebaran malware, peretasan sistem elektronik, pencurian data pribadi, pemerasan digital, penyebaran berita bohong (hoaks), hingga berbagai bentuk kekerasan berbasis gender secara daring. Berbeda dengan kejahatan konvensional, cybercrime memiliki karakteristik lintas batas negara (transnational crime), memanfaatkan anonimitas pelaku, serta memerlukan kemampuan teknologi yang tinggi sehingga proses pengungkapan tindak pidana menjadi semakin sulit. Dalam perspektif kriminologi, munculnya cybercrime merupakan konsekuensi dari perubahan sosial akibat kemajuan teknologi. Kriminologi tidak hanya mempelajari pelaku kejahatan, tetapi juga faktor-faktor penyebab terjadinya kejahatan, lingkungan sosial yang memengaruhi perilaku kriminal, serta efektivitas kebijakan penanggulangan kejahatan. Berbagai teori kriminologi, seperti Routine Activity Theory, Social Learning Theory, maupun Rational Choice Theory menjelaskan bahwa peluang melakukan kejahatan akan semakin besar ketika terdapat target yang rentan, tidak adanya pengawasan yang memadai, serta keuntungan yang diperoleh pelaku jauh lebih besar dibandingkan risiko yang dihadapi. Dalam konteks dunia digital, kondisi tersebut semakin mudah ditemukan karena masyarakat banyak melakukan aktivitas ekonomi maupun sosial melalui internet tanpa disertai kemampuan keamanan digital yang memadai (Annisa et al., 2025).

Di sisi lain, viktimologi memberikan perhatian terhadap korban sebagai pihak yang mengalami penderitaan akibat tindak pidana. Selama bertahun-tahun sistem peradilan pidana lebih berorientasi kepada pelaku (offender oriented), sementara kepentingan korban sering kali belum memperoleh perhatian yang proporsional. Padahal korban merupakan pihak yang secara langsung mengalami kerugian material, psikologis, maupun sosial akibat kejahatan. Viktimologi mempelajari karakteristik korban, hubungan antara pelaku dengan korban, tingkat kerentanan seseorang menjadi korban, serta bentuk perlindungan yang seharusnya diberikan oleh negara. Korban cybercrime memiliki karakteristik yang berbeda dibandingkan korban kejahatan konvensional. Selain mengalami kerugian finansial, korban sering mengalami kehilangan data pribadi, pencemaran nama baik, tekanan psikologis, bahkan trauma berkepanjangan akibat penyebaran informasi pribadi di ruang digital. Dalam beberapa kasus, korban juga menghadapi secondary victimization, yaitu penderitaan lanjutan akibat proses hukum yang kurang berpihak kepada korban atau rendahnya pemahaman aparat penegak hukum terhadap karakteristik kejahatan siber. Kondisi tersebut menunjukkan bahwa perlindungan terhadap korban cybercrime masih memerlukan pembenahan baik dari sisi regulasi maupun implementasinya. Indonesia sebenarnya telah memiliki berbagai regulasi yang mengatur tindak pidana di ruang siber, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana, serta berbagai peraturan

pelaksana lainnya. Meskipun demikian, implementasi perlindungan terhadap korban masih menghadapi berbagai kendala, antara lain keterbatasan kemampuan digital aparat penegak hukum, sulitnya pembuktian elektronik, rendahnya kesadaran masyarakat dalam menjaga keamanan data pribadi, serta belum optimalnya mekanisme pemulihan korban (Prof. Dr. Henny Saida Flora, 2026).

Di sisi lain, penelitian mengenai viktimologi digital menunjukkan bahwa karakteristik korban cybercrime dipengaruhi oleh tingkat literasi digital, usia, aktivitas media sosial, serta kemampuan individu dalam melindungi data pribadi. Masyarakat dengan tingkat literasi digital yang rendah cenderung lebih rentan menjadi korban berbagai bentuk penipuan maupun pencurian data elektronik. Meskipun berbagai penelitian telah membahas cybercrime maupun viktimologi secara terpisah, masih relatif sedikit penelitian yang mengintegrasikan perspektif kriminologi dan viktimologi dalam menganalisis perlindungan hukum terhadap korban kejahatan siber di Indonesia. Sebagian besar penelitian lebih menitikberatkan pada aspek penindakan terhadap pelaku dibandingkan mekanisme perlindungan korban. Padahal paradigma hukum pidana modern menempatkan korban sebagai salah satu subjek utama yang harus memperoleh akses terhadap keadilan, perlindungan, restitusi, kompensasi, rehabilitasi, dan pemulihan psikologis. Urgensi penelitian ini semakin meningkat seiring pesatnya digitalisasi berbagai layanan publik maupun transaksi ekonomi di Indonesia. Penggunaan layanan keuangan digital, perdagangan elektronik, media sosial, dan sistem pemerintahan berbasis elektronik memperbesar peluang terjadinya berbagai bentuk kejahatan siber yang menyasar masyarakat sebagai pengguna layanan digital. Oleh karena itu, diperlukan kajian yang mampu menjelaskan hubungan antara faktor penyebab cybercrime, karakteristik korban, serta efektivitas perlindungan hukum berdasarkan perspektif kriminologi dan viktimologi secara terpadu. Penelitian ini diharapkan dapat memberikan kontribusi akademik terhadap pengembangan ilmu kriminologi dan viktimologi, khususnya dalam memahami dinamika kejahatan siber di Indonesia. Selain itu, hasil penelitian juga diharapkan menjadi bahan pertimbangan bagi pembentuk kebijakan, aparat penegak hukum, serta lembaga perlindungan korban dalam merumuskan strategi pencegahan dan perlindungan hukum yang lebih efektif terhadap korban cybercrime. Dengan demikian, penelitian ini tidak hanya memiliki nilai teoritis, tetapi juga memberikan manfaat praktis bagi pengembangan sistem peradilan pidana yang berorientasi pada perlindungan hak-hak korban di era digital. Berdasarkan uraian tersebut, penelitian ini berfokus pada dua rumusan permasalahan utama. Pertama, bagaimana perspektif kriminologi menjelaskan faktor-faktor penyebab meningkatnya kejahatan siber di Indonesia. Kedua, bagaimana perspektif viktimologi menjelaskan bentuk perlindungan hukum yang ideal bagi korban kejahatan siber dalam sistem hukum pidana Indonesia. Melalui analisis terhadap kedua perspektif tersebut, penelitian ini diharapkan mampu memberikan rekomendasi mengenai model perlindungan korban yang lebih komprehensif sehingga mampu menjawab tantangan perkembangan kejahatan digital pada masa kini maupun di masa yang akan datang (Ahmad & Utari, 2025).

LANDASAN TEORI

A. Kriminologi

Kriminologi merupakan cabang ilmu yang mempelajari kejahatan secara ilmiah, meliputi penyebab terjadinya kejahatan, karakteristik pelaku, korban, reaksi masyarakat, hingga upaya pencegahan dan penanggulangannya. Menurut Edwin H. Sutherland, kriminologi adalah keseluruhan pengetahuan mengenai kejahatan sebagai fenomena sosial yang mencakup proses pembentukan hukum, pelanggaran hukum, serta reaksi masyarakat terhadap pelanggaran hukum

tersebut. Dengan demikian, ruang lingkup kriminologi tidak hanya terbatas pada perilaku pelaku kejahatan, tetapi juga mencakup faktor-faktor sosial, ekonomi, budaya, politik, dan teknologi yang memengaruhi munculnya kejahatan. Dalam perkembangannya, objek kajian kriminologi semakin luas, terutama setelah berkembangnya teknologi informasi yang melahirkan berbagai bentuk kejahatan digital. Cybercrime menjadi salah satu bentuk kejahatan modern yang memerlukan pendekatan multidisipliner karena melibatkan aspek hukum, teknologi informasi, psikologi, ekonomi, hingga hubungan internasional. Oleh sebab itu, pendekatan kriminologi menjadi penting dalam memahami perubahan pola kejahatan di era digital (Lubis, 2026).

1. Routine Activity Theory

Routine Activity Theory yang menjelaskan bahwa suatu kejahatan terjadi apabila terdapat tiga unsur utama secara bersamaan, yaitu: (1) Pelaku yang termotivasi (motivated offender); (2) Target yang layak menjadi korban (suitable target); dan (3) Tidak adanya penjaga yang mampu mencegah kejahatan (absence of capable guardian). Dalam konteks cybercrime, ketiga unsur tersebut sangat mudah ditemukan. Pelaku memperoleh kemudahan melakukan kejahatan melalui internet dengan identitas anonim. Target berupa data pribadi, rekening bank, akun media sosial, maupun sistem elektronik menjadi sasaran yang mudah diakses apabila sistem keamanan rendah. Sementara itu, pengawasan terhadap aktivitas digital sering kali belum optimal sehingga peluang terjadinya kejahatan semakin besar. Teori ini menjelaskan bahwa meningkatnya penggunaan internet secara masif menyebabkan meningkatnya peluang kejahatan apabila tidak diimbangi dengan sistem keamanan digital yang memadai (Lubis, 2026).

2. Rational Choice Theory

Rational Choice Theory menyatakan bahwa pelaku kejahatan melakukan tindakan kriminal setelah mempertimbangkan keuntungan dan kerugian yang akan diperoleh. Apabila keuntungan dipandang lebih besar dibandingkan risiko tertangkap, maka seseorang cenderung melakukan tindak pidana. Pada cybercrime, pelaku dapat memperoleh keuntungan finansial dalam jumlah besar melalui penipuan daring, phishing, ransomware, maupun pencurian data pribadi dengan risiko yang relatif kecil karena sulitnya identifikasi pelaku dan kompleksitas pembuktian digital. Kondisi tersebut menjadikan cybercrime sebagai salah satu jenis kejahatan yang berkembang paling cepat di dunia (Annisa et al., 2025).

3. Social Learning Theory

Perilaku kriminal dipelajari melalui proses interaksi sosial. Individu dapat mempelajari teknik, motivasi, serta pembenaran terhadap suatu tindakan kriminal melalui lingkungan sosialnya. Dalam perkembangan teknologi digital, media sosial, forum internet, hingga komunitas daring memungkinkan seseorang mempelajari teknik hacking, carding, phishing, maupun penyebaran malware secara cepat. Dengan demikian, teknologi tidak hanya menjadi sarana melakukan kejahatan tetapi juga media pembelajaran perilaku kriminal (Hera et al., 2026).

B. Viktimologi

Viktimologi merupakan ilmu yang mempelajari korban kejahatan, hubungan antara korban dan pelaku, penyebab seseorang menjadi korban, dampak viktimisasi, serta bentuk perlindungan yang diberikan kepada korban. Menurut Benjamin Mendelsohn, viktimologi adalah ilmu yang mempelajari korban dalam arti luas, termasuk hubungan korban dengan pelaku maupun sistem peradilan pidana. Perkembangan viktimologi kemudian menempatkan korban sebagai subjek yang memiliki hak memperoleh perlindungan, kompensasi, restitusi, rehabilitasi, dan pemulihan. Pendekatan viktimologi modern tidak lagi memandang korban sebagai pihak pasif, melainkan sebagai individu yang memiliki hak konstitusional yang wajib dipenuhi oleh negara (Budana, 2026).

Tipologi Korban

Mendelsohn mengklasifikasikan korban menjadi beberapa kategori, antara lain: (1) Korban yang benar-benar tidak bersalah (completely innocent victim); (2) Korban karena ketidaktahuan atau kelalaian; (3) Korban yang turut berperan terhadap terjadinya kejahatan; (4) Korban yang lebih bersalah dibanding pelaku; dan (5) Korban yang sepenuhnya bertanggung jawab. Dalam cybercrime, sebagian besar korban termasuk kategori korban yang tidak bersalah karena menjadi sasaran kejahatan tanpa mengetahui adanya ancaman digital. Namun demikian, rendahnya literasi digital dapat meningkatkan risiko seseorang mengalami viktimisasi (Akbar, 2026).

Secondary Victimization

Korban kejahatan sering mengalami penderitaan lanjutan setelah tindak pidana terjadi. Kondisi ini disebut secondary victimization. Pada cybercrime, secondary victimization dapat berupa: (1) sulitnya proses pelaporan; (2) lambatnya penanganan perkara; (3) penyebaran data pribadi secara terus-menerus; (4) stigma sosial; (5) trauma psikologis; dan (6) hilangnya kepercayaan terhadap sistem hukum. Oleh karena itu, sistem peradilan pidana modern menekankan pentingnya victim-oriented justice, yaitu sistem hukum yang berorientasi pada pemulihan korban (An Nisya Nursabilah et al., 2025).

C. Cybercrime Sebagai Kejahatan Modern

Cybercrime merupakan segala bentuk kejahatan yang menggunakan komputer, jaringan internet, maupun sistem elektronik sebagai alat, sasaran, ataupun media melakukan tindak pidana. Karakteristik cybercrime meliputi: (1) lintas negara (transnational crime); (2) menggunakan teknologi informasi; (3) identitas pelaku sulit diketahui; (4) pembuktian bergantung pada bukti elektronik; dan (5) perkembangan modus operandi sangat cepat. Jenis cybercrime yang paling banyak terjadi meliputi: (1) online fraud; (2) phishing; (3) hacking; (4) identity theft; (5) malware; (6) ransomware; (7) cyber bullying; (8) cyber stalking; (9) penyebaran konten ilegal; dan (10) pencurian data pribadi. Karakteristik tersebut menyebabkan penanganan cybercrime membutuhkan kerja sama antara aparat penegak hukum, penyelenggara sistem elektronik, ahli digital forensik, serta masyarakat (Garnita & Kuswandi, 2025).

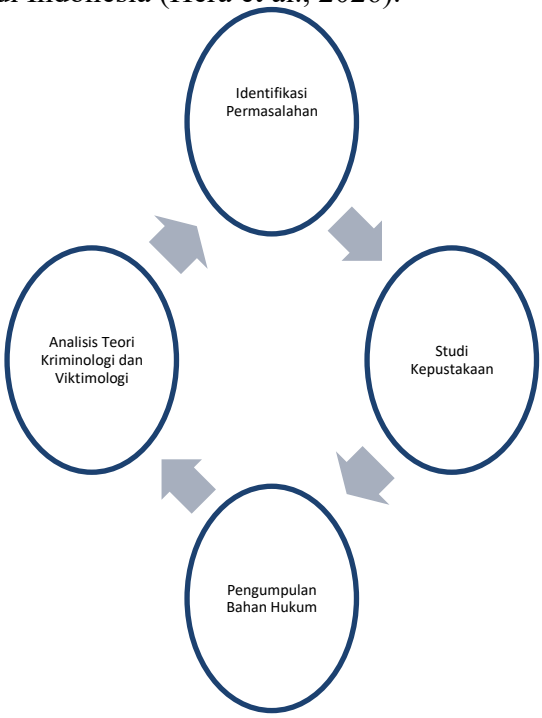
D. Perlindungan Hukum Korban

Perlindungan Hukum Korban merupakan salah satu tujuan hukum pidana modern yang tidak hanya berfokus pada penghukuman pelaku, tetapi juga pada pemulihan hak dan kesejahteraan korban. Di Indonesia, perlindungan tersebut diatur dalam berbagai regulasi, antara lain Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana. Bentuk perlindungan yang diberikan mencakup perlindungan fisik dan psikologis, bantuan hukum, restitusi, kompensasi, rehabilitasi, pemulihan nama baik, perlindungan data pribadi, serta pendampingan selama proses peradilan. Dalam perspektif viktimologi, perlindungan korban bertujuan tidak hanya memberikan keadilan melalui penjatuhan sanksi kepada pelaku, tetapi juga memastikan korban memperoleh pemulihan secara menyeluruh sehingga dapat kembali menjalankan kehidupan sosial secara normal (Apriyani et al., 2025).

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (normative legal research) dengan menggunakan pendekatan peraturan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), serta pendekatan kepustakaan (library research). Pendekatan

tersebut dipilih karena penelitian berfokus pada analisis norma hukum yang mengatur perlindungan korban cybercrime berdasarkan perspektif kriminologi dan viktimologi. Sumber data yang digunakan terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban, Kitab Undang-Undang Hukum Pidana, serta berbagai regulasi lain yang berkaitan dengan perlindungan korban kejahatan siber. Bahan hukum sekunder diperoleh dari buku-buku kriminologi, viktimologi, hukum pidana, artikel jurnal nasional maupun internasional bereputasi, hasil penelitian terdahulu, serta laporan lembaga pemerintah yang berkaitan dengan cybercrime. Sementara itu, bahan hukum tersier berasal dari kamus hukum, ensiklopedia hukum, dan berbagai referensi pendukung lainnya. Teknik pengumpulan data dilakukan melalui studi kepustakaan (library research), yaitu mengidentifikasi, menginventarisasi, membaca, serta mengkaji berbagai sumber hukum yang relevan dengan fokus penelitian. Analisis data menggunakan metode analisis kualitatif dengan teknik deskriptif-analitis. Seluruh bahan hukum dianalisis secara sistematis melalui proses reduksi data, klasifikasi, interpretasi norma hukum, kemudian dibandingkan dengan teori kriminologi dan viktimologi untuk memperoleh kesimpulan yang komprehensif mengenai perlindungan hukum terhadap korban cybercrime di Indonesia (Hera et al., 2026).



Gambar 1. Diagram

HASIL DAN PEMBAHASAN

A. Analisis Kriminologi terhadap Meningkatnya Kejahatan Siber di Indonesia

Perkembangan teknologi digital telah mengubah pola kehidupan masyarakat Indonesia secara signifikan. Aktivitas ekonomi, pendidikan, pemerintahan, hingga komunikasi interpersonal kini banyak dilakukan melalui internet. Transformasi digital tersebut membawa berbagai manfaat berupa efisiensi, kemudahan akses informasi, serta peningkatan produktivitas. Namun, di sisi lain, digitalisasi juga menciptakan ruang baru bagi berkembangnya berbagai bentuk tindak pidana berbasis teknologi informasi atau **cybercrime**. Dari perspektif kriminologi, perubahan lingkungan

sosial akibat kemajuan teknologi merupakan salah satu faktor yang memengaruhi munculnya bentuk-bentuk kejahatan baru yang memiliki karakteristik berbeda dengan kejahatan konvensional. Cybercrime tidak lagi dilakukan secara sederhana, melainkan melibatkan teknologi yang semakin canggih, penggunaan identitas anonim, jaringan lintas negara, serta pemanfaatan kelemahan sistem keamanan digital. Pelaku dapat menjalankan aksinya tanpa harus bertemu langsung dengan korban sehingga risiko untuk dikenali menjadi lebih kecil. Kondisi tersebut menyebabkan cybercrime berkembang sangat cepat dibandingkan bentuk kejahatan konvensional. Berdasarkan kajian kriminologi, meningkatnya kejahatan siber dipengaruhi oleh kombinasi faktor internal pelaku dan faktor eksternal yang berasal dari lingkungan sosial maupun perkembangan teknologi. Faktor-faktor tersebut saling berinteraksi sehingga menciptakan peluang terjadinya tindak pidana di ruang digital (Annisa et al., 2025).

1. Faktor Perkembangan Teknologi Informasi

Kemajuan teknologi merupakan faktor utama yang memengaruhi meningkatnya cybercrime. Internet memungkinkan setiap individu terhubung dengan berbagai sistem informasi dalam waktu yang sangat singkat. Selain memberikan kemudahan, kondisi tersebut juga membuka peluang bagi pelaku untuk mengeksploitasi kelemahan sistem keamanan elektronik. Saat ini berbagai layanan keuangan digital, perdagangan elektronik, dompet digital, media sosial, hingga penyimpanan data berbasis komputasi awan (cloud computing) menjadi target utama pelaku cybercrime. Semakin banyak data yang tersimpan secara digital, semakin besar pula peluang terjadinya pencurian data maupun penyalahgunaan informasi pribadi. Pelaku memanfaatkan berbagai teknik seperti phishing, malware, social engineering, ransomware, carding, hingga pencurian identitas (identity theft). Modus tersebut terus berkembang mengikuti inovasi teknologi sehingga aparat penegak hukum harus selalu memperbarui kemampuan investigasi digital (Prof. Dr. Henny Saida Flora, 2026).

2. Faktor Ekonomi

Perspektif kriminologi menjelaskan bahwa kondisi ekonomi turut memengaruhi motivasi seseorang melakukan tindak pidana. Cybercrime sering dipandang sebagai kejahatan dengan keuntungan ekonomi tinggi tetapi risiko relatif rendah. Pelaku dapat memperoleh keuntungan dalam jumlah besar melalui penipuan daring, pembobolan rekening, pencurian data kartu kredit, maupun penjualan data pribadi. Dibandingkan kejahatan konvensional, cybercrime tidak memerlukan kontak fisik dengan korban sehingga biaya operasional pelaku relatif kecil. Kondisi tersebut sesuai dengan Rational Choice Theory yang menyatakan bahwa seseorang akan melakukan kejahatan apabila keuntungan yang diperoleh diperkirakan lebih besar dibandingkan risiko yang akan diterima. Sulitnya identifikasi pelaku serta proses pembuktian digital semakin memperkuat persepsi bahwa cybercrime merupakan tindak pidana yang menguntungkan (Garnita & Kuswandi, 2025).

3. Faktor Rendahnya Literasi Digital

Hasil kajian menunjukkan bahwa sebagian besar korban cybercrime memiliki tingkat literasi digital yang masih rendah. Banyak masyarakat belum memahami pentingnya menjaga kerahasiaan data pribadi, penggunaan autentikasi ganda, keamanan kata sandi, maupun cara mengenali tautan palsu. Pelaku memanfaatkan kondisi tersebut melalui teknik social engineering, yaitu manipulasi psikologis yang bertujuan memperoleh informasi rahasia korban. Dalam banyak kasus, korban secara sukarela memberikan kode OTP, PIN, ataupun informasi rekening karena percaya terhadap pelaku yang menyamar sebagai petugas bank, aparat pemerintah, maupun penyedia layanan digital. Rendahnya literasi digital menyebabkan masyarakat menjadi target yang mudah bagi pelaku kejahatan. Oleh karena itu, pencegahan cybercrime tidak cukup dilakukan

melalui penegakan hukum, tetapi juga memerlukan peningkatan edukasi masyarakat (Apriyani et al., 2025).

4. Faktor Lemahnya Sistem Keamanan Digital

Keamanan sistem informasi menjadi salah satu aspek penting dalam pencegahan cybercrime. Banyak organisasi maupun individu masih menggunakan sistem keamanan yang lemah sehingga mudah disusupi oleh pelaku. Beberapa kelemahan yang sering ditemukan meliputi: (1) penggunaan kata sandi yang sederhana; (2) tidak melakukan pembaruan sistem (software update); (3) tidak menggunakan autentikasi dua faktor; (4) rendahnya pengamanan server; dan (5) lemahnya pengelolaan data pribadi. Kondisi tersebut menunjukkan bahwa cybercrime tidak selalu terjadi karena kecanggihan pelaku, tetapi juga akibat lemahnya sistem perlindungan yang dimiliki korban (Hera et al., 2026).

5. Faktor Anonimitas Internet

Internet memberikan kesempatan kepada pelaku untuk menyembunyikan identitas melalui berbagai teknologi seperti Virtual Private Network (VPN), akun palsu, server luar negeri, cryptocurrency, maupun jaringan terenkripsi. Anonimitas tersebut menyulitkan aparat penegak hukum dalam melakukan pelacakan identitas pelaku. Bahkan dalam beberapa kasus, pelaku melakukan aksinya dari negara lain sehingga memerlukan kerja sama internasional. Karakteristik ini menjadikan cybercrime sebagai salah satu bentuk **transnational organized crime** yang memerlukan koordinasi lintas yurisdiksi (Annisa et al., 2025).

Analisis Berdasarkan Teori Kriminologi

A. Routine Activity Theory

Routine Activity Theory menjelaskan bahwa kejahatan terjadi apabila terdapat pelaku yang termotivasi, target yang layak, dan tidak adanya pengawasan yang memadai. Dalam cybercrime, ketiga unsur tersebut dapat dijelaskan sebagai berikut.

Unsur	Kondisi pada Cybercrime
Motivated Offender	Pelaku memiliki kemampuan teknologi serta motivasi ekonomi.
Suitable Target	Pengguna internet, rekening digital, akun media sosial, dan data pribadi.
Absence of Capable Guardian	Rendahnya keamanan sistem, lemahnya literasi digital, dan keterbatasan pengawasan.

Teori ini menunjukkan bahwa meningkatnya aktivitas digital masyarakat secara otomatis meningkatkan peluang terjadinya cybercrime apabila tidak diimbangi dengan peningkatan keamanan informasi (Prof. Dr. Henny Saida Flora, 2026).

B. Rational Choice Theory

Berdasarkan Rational Choice Theory, pelaku melakukan perhitungan rasional sebelum melakukan tindak pidana. Pada cybercrime, keuntungan yang dipertimbangkan antara lain: (1) memperoleh uang dalam jumlah besar; (2) identitas sulit dilacak; (3) kemungkinan tertangkap relatif kecil; dan (4) korban tersebar di berbagai wilayah. Sebaliknya, risiko yang dipertimbangkan pelaku masih dianggap rendah karena proses pembuktian elektronik memerlukan kemampuan teknis yang tinggi (Ahmad & Utari, 2025).

C. Social Learning Theory

Social Learning Theory menjelaskan bahwa perilaku kriminal dipelajari melalui proses interaksi sosial. Saat ini berbagai forum internet bahkan menyediakan tutorial mengenai hacking, phishing, malware, hingga carding. Meskipun banyak aktivitas tersebut bersifat ilegal, informasi tersebut tetap dapat diakses oleh individu yang memiliki motivasi melakukan kejahatan. Perkembangan teknologi komunikasi menyebabkan proses pembelajaran perilaku kriminal

menjadi jauh lebih cepat dibandingkan sebelumnya (Lubis, 2026).

Hasil Analisis Penelitian

Hasil analisis menunjukkan bahwa meningkatnya cybercrime di Indonesia bukan hanya disebabkan oleh kecanggihan teknologi, tetapi merupakan akibat interaksi berbagai faktor kriminogen, yaitu: (1) pesatnya digitalisasi masyarakat; (2) rendahnya literasi digital; (3) lemahnya sistem keamanan informasi; (4) tingginya motivasi ekonomi pelaku; (5) sulitnya identifikasi pelaku; (6) perkembangan modus operandi yang sangat cepat; dan (6) belum optimalnya kapasitas aparat penegak hukum dalam investigasi digital. Kombinasi berbagai faktor tersebut menyebabkan cybercrime terus berkembang baik dari sisi jumlah maupun kompleksitas kasus (Budana, 2026).

Tabel 1. Faktor-Faktor Penyebab Cybercrime Berdasarkan Analisis Kriminologi

No	Faktor	Tingkat Pengaruh	Dampak
1	Perkembangan teknologi	Sangat Tinggi	Meningkatkan peluang kejahatan digital
2	Rendahnya literasi digital	Sangat Tinggi	Korban mudah ditipu
3	Motivasi ekonomi	Tinggi	Mendorong pelaku memperoleh keuntungan ilegal
4	Lemahnya keamanan sistem	Tinggi	Data mudah diretas
5	Anonimitas internet	Tinggi	Pelaku sulit diidentifikasi
6	Pembuktian elektronik	Sedang	Penyidikan menjadi lebih kompleks
7	Kerja sama internasional terbatas	Sedang	Penegakan hukum lintas negara kurang optimal

Interpretasi Hasil

Berdasarkan hasil penelitian, dapat dipahami bahwa cybercrime merupakan fenomena sosial yang tidak hanya dipengaruhi oleh perilaku individu pelaku, tetapi juga oleh perkembangan teknologi, perubahan pola aktivitas masyarakat, kondisi ekonomi, serta efektivitas sistem hukum. Pendekatan kriminologi menunjukkan bahwa pencegahan cybercrime harus dilakukan secara komprehensif melalui kombinasi kebijakan penal dan nonpenal. Pendekatan penal diwujudkan melalui penegakan hukum yang tegas terhadap pelaku, penguatan regulasi mengenai kejahatan siber, peningkatan kapasitas penyidik digital forensik, serta kerja sama internasional dalam pemberantasan kejahatan lintas negara. Sementara itu, pendekatan nonpenal dilakukan melalui peningkatan literasi digital masyarakat, penguatan sistem keamanan informasi pada instansi pemerintah maupun swasta, edukasi mengenai perlindungan data pribadi, serta pembangunan budaya keamanan siber (cybersecurity awareness). Dengan demikian, analisis kriminologi menunjukkan bahwa strategi penanggulangan cybercrime tidak cukup hanya mengandalkan penghukuman terhadap pelaku, tetapi juga harus berorientasi pada pencegahan melalui pengurangan peluang kejahatan, peningkatan pengawasan digital, dan penguatan kapasitas masyarakat sebagai pengguna teknologi informasi (Akbar, 2026).

B. Analisis Viktimologi terhadap Korban Kejahatan Siber

Viktimologi merupakan cabang ilmu yang mempelajari korban tindak pidana secara komprehensif, meliputi karakteristik korban, hubungan antara korban dengan pelaku, proses terjadinya viktimisasi, dampak yang dialami korban, serta bentuk perlindungan yang seharusnya diberikan oleh negara. Dalam perkembangan hukum pidana modern, korban tidak lagi dipandang

hanya sebagai alat pembuktian dalam proses peradilan, melainkan sebagai subjek hukum yang memiliki hak untuk memperoleh perlindungan, pemulihan, dan keadilan. Dalam konteks cybercrime, korban memiliki karakteristik yang berbeda dibandingkan korban kejahatan konvensional. Kejahatan yang terjadi di ruang digital sering kali menyebabkan kerugian yang bersifat multidimensional, yaitu kerugian ekonomi, psikologis, sosial, bahkan reputasi. Selain itu, dampak yang ditimbulkan dapat berlangsung dalam jangka waktu yang lama karena informasi atau data pribadi yang telah tersebar di internet sulit untuk dihapus sepenuhnya (An Nisya Nursabilah et al., 2025).

1. Karakteristik Korban Cybercrime

Hasil penelitian menunjukkan bahwa korban cybercrime berasal dari berbagai lapisan masyarakat tanpa memandang usia, jenis kelamin, pendidikan, maupun status ekonomi. Namun, kelompok yang memiliki tingkat kerentanan lebih tinggi meliputi pengguna internet dengan literasi digital rendah, lanjut usia, pelaku UMKM, pengguna media sosial yang aktif membagikan informasi pribadi, mahasiswa dan pelajar, serta masyarakat yang sering bertransaksi melalui layanan perbankan atau dompet digital. Kerentanan tersebut umumnya disebabkan oleh kurangnya pemahaman mengenai keamanan digital, rendahnya kewaspadaan terhadap modus kejahatan siber, serta belum optimalnya perlindungan data pribadi (Garnita & Kuswandi, 2025).

2. Bentuk Viktimisasi pada Cybercrime

Dalam perspektif viktimologi, viktimisasi adalah proses seseorang menjadi korban akibat suatu tindak pidana. Cybercrime menghasilkan berbagai bentuk viktimisasi yang dapat diklasifikasikan sebagai berikut.

a. Viktimisasi Ekonomi

Viktimisasi ekonomi merupakan dampak yang paling umum dialami korban cybercrime, berupa kehilangan saldo rekening, pencurian dana melalui layanan perbankan digital, penipuan transaksi daring, penyalahgunaan kartu kredit, pencurian aset digital, hingga pemerasan menggunakan ransomware. Kerugian yang ditimbulkan sangat bervariasi, mulai dari ratusan ribu hingga miliaran rupiah, bergantung pada jenis kejahatan dan nilai aset yang dimiliki korban.

b. Viktimisasi Psikologis

Selain mengalami kerugian finansial, korban cybercrime juga sering menghadapi dampak psikologis seperti kecemasan, stres, rasa takut menggunakan layanan digital, kehilangan rasa aman, depresi, dan trauma berkepanjangan. Tidak sedikit korban yang menyalahkan diri sendiri atas kejadian yang dialami, sehingga memengaruhi kepercayaan diri serta kualitas kehidupan sehari-hari.

c. Viktimisasi Sosial

Cybercrime juga menimbulkan dampak sosial berupa rusaknya reputasi, hilangnya kepercayaan dari keluarga maupun lingkungan kerja, penyebaran data pribadi, perundungan di dunia maya (cyberbullying), dan pengucilan sosial. Pada kasus pencurian identitas atau penyebaran konten pribadi tanpa izin, dampak sosial yang dialami korban bahkan dapat berlangsung lebih lama dibandingkan kerugian ekonomi (Apriyani et al., 2025).

Secondary Victimization

Secondary victimization adalah penderitaan tambahan yang dialami korban akibat respons yang kurang memadai dari lingkungan atau sistem peradilan pidana, seperti proses pelaporan yang rumit, lamanya penyidikan, kurangnya pemahaman aparat terhadap bukti elektronik, minimnya informasi mengenai perkembangan perkara, serta belum optimalnya perlindungan identitas korban. Kondisi ini dapat memperburuk tekanan psikologis yang dialami korban sehingga diperlukan

pendekatan **victim-oriented justice** yang berfokus pada perlindungan dan pemulihan hak-hak korban (Hera et al., 2026).

Analisis Berdasarkan Teori Viktimologi

A. Teori Benjamin Mendelsohn

Benjamin Mendelsohn mengemukakan bahwa korban dapat diklasifikasikan berdasarkan tingkat keterlibatannya dalam terjadinya tindak pidana. Dalam cybercrime, sebagian besar korban termasuk kategori **completely innocent victim**, yaitu korban yang sama sekali tidak memiliki niat maupun kontribusi terhadap terjadinya tindak pidana. Misalnya, seseorang yang rekening banknya diretas melalui kebocoran data pada sistem penyedia layanan. Namun demikian, terdapat pula korban yang menjadi lebih rentan akibat kurangnya pemahaman mengenai keamanan digital, seperti membagikan kode OTP, menggunakan kata sandi yang lemah, atau mengakses tautan yang tidak terpercaya. Meskipun demikian, kondisi tersebut tidak menghilangkan tanggung jawab pidana pelaku maupun hak korban untuk memperoleh perlindungan hukum (Annisa et al., 2025).

B. Lifestyle Exposure Theory

Lifestyle Exposure Theory menjelaskan bahwa gaya hidup seseorang memengaruhi tingkat risiko menjadi korban kejahatan. Dalam era digital, aktivitas seperti sering bertransaksi secara daring, menggunakan berbagai aplikasi digital, membagikan informasi pribadi di media sosial, mengakses jaringan internet publik, serta mengunduh aplikasi dari sumber yang tidak resmi dapat meningkatkan kerentanan terhadap cybercrime apabila tidak disertai dengan penerapan keamanan digital yang memadai. Teori ini menunjukkan bahwa perubahan pola hidup masyarakat digital turut berkontribusi terhadap meningkatnya risiko viktimisasi di ruang siber (Prof. Dr. Henny Saida Flora, 2026).

C. Opportunity Theory

Opportunity Theory menyatakan bahwa kejahatan terjadi karena adanya kesempatan yang dimanfaatkan oleh pelaku. Dalam cybercrime, kesempatan tersebut muncul akibat lemahnya keamanan akun, penggunaan kata sandi yang mudah ditebak, tidak adanya autentikasi dua faktor, rendahnya pengawasan terhadap transaksi elektronik, serta kurangnya kesadaran masyarakat dalam melindungi data pribadi. Semakin besar peluang yang tersedia, semakin tinggi pula risiko terjadinya kejahatan siber (Ahmad & Utari, 2025).

Analisis Perlindungan Korban

Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap korban cybercrime di Indonesia telah didukung oleh berbagai regulasi yang memberikan hak atas perlindungan hukum, kerahasiaan identitas, bantuan hukum, informasi perkembangan perkara, restitusi, pendampingan psikologis, dan rehabilitasi. Namun, implementasi perlindungan tersebut masih belum optimal karena terkendala oleh keterbatasan sumber daya, kompleksitas pembuktian digital, serta belum meratanya pemahaman aparat penegak hukum mengenai pendekatan viktimologi dalam penanganan korban kejahatan siber (Lubis, 2026).

Tabel 2. Bentuk Viktimisasi pada Korban Cybercrime

Jenis Viktimisasi	Dampak terhadap Korban	Tingkat Pengaruh
Ekonomi	Kehilangan uang dan aset digital	Sangat Tinggi
Psikologis	Trauma, stres, kecemasan	Sangat Tinggi
Sosial	Rusaknya reputasi dan hubungan sosial	Tinggi
Privasi	Kebocoran data pribadi	Sangat Tinggi
Hukum	Kesulitan memperoleh pemulihan hak	Sedang

Pembahasan

Hasil penelitian menunjukkan bahwa korban cybercrime tidak hanya mengalami kerugian ekonomi, tetapi juga menghadapi dampak psikologis dan sosial yang kompleks. Perspektif viktimologi menegaskan bahwa keberhasilan penanggulangan cybercrime tidak cukup diukur dari jumlah pelaku yang berhasil dipidana, tetapi juga dari sejauh mana negara mampu memberikan perlindungan dan pemulihan kepada korban. Pendekatan yang berorientasi pada korban menuntut adanya mekanisme yang lebih responsif, mulai dari penerimaan laporan, pendampingan selama proses penyidikan, perlindungan terhadap data pribadi, hingga pemberian restitusi dan rehabilitasi. Dalam praktiknya, korban masih sering menghadapi hambatan administratif, kurangnya informasi mengenai hak-haknya, serta lamanya proses penanganan perkara. Kondisi tersebut berpotensi menimbulkan secondary victimization yang memperburuk penderitaan korban. Selain itu, penelitian ini memperlihatkan bahwa tingkat literasi digital masyarakat memiliki hubungan erat dengan tingkat kerentanan menjadi korban. Oleh karena itu, strategi perlindungan korban harus dilakukan secara preventif melalui peningkatan literasi digital, edukasi mengenai keamanan siber, penguatan sistem perlindungan data pribadi, serta kerja sama antara pemerintah, aparat penegak hukum, penyelenggara sistem elektronik, lembaga pendidikan, dan masyarakat. Dengan demikian, analisis viktimologi menunjukkan bahwa perlindungan korban cybercrime harus menjadi bagian integral dari kebijakan penanggulangan kejahatan siber. Pendekatan tersebut tidak hanya berorientasi pada penghukuman pelaku, tetapi juga memastikan bahwa korban memperoleh pemulihan hak, rasa aman, dan akses terhadap keadilan sebagai wujud perlindungan hak asasi manusia dalam sistem peradilan pidana modern (Budana, 2026).

C. Analisis Perlindungan Hukum Korban Cybercrime di Indonesia

Perlindungan hukum terhadap korban merupakan salah satu indikator penting dalam sistem peradilan pidana modern. Paradigma hukum pidana yang sebelumnya lebih berorientasi pada penghukuman pelaku (offender oriented) kini mengalami perkembangan menuju sistem yang memberikan perhatian seimbang terhadap hak-hak korban (victim oriented justice). Dalam perkara cybercrime, perubahan paradigma tersebut menjadi semakin penting mengingat karakteristik kejahatan siber yang dapat menimbulkan kerugian ekonomi, psikologis, sosial, bahkan mengancam hak atas privasi seseorang. Di Indonesia, perlindungan korban cybercrime telah memperoleh dasar hukum melalui berbagai peraturan perundang-undangan. Namun demikian, efektivitas perlindungan tersebut masih dipengaruhi oleh berbagai faktor, seperti kualitas regulasi, kemampuan aparat penegak hukum, perkembangan teknologi informasi, serta tingkat kesadaran masyarakat mengenai keamanan digital (Akbar, 2026).

1. Analisis Regulasi Perlindungan Korban

a. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi regulasi utama dalam penanganan tindak pidana siber dengan mengatur berbagai bentuk kejahatan, seperti akses ilegal, intersepsi ilegal, manipulasi data elektronik, penipuan elektronik, penyebaran konten ilegal, dan pencurian informasi elektronik. Meskipun memberikan dasar hukum yang kuat bagi penegakan hukum, regulasi ini masih lebih berfokus pada pemidanaan pelaku dibandingkan pada mekanisme perlindungan dan pemulihan korban.

b. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan perlindungan terhadap hak privasi masyarakat melalui pengaturan hak pemilik data, seperti hak memperoleh informasi, memperbaiki, menghapus data, menarik persetujuan pemrosesan, dan memperoleh ganti kerugian atas penyalahgunaan data pribadi. Regulasi ini menjadi landasan

penting dalam mencegah dan menangani cybercrime yang berkaitan dengan kebocoran maupun penyalahgunaan data pribadi.

c. Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban

Undang-Undang Nomor 31 Tahun 2014 menjamin hak korban untuk memperoleh perlindungan keamanan, bantuan medis, rehabilitasi psikologis, bantuan hukum, restitusi, dan kompensasi. Namun, penerapannya dalam kasus cybercrime masih belum optimal karena mekanisme perlindungan yang tersedia lebih banyak dirancang untuk tindak pidana konvensional dibandingkan kejahatan berbasis teknologi (An Nisya Nursabilah et al., 2025).

2. Efektivitas Perlindungan Korban

a. Kendala Regulasi

Meskipun Indonesia telah memiliki berbagai regulasi terkait cybercrime, perlindungan korban masih menghadapi kendala berupa belum adanya pengaturan teknis yang komprehensif mengenai pemulihan korban, terbatasnya penerapan restitusi, proses ganti kerugian yang bergantung pada putusan pengadilan, serta perkembangan modus kejahatan siber yang lebih cepat dibandingkan pembaruan regulasi.

b. Kendala Penegakan Hukum

Penegakan hukum terhadap cybercrime masih menghadapi berbagai hambatan, seperti keterbatasan tenaga ahli digital forensik, kompleksitas pembuktian elektronik, penggunaan server di luar negeri, anonimitas pelaku, terbatasnya kerja sama internasional, serta lamanya proses penyidikan. Kondisi tersebut menyebabkan penyelesaian perkara cybercrime sering memerlukan waktu yang lebih panjang dibandingkan tindak pidana konvensional.

c. Kendala dari Sisi Korban

Dari sisi korban, rendahnya tingkat pelaporan masih menjadi tantangan karena banyak korban merasa malu, tidak memahami prosedur pelaporan, menganggap kerugiannya sulit dipulihkan, khawatir data pribadinya semakin tersebar, atau belum mengetahui hak-haknya sebagai korban. Akibatnya, jumlah kasus cybercrime yang dilaporkan diperkirakan masih lebih rendah dibandingkan jumlah kejadian yang sebenarnya (*dark number of crime*) (Garnita & Kuswandi, 2025).

Sintesis Analisis Kriminologi dan Viktimologi

Hasil penelitian menunjukkan bahwa pendekatan kriminologi dan viktimologi saling melengkapi dalam menjelaskan fenomena cybercrime. Perspektif kriminologi berfokus pada faktor penyebab munculnya kejahatan, karakteristik pelaku, peluang terjadinya tindak pidana, serta strategi pencegahan. Sebaliknya, perspektif viktimologi menitikberatkan pada karakteristik korban, dampak viktimisasi, kebutuhan korban, dan mekanisme pemulihan yang harus diberikan oleh negara. Integrasi kedua pendekatan tersebut menghasilkan pemahaman yang lebih komprehensif. Upaya penanggulangan cybercrime tidak cukup hanya dilakukan melalui penghukuman terhadap pelaku, tetapi juga harus memastikan bahwa korban memperoleh perlindungan hukum yang memadai, termasuk pemulihan ekonomi, psikologis, dan sosial (Apriyani et al., 2025).

Tabel 3. Perbandingan Perspektif Kriminologi dan Viktimologi

Aspek	Kriminologi	Viktimologi
Fokus Kajian	Penyebab kejahatan dan pelaku	Korban dan dampak kejahatan
Tujuan	Pencegahan dan penanggulangan kejahatan	Perlindungan dan pemulihan korban
Objek Analisis	Pelaku, lingkungan, faktor sosial	Korban, hak korban, proses viktimisasi

Pendekatan	Offender oriented	Victim oriented
Hasil yang Diharapkan	Menurunnya angka kejahatan	Terpenuhinya hak-hak korban

Model Perlindungan Korban Cybercrime yang Direkomendasikan

Berdasarkan hasil penelitian, perlindungan korban cybercrime perlu menerapkan model terpadu (*integrated victim protection model*) yang melibatkan pemerintah, aparat penegak hukum, penyelenggara sistem elektronik, lembaga perlindungan saksi dan korban, sektor perbankan, serta masyarakat. Model ini mencakup upaya pencegahan melalui peningkatan literasi digital, perlindungan awal dengan mekanisme pelaporan yang mudah dan respons cepat, penegakan hukum berbasis digital forensik, pemulihan korban melalui bantuan hukum, rehabilitasi dan restitusi, serta evaluasi kebijakan secara berkala agar mampu menyesuaikan dengan perkembangan teknologi dan modus kejahatan siber (Hera et al., 2026).

Implikasi Penelitian

Penelitian ini memiliki implikasi teoritis dan praktis. Secara teoritis, hasil penelitian memperkaya kajian kriminologi dan viktimologi dengan menunjukkan bahwa cybercrime merupakan fenomena multidimensional yang tidak dapat dijelaskan hanya melalui satu perspektif. Integrasi kedua disiplin ilmu memberikan pemahaman yang lebih utuh mengenai hubungan antara pelaku, korban, lingkungan digital, dan sistem hukum. Secara praktis, penelitian ini memberikan rekomendasi bagi pembentuk kebijakan untuk memperkuat regulasi mengenai perlindungan korban, meningkatkan kapasitas aparat penegak hukum dalam investigasi digital, mengoptimalkan mekanisme restitusi dan rehabilitasi, serta memperluas program literasi digital bagi masyarakat. Selain itu, penyelenggara sistem elektronik diharapkan menerapkan standar keamanan informasi yang lebih tinggi guna mencegah kebocoran data dan meminimalkan risiko terjadinya viktimisasi. Secara keseluruhan, hasil penelitian menunjukkan bahwa keberhasilan penanggulangan cybercrime tidak hanya ditentukan oleh efektivitas penindakan terhadap pelaku, tetapi juga oleh kemampuan negara dalam menjamin perlindungan hak-hak korban. Oleh karena itu, kebijakan hukum pidana di bidang kejahatan siber harus mengintegrasikan pendekatan kriminologi dan viktimologi agar tercipta sistem peradilan pidana yang lebih adil, responsif, dan berorientasi pada pemulihan korban (Annisa et al., 2025).

KESIMPULAN

Penelitian ini menunjukkan bahwa perkembangan teknologi informasi telah membawa perubahan mendasar terhadap karakteristik kejahatan di Indonesia. Cybercrime berkembang menjadi salah satu bentuk kejahatan modern yang memiliki kompleksitas tinggi karena memanfaatkan teknologi digital, bersifat lintas negara, menggunakan identitas anonim, serta didukung oleh perkembangan teknologi yang berlangsung sangat cepat. Kondisi tersebut menyebabkan penanganan cybercrime tidak lagi dapat dilakukan hanya melalui pendekatan hukum pidana konvensional, tetapi memerlukan pendekatan multidisipliner yang mengintegrasikan aspek hukum, teknologi informasi, kriminologi, dan viktimologi. Berdasarkan perspektif kriminologi, meningkatnya cybercrime dipengaruhi oleh berbagai faktor yang saling berkaitan, yaitu pesatnya perkembangan teknologi informasi, tingginya motivasi ekonomi pelaku, rendahnya literasi digital masyarakat, lemahnya sistem keamanan informasi, serta anonimitas yang diberikan oleh internet. Analisis menggunakan Routine Activity Theory, Rational Choice Theory, dan Social Learning Theory menunjukkan bahwa peluang melakukan cybercrime semakin besar ketika terdapat target yang rentan, pengawasan yang lemah, serta keuntungan yang diperoleh pelaku lebih besar daripada risiko yang dihadapi. Dengan demikian, penanggulangan cybercrime harus dilakukan melalui

kombinasi kebijakan penal dan nonpenal yang mencakup penegakan hukum, peningkatan keamanan siber, serta edukasi masyarakat. Dari perspektif viktimologi, penelitian ini menemukan bahwa korban cybercrime mengalami dampak yang jauh lebih kompleks dibandingkan kerugian ekonomi semata. Korban juga menghadapi tekanan psikologis, kehilangan rasa aman, kerusakan reputasi, penyalahgunaan data pribadi, serta berbagai bentuk secondary victimization yang muncul akibat proses penanganan perkara yang belum sepenuhnya berpihak kepada korban. Oleh karena itu, perlindungan terhadap korban harus mencakup aspek preventif, represif, dan rehabilitatif agar hak-hak korban dapat dipulihkan secara optimal.

DAFTAR REFERENSI

Ahmad, M. R. A., & Utari, I. S. (2025). Perlindungan Hukum Pengguna E-Commerce: Perspektif Viktimologi dalam Menghadapi Kejahatan Siber. *Bookchapter Hukum Dan Lingkungan*, *1*, 967–989. https://bookchapter.unnes.ac.id/index.php/hk/article/view/545

Akbar, R. M. F. (2026). TINJAUAN VIKTIMOLOGIS PENYEBARAN DATA PRIBADI: HAK RESTITUSI KORBAN DI ERA DIGITAL. *Jurnal Hukum Dan Kewarganegaraan*, *16*(7), 1–14.

An Nisya Nursabilah, Nazmi Viranha Khurulani, Anggia Prasanti, Dea Aulia Zuhra, Allyah Alicia Hg, & Nabila Nabanurohmah. (2025). Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Scam Serta Dampaknya Bagi Korban Sebagai Bentuk Viktimisasi Sekunder. *Hukum Inovatif : Jurnal Ilmu Hukum Sosial Dan Humaniora*, *2*(3), 168–187. https://doi.org/10.62383/humif.v2i3.1912

Annisa, K., Mahendra, P. K., & Rika, E. (2025). Perlindungan Hukum Terhadap Korban Kejahatan Siber di Indonesia Dalam Perspektif Hukum Internasional. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(6), 10563–10573.

Apriyani, R., Bulqis, B., Lestarika, D. P., Royani, F., Fadillah, A. N., Asriyani, A., Hardimen, H., Wardana, K. W., Setyowati, D., Adriani, F., & others. (2025). *Kriminologi dan Viktimologi*. CV. Gita Lentera. https://books.google.co.id/books?id=irdKEQAAQBAJ

Budana, K. E. (2026). Perlindungan Korban dalam Penyebaran Video Kecelakaan Lalu Lintas di Era Digital: Perspektif Viktimologi dan Hukum Positif Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(2), 2026–2035.

Garnita, C. F., & Kuswandi, K. (2025). Analisis Kriminologi dalam Tindak Pidana Pencurian Data Pribadi di Era Digital. *Indonesian Journal of Law and Justice*, *3*(2), 11. https://doi.org/10.47134/ijlj.v3i2.5288

Hera, M., Manik, A., Amelia, A., & Putri, A. (2026). Peran Korban dalam Tindak Pidana Penipuan Transaksi Elektronik : Perspektif Cyber Victimology. *Jurnal Kajian Hukum Dan Kebijakan Publik*, *3*(2), 899–906.

Lubis, T. L. (2026). PERLINDUNGAN HUKUM TERHADAP KORBAN KEJAHATAN DITINJAU DARI PERSPEKTIF VIKTIMOLOGI. *Jurnal Hukum Dan Kewarganegaraan*, *16*(6), 1–10. https://repositorio.ufsc.br/bitstream/handle/123456789/186602/PPAU0156-D.pdf?sequence=-1&isAllowed=y%0Ahttp://journal.stainkudus.ac.id/index.php/equilibrium/article/view/1268/1127%0Ahttp://www.scielo.br/pdf/rae/v45n1/v45n1a08%0Ahttp://dx.doi.org/10.1016/j

Prof. Dr. Henny Saida Flora, S. H. M. H. M. K. M. H. K. (2026). *VIKTIMOLOGI (Perlindungan Hukum Terhadap Korban Kejahatan)*. CV. NUSANTARA PRESS INDONESIA. https://books.google.co.id/books?id=fuvREQAAQBAJ