



Perlindungan Hukum Bagi Korban Tindak Pidana *Cyber Scam* Serta Dampaknya Bagi Korban Sebagai Bentuk Viktimisasi Sekunder

An Nisya Nursabilah^{1*}, Nazmi Viranha Khurulani², Anggia Prasanti³, Dea Aulia Zuhra⁴, Allyah Alicia Hg⁵, Nabila Nabanurohmah⁶.

¹⁻⁶ Universitas Sultan Ageng Tirtayasa, Indonesia.

E-mail: 1111220044@untirta.ac.id¹, 1111220045@untirta.ac.id², 1111220047@untirta.ac.id³, 1111220152@untirta.ac.id⁴, 1111220154@untirta.ac.id⁵, 1111220323@untirta.ac.id⁶

Abstrack. *The rapid development of digital technology has increased the potential for cybercrime, including cyber scams, which cause great losses to victims both materially and psychologically. In this context, the state is obliged to provide legal protection to victims, but in practice there are still many legal gaps and the implementation is not optimal. This research aims to analyze the form of legal protection for victims of cyber scams and the impact of these crimes in triggering secondary victimization. This research uses an empirical juridical method with a descriptive-analytical approach that combines primary data from observations and interviews and secondary data from legal literature and legislation. The results show that despite the existence of legal umbrellas such as the ITE Law and the Witness and Victim Protection Law, the victim protection mechanism has not been running effectively. Victims not only experience economic losses (primary victimization), but also psychological, social, and legal pressure from an unresponsive system (secondary victimization). The contribution of this research provides urgency for improving the regulation and implementation of victim-oriented legal protection, as well as the importance of digital literacy and empathy of legal officers in handling cybercrime cases.*

Keywords: *cyber scam; Legal protection; secondary victimization; UU ITE; victims.*

Abstrak. Pesatnya perkembangan teknologi digital telah meningkatkan potensi terjadinya kejahatan siber, termasuk *cyber scam*, yang menimbulkan kerugian besar bagi korban baik secara materiil maupun psikologis. Dalam konteks ini, negara berkewajiban untuk memberikan perlindungan hukum kepada korban, namun dalam praktiknya masih terdapat banyak kekosongan hukum dan pelaksanaan yang belum optimal. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap korban tindak pidana *cyber scam* dan dampak kejahatan tersebut dalam memicu viktimisasi sekunder. Penelitian ini menggunakan metode yuridis empiris dengan pendekatan deskriptif-analitis yang menggabungkan data primer dari observasi dan wawancara serta data sekunder dari literatur hukum dan peraturan perundang-undangan. Hasil penelitian menunjukkan bahwa meskipun telah terdapat payung hukum seperti UU ITE dan UU Perlindungan Saksi dan Korban, mekanisme perlindungan korban belum berjalan secara efektif. Korban tidak hanya mengalami kerugian ekonomi (viktimisasi primer), tetapi juga tekanan psikologis, sosial, dan hukum dari sistem yang tidak responsif (viktimisasi sekunder). Kontribusi penelitian ini memberikan urgensi bagi perbaikan regulasi dan pelaksanaan perlindungan hukum yang berorientasi pada korban, serta pentingnya literasi digital dan empati aparat hukum dalam menangani kasus kejahatan siber.

Kata Kunci: penipuan cyber; Perlindungan hukum; viktimisasi sekunder; UU ITE; korban.

1. PENDAHULUAN

Perkembangan teknologi dan informasi telah memberikan dampak yang sangat signifikan bagi kehidupan manusia di era modern. Saat ini, hampir semua aspek kehidupan dipengaruhi oleh keberadaan teknologi yang terus berkembang pesat. Revolusi teknologi membawa banyak kemudahan bagi manusia dalam menjalankan aktivitas sehari-hari, mulai dari pekerjaan, komunikasi, hingga transaksi ekonomi. Dunia siber memungkinkan publik untuk mengakses berbagai data, berita, dan pengetahuan kapan saja dan di mana saja. Fenomena ini telah menciptakan masyarakat yang lebih terhubung secara global dan membuka peluang bagi berbagai sektor untuk berkembang. Indonesia sebagai negara berkembang juga tidak

ketinggalan dalam memanfaatkan teknologi ini. Terbukti bahwa tercatat jumlah individu yang terhubung dengan internet di Indonesia saat ini mencapai 212 juta jiwa, dengan tingkat penetrasi internet sebesar 74,6% dengan sebanyak 143 juta identitas pengguna media sosial tercatat pada Januari 2025, mencakup 50,2% dari total populasi (Simon Kemp, 2025). Jika dahulu internet hanya dapat dinikmati oleh kalangan tertentu seperti masyarakat perkotaan atau golongan ekonomi atas, kini seluruh lapisan masyarakat memiliki akses terhadap teknologi ini berkat semakin terjangkaunya perangkat digital dan paket data internet (Astri, 2024).

Tren penggunaan internet di Indonesia menunjukkan peningkatan yang signifikan. Hal ini menunjukkan bahwa teknologi digital telah menjadi bagian integral dari kehidupan masyarakat Indonesia. Dengan populasi yang besar dan tingkat adopsi teknologi yang terus meningkat, Indonesia memiliki potensi besar untuk terus berkembang di era digital. Namun demikian, perkembangan ini juga membawa tantangan tersendiri seperti ancaman keamanan siber dan perlunya literasi digital bagi masyarakat agar dapat memanfaatkan teknologi secara bijak dan maksimal (Madinah Mokobombang, Zulfikri Darwis, & Sabil Mokodenseho, 2023).

Namun, di tengah berbagai keuntungan tersebut, muncul ancaman serius berupa kejahatan dunia maya atau *cyber scam*. Kejahatan dunia maya merujuk pada tindakan kriminal yang dilakukan dengan memanfaatkan teknologi informasi sebagai alat utama. *Cyber scam* tidak hanya merugikan individu atau perusahaan secara finansial dan psikologis, tetapi juga berpotensi mengancam keamanan nasional. Pelaku kejahatan dunia maya dapat menyasar instansi pemerintah, bank, atau bahkan infrastruktur vital negara. Untuk mengurangi risiko kejahatan dunia maya, diperlukan upaya pencegahan yang serius dari berbagai pihak. Masyarakat perlu meningkatkan kesadaran tentang keamanan digital melalui edukasi mengenai ancaman *cyber scam* ini. Selain itu, intervensi dari *stakeholder* dalam memperkuat sistem keamanan digital mereka dengan teknologi enkripsi dan *firewall* canggih sangat dibutuhkan dalam mengatasi dilema ini. Pemerintah perlu memberikan payung hukum yang jelas terkait dengan kejahatan dunia maya seiring dengan pertumbuhan zaman. Saat ini, peraturan yang berlaku di Indonesia yang mengatur terkait kejahatan *cyber* yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

Korban *cyber scam* tidak hanya mengalami kerugian secara materiil, tetapi juga dapat mengalami kerugian psikologis dan sosial yang mendalam. Fenomena ini dapat menyebabkan viktimisasi sekunder, yaitu kondisi di mana korban mengalami penderitaan lebih lanjut akibat dari proses hukum, perlakuan aparat penegak hukum, maupun stigma dari lingkungan sosial. Sering kali, korban tidak hanya kehilangan uang atau data pribadi, tetapi juga menghadapi kesulitan dalam mendapatkan perlindungan hukum yang memadai, serta kurangnya empati dari

masyarakat maupun aparat penegak hukum dalam menangani kasus tersebut (Tanthawi, Dahlan Ali, 2017).

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan kerangka hukum yang sangat penting dalam mengatur berbagai aspek transaksi elektronik dan perlindungan data di era digital di Indonesia. Dengan pesatnya perkembangan teknologi informasi dan komunikasi (TIK), UU ITE berfungsi untuk memberikan kepastian hukum serta melindungi hak-hak individu maupun entitas dalam transaksi elektronik. Dalam konteks ini, UU ITE berperan sebagai *lex specialis* yang mengatur berbagai bentuk penipuan dan kejahatan siber yang terjadi melalui media sosial dan platform digital lainnya. Keberadaan undang-undang ini menjadi semakin krusial mengingat tingginya tingkat adopsi teknologi di masyarakat (Rachmat, 2023).

Namun, implementasi UU ITE tidak tanpa tantangan. Salah satu masalah utama adalah ketidakjelasan dalam beberapa ketentuannya, yang dapat menyulitkan proses penegakan hukum. Penelitian menunjukkan bahwa terdapat kekosongan hukum dalam perlindungan hukum terhadap korban penipuan melalui media sosial yang diatur dalam UU ITE. Meskipun undang-undang ini telah mengakui alat bukti elektronik, masih terdapat kekurangan dalam pengaturan prosedural terkait penggunaan alat bukti tersebut. Hal ini menunjukkan perlunya pembaruan dan penyesuaian regulasi agar UU ITE dapat berfungsi secara efektif dalam menghadapi tantangan kejahatan siber yang terus berkembang (Sedau, K. S., Masu, R. R., & Tungga, 2023).

Perubahan-perubahan ini sangat diperlukan agar regulasi mampu mengikuti dinamika dunia digital yang semakin kompleks dan memberikan perlindungan hukum yang lebih komprehensif bagi masyarakat. Misalnya, pada Desember 2023, Rancangan Undang-Undang tentang Perubahan Kedua atas UU ITE disahkan untuk memperkuat jaminan pengakuan serta penghormatan atas hak dan kebebasan individu dalam ruang digital. Perubahan tersebut mencakup pengaturan mengenai identitas digital, perlindungan anak dalam sistem elektronik, serta kewenangan Penyidik Pegawai Negeri Sipil (PPNS) dalam menangani tindak pidana siber (Karolus Charlaes, Aziz, Rahmad, & Sunarto, 2025).

Penelitian yang dilakukan oleh (Maya Sri Novita, 2025) dalam penelitiannya berjudul “Pentingnya Perlindungan Hukum Bagi Korban Tindak Pidana Penipuan dalam Proses Transaksi Jual Beli Secara *Online (E-Commerce)*” menyoroti maraknya kasus penipuan dalam transaksi daring yang dilakukan melalui berbagai platform e-commerce. Penelitian ini menyimpulkan bahwa meskipun terdapat perangkat hukum seperti UU ITE, KUHP, dan UU Perlindungan Konsumen, implementasi perlindungan terhadap korban masih menghadapi

kendala signifikan, seperti sulitnya penelusuran pelaku, lemahnya penegakan hukum, dan belum optimalnya pemberian ganti rugi terhadap korban. Maya mengusulkan penguatan literasi hukum masyarakat serta sinergi antara teknologi, regulasi, dan edukasi sebagai solusi menyeluruh dalam upaya memberikan perlindungan hukum yang efektif.

Selanjutnya, dalam penelitian (Yunus Darmono, 2023) berjudul “Perlindungan Hukum terhadap Korban Tindak Pidana *Cyber Crime* di Indonesia”, fokus utama diarahkan pada pentingnya posisi korban dalam sistem hukum positif Indonesia. Penelitian ini mengkritisi UU ITE yang lebih berorientasi pada pelaku kejahatan, sementara posisi korban justru kurang diperhatikan secara eksplisit. Yunus menegaskan bahwa meskipun UU No. 31 Tahun 2014 tentang Perlindungan Saksi dan Korban memberikan sejumlah hak seperti restitusi dan kompensasi, dalam praktiknya, hak-hak tersebut sering kali tidak diakses oleh korban kejahatan siber. Ia mengusulkan agar pemerintah menyempurnakan regulasi melalui pembentukan instrumen hukum yang secara spesifik mengatur hak dan perlindungan korban kejahatan digital.

Berbeda dengan kedua penelitian tersebut, penelitian ini akan mengkaji secara lebih mendalam mengenai perlindungan hukum terhadap korban *cyber scam*, khususnya dalam kasus-kasus penipuan digital seperti pembelian pulsa dan tiket konser palsu, serta menganalisis bentuk-bentuk viktimisasi sekunder yang dialami korban. Viktimisasi sekunder merupakan kondisi di mana korban tidak hanya dirugikan oleh pelaku, tetapi juga oleh sistem hukum, masyarakat, atau lingkungan sekitarnya, misalnya melalui pengabaian pelaporan, tidak adanya pemulihan kerugian, atau stigma sosial. Dengan demikian, penelitian ini tidak hanya membahas aspek normatif perlindungan korban, tetapi juga dampak lanjutan yang ditimbulkan setelah korban mengalami *cyber scam*, yang belum sepenuhnya diuraikan dalam dua penelitian terdahulu. Penelitian ini bertujuan untuk mengisi kekosongan tersebut serta memberikan landasan bagi perbaikan kebijakan dan mekanisme perlindungan korban dalam konteks kejahatan siber modern.

Oleh karena itu, penting untuk mengkaji bagaimana bentuk perlindungan hukum yang dapat dan seharusnya diberikan kepada korban tindak pidana *cyber scam*, serta bagaimana dampak psikologis dan sosial dari kejahatan ini dapat dikategorikan sebagai bentuk viktimisasi sekunder. Dengan memahami kedua aspek tersebut, diharapkan dapat dirumuskan langkah-langkah yang lebih komprehensif untuk meningkatkan perlindungan korban dan mendorong sistem hukum yang lebih responsif terhadap kejahatan siber yang terus berkembang.

2. METODOLOGI PENELITIAN

Metode yang digunakan adalah metode yuridis empiris, yang merupakan pendekatan yang mengintegrasikan kajian normatif dengan observasi terhadap praktik hukum yang berlangsung di masyarakat (Arikunto, 2012). Metode ini bertujuan untuk menganalisis dan memahami fenomena hukum tidak hanya dari segi norma-norma yang tertulis, tetapi juga dari realitas dan dinamika sosial yang memengaruhi penerapan hukum. Dengan demikian, penelitian ini diharapkan dapat memberikan gambaran yang komprehensif mengenai implementasi hukum dalam konteks yang lebih luas. Pendekatan yang digunakan dalam penelitian dengan metode yuridis empiris adalah pendekatan yang menggabungkan aspek normatif dan empiris. Pendekatan ini bertujuan untuk mengintegrasikan analisis terhadap hukum sebagai norma tertulis dengan fakta-fakta sosial yang terjadi di lapangan, sehingga menghasilkan pemahaman yang komprehensif mengenai implementasi hukum dalam konteks sosial (Abdulkadir Muhammad, 2004).

Spesifikasi penelitian bersifat deskriptif analitis, di mana peneliti berusaha untuk menggambarkan dan menganalisis keadaan atau gejala tertentu yang berkaitan dengan permasalahan hukum yang diteliti. Penelitian ini akan mengidentifikasi dan menjelaskan berbagai faktor yang memengaruhi pelaksanaan norma hukum serta dampaknya terhadap masyarakat. Dalam hal pengumpulan data, penelitian ini akan menggunakan jenis data primer dan sekunder. Data primer akan diperoleh melalui observasi langsung di lapangan untuk mengumpulkan fakta-fakta empiris mengenai penerapan hukum dalam praktik. Sementara itu, data sekunder akan dikumpulkan melalui kajian literatur, dokumen resmi, peraturan perundang-undangan, serta sumber-sumber tertulis lainnya yang dapat mendukung analisis dan pemahaman terhadap isu hukum yang sedang diteliti (Waluyo, 2002).

Metode analisis data akan dilakukan secara deskriptif kualitatif. Peneliti akan mengelompokkan data berdasarkan sub-aspek yang relevan dan melakukan interpretasi terhadap setiap sub-aspek tersebut. Analisis ini bertujuan untuk memberikan makna pada setiap temuan serta memahami hubungan antara berbagai faktor yang memengaruhi penerapan hukum. Dengan pendekatan ini, diharapkan hasil penelitian dapat memberikan kesimpulan yang jelas dan mendalam mengenai permasalahan hukum yang diteliti serta memberikan rekomendasi kebijakan yang bermanfaat bagi pengembangan sistem hukum di Indonesia (Narbuko & Achmadi, 2001).

3. HASIL DAN PEMBAHASAN

Perlindungan Hukum terhadap Korban Kejahatan Cyberscam

Kejahatan di dunia maya muncul sebagai konsekuensi negatif dari kemajuan teknologi. Beragam bentuk dan jenis kejahatan ini menimbulkan dampak terhadap perlindungan hukum bagi para penggunanya. Hal ini menjadi penting karena setiap individu berhak mendapatkan perlindungan yang sesuai dengan nilai harkat dan martabat kemanusiaannya. Sebagai bentuk tanggung jawab negara dalam melindungi warganya, negara harus memberikan jaminan hukum serta mengambil langkah nyata untuk melindungi masyarakat dari berbagai tindak kejahatan atau perilaku menyimpang, baik yang terjadi di dunia nyata maupun di ranah digital.

Saat ini, landasan hukum yang digunakan untuk menangani kasus-kasus kejahatan dunia maya (*cybercrime*) adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Hadirnya UU ITE ini sebagai respons dari perkembangan dan kemajuan Teknologi Informasi yang demikian pesat yang telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru. Kehadiran UU ITE diharapkan mampu memberikan perlindungan hukum bagi masyarakat pengguna teknologi informasi di Indonesia. Hal ini menjadi krusial mengingat jumlah pengguna internet yang terus meningkat setiap tahunnya. Di satu sisi, pertumbuhan penggunaan internet memberikan berbagai kemudahan dalam menjalankan aktivitas sehari-hari. Namun di sisi lain, hal ini juga membuka peluang bagi oknum-oknum tertentu untuk melakukan tindakan kriminal. Perkembangan teknologi tidak hanya memengaruhi cara hidup dan pola pikir masyarakat, tetapi juga menyebabkan maraknya kejahatan berbasis teknologi informasi. Fenomena *cybercrime* yang tumbuh pesat dan melintasi batas-batas negara ini memang patut diwaspadai, mengingat karakteristiknya yang berbeda dengan bentuk kejahatan konvensional (Wahyudi, 2013).

Maraknya pengguna internet di Indonesia, khususnya media sosial, memicu tantangan yang besar terhadap tingginya tindak kejahatan yang terjadi dengan memanfaatkan kemajuan teknologi. Bahwa pada tahun 2025 ini diprediksi akan menjadi tahun yang penuh tantangan di ranah siber dengan semakin canggihnya teknologi secara global (Berita Keamanan Siber, 2025). Hal tersebut tentunya menjadi dilema yang besar terhadap tindak pidana *cybercrime* yang dapat mengancam pengguna internet, khususnya media sosial. Meskipun dunia *cyber* adalah dunia virtual, hukum tetap diperlukan untuk mengatur tindakan masyarakat karena dua alasan. *Pertama*, masyarakat di dunia maya adalah masyarakat di dunia nyata, yang memiliki nilai dan kepentingan yang harus dilindungi. *Kedua*, transaksi yang dilakukan oleh masyarakat

di dunia maya memiliki dampak dalam dunia nyata, baik secara ekonomi maupun non-ekonomi (Wahyudi, 2013).

Kejahatan yang berkaitan dengan teknologi informasi secara umum dapat diklasifikasikan ke dalam dua kategori utama. Pertama, kejahatan yang memiliki tujuan untuk merusak atau menyerang sistem dan jaringan komputer. Kedua, kejahatan yang memanfaatkan komputer atau internet sebagai sarana untuk menjalankan aksi kriminal (Saputra, Soesanto, & Cahyaningtyas, 2024). Penyalahgunaan teknologi informasi yang dilakukan melalui perangkat komputer dan jaringan internet dapat menimbulkan kerugian bagi individu, masyarakat, bahkan negara. Tindakan ini biasanya dilakukan oleh peretas (*hacker*) atau kelompok perusak sistem (*cracker*) dari lokasi tertentu tanpa sepengetahuan korban, yang dapat mengakibatkan kerugian dalam bentuk moral, materiil, maupun waktu akibat rusaknya data. Untuk menanggulangi kejahatan siber (*cybercrime*), diperlukan aparat penegak hukum yang memiliki pemahaman dan kemampuan dalam bidang teknologi informasi.

Namun, sangat disayangkan bahwa salah satu kendala utama yang dihadapi oleh para korban adalah kurangnya pengetahuan tentang komputer dan internet, sehingga banyak dari mereka tidak mengetahui cara melaporkan tindak pidana yang dialaminya. Sejalan dengan penuturan dari Alma Nursalsabila, yang merupakan korban dari tindak pidana *cyberscam* penipuan, bahwa ia mengatakan bingung dan tidak tahu harus melapor kemana ketika menyadari bahwa ia menjadi korban dari *cyberscam* penipuan tersebut (Alma Nursalsabila, 2025). Pun, hal yang sama terjadi pada Diera A. yang merupakan korban *cyberscam* penipuan tiket *online* pada *platform* instagram, mengatakan tidak tahu harus melakukan pengaduan kemana dan membiarkan kejadian tersebut tanpa adanya tindak lanjut lagi setelah menyadari ia menjadi korban dari penipuan tiket *online* di sosial media (Diera A., 2025). Hal tersebut memungkinkan pelaku untuk melakukan tindak kejahatan terus-menerus tanpa adanya efek jera atau mendapatkan sanksi pidana, sehingga korban dari *cyberscam* ini akan meningkat.

Akibat kejahatan siber (*cybercrime*) menimbulkan banyaknya korban yang dirugikan. Misalnya korban kejahatan penipuan melalui internet maupun media *online* lainnya. Dalam Pasal 28 Ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang berbunyi: “*Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.*” Dalam pasal tersebut mengatur terkait larangan terhadap perbuatan dalam transaksi elektronik, khususnya terkait penyebaran informasi palsu dan menyesatkan yang dilakukan secara sengaja dan tanpa hak, serta berpotensi merugikan konsumen (Rachmat, 2022).

Sementara itu, ketentuan mengenai sanksi pidana atas pelanggaran terhadap Pasal 28 Ayat (1) diatur dalam Pasal 45A Ayat (1) UU ITE yang berbunyi:

- (1). Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- (2). Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pasal 28 Ayat (1) UU ITE dapat diartikan sebagai ketentuan yang mengatur tindakan penyampaian informasi yang tampak seolah-olah benar, khususnya dalam konteks penjualan barang secara daring. Namun, apabila ditelaah lebih mendalam, unsur-unsur yang tercantum dalam pasal tersebut masih dianggap belum sepenuhnya mencakup karakteristik perbuatan yang menyampaikan informasi palsu dalam transaksi jual beli di dunia maya. Berbeda dengan Pasal 378 KUHP, yang secara rinci menguraikan unsur-unsur dalam tindak pidana penipuan berbasis informasi fiktif. Perbedaan ini menjadi landasan penting untuk meninjau lebih jauh efektivitas perlindungan hukum yang diberikan oleh UU ITE terhadap korban penipuan melalui internet (Rachmat, 2022).

Perlindungan terhadap korban kejahatan sangatlah penting, karena masyarakat dipandang sebagai suatu sistem kepercayaan yang telah melembaga (*system of institutionalized trust*). Kepercayaan ini terwujud melalui norma-norma yang tertanam dalam institusi-institusi formal, seperti kepolisian, kejaksaan, dan pengadilan. Ketika terjadi tindak kejahatan terhadap individu, hal tersebut dapat merusak tatanan kepercayaan yang telah dibangun dalam masyarakat. Maka, pengaturan dalam hukum pidana maupun hukum lainnya yang berkaitan dengan korban memiliki peran penting sebagai upaya untuk memulihkan dan memperkuat kembali sistem kepercayaan tersebut (Dermawan, 2019).

Kedua, perlunya perlindungan terhadap korban juga didasarkan pada konsep kontrak sosial dan prinsip solidaritas, di mana negara memiliki hak monopoli atas seluruh respons sosial terhadap tindak kejahatan, termasuk pelarangan terhadap tindakan-tindakan yang bersifat pribadi. Oleh karena itu, ketika terjadi kejahatan, negara berkewajiban untuk memberikan

perhatian menyeluruh kepada para korban, baik melalui peningkatan layanan maupun melalui pengaturan yang menjamin hak-hak mereka. Ketiga, perlindungan terhadap korban juga berkaitan dengan salah satu tujuan dari pemidanaan, yaitu penyelesaian konflik. Penyelesaian atas konflik yang muncul akibat tindak pidana bertujuan untuk memulihkan keseimbangan sosial serta menciptakan rasa damai dalam masyarakat (Didik M & Arief, 2005).

Dalam kasus tindak pidana yang terjadi dalam transaksi elektronik, seperti penipuan melalui internet, korban merupakan pihak yang paling merasakan penderitaan dan kerugian. Hal tersebut sangat penting bagi negara untuk memberikan perlindungan yang memadai kepada mereka. Hak-hak korban harus diakui dan dijamin sebagai bagian dari prinsip kesetaraan di hadapan hukum (*equality before the law*), yang menjamin perlakuan yang adil bagi setiap individu tanpa diskriminasi. Sayangnya, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) belum secara tegas mengatur mekanisme perlindungan bagi korban yang mengalami tindak pidana dalam transaksi elektronik. Ketentuan dalam UU ITE hanya secara eksplisit menyebutkan hak korban apabila terjadi tindak pidana, seperti penipuan melalui internet, yaitu hak untuk memperoleh penyelesaian perkara dan menuntut pertanggungjawaban pidana terhadap pelaku kejahatan. Namun, hak-hak korban diatur dalam Pasal 5 (1) Undang-Undang Republik Indonesia Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi Dan Korban, yaitu:

Pasal 5 (1) Saksi dan Korban berhak:

- a. memperoleh perlindungan atas keamanan pribadi, Keluarga, dan harta bendanya, serta bebas dari Ancaman yang berkenaan dengan kesaksian yang akan, sedang, atau telah diberikannya;
- b. ikut serta dalam proses memilih dan menentukan bentuk perlindungan dan dukungan keamanan;
- c. memberikan keterangan tanpa tekanan;
- d. mendapat penerjemah;
- e. bebas dari pertanyaan yang menjerat;
- f. mendapat informasi mengenai perkembangan kasus;
- g. mendapat informasi mengenai putusan pengadilan;
- h. mendapat informasi dalam hal terpidana dibebaskan;
- i. dirahasiakan identitasnya;
- j. mendapat identitas baru;
- k. mendapat tempat kediaman sementara;
- l. mendapat tempat kediaman baru;

- m. memperoleh penggantian biaya transportasi sesuai dengan kebutuhan;
- n. mendapat nasihat hukum;
- o. memperoleh bantuan biaya hidup sementara sampai batas waktu Perlindungan berakhir; dan/atau
- p. mendapat pendampingan.

Hak korban untuk menuntut pemidanaan terhadap pelaku tindak pidana berkaitan erat dengan tujuan dari pemidanaan itu sendiri, yaitu sebagai upaya pencegahan terhadap terulangnya kejahatan di masa mendatang. Dalam konteks UU ITE, hak korban terhadap pemidanaan pelaku tindak pidana transaksi elektronik tercermin melalui ketentuan pidana yang diatur dalam Pasal 45 hingga Pasal 52. Secara khusus, hak korban terhadap pemidanaan pelaku penipuan melalui internet diatur dalam Pasal 45 Ayat (1) UU ITE, yang menetapkan sanksi pidana berupa hukuman penjara dan denda bagi pelaku kejahatan tersebut (ERLYNA & Isnawati, 2024). Hak korban penipuan melalui internet terkait dengan penyelesaian perkara dapat dipahami melalui ketentuan hukum formil dalam UU ITE, khususnya yang mengatur mengenai penyidikan, yang tercantum dalam Pasal 42 hingga Pasal 44 UU ITE. Selain diatur oleh UU ITE, hak korban dalam penyelesaian perkara juga sangat berkaitan dengan ketentuan dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang mengatur prosedur penyelesaian perkara pidana.

Terkait dengan korban tindak pidana, seperti halnya korban penipuan melalui internet, Kitab Undang-Undang Hukum Acara Pidana (KUHAP) telah mengatur beberapa hak bagi korban kejahatan. Namun, hak-hak yang diberikan kepada korban dalam KUHAP tergolong sangat terbatas, jika dibandingkan dengan hak-hak yang diberikan kepada tersangka atau terdakwa (Rachmat, 2022). Kasus penipuan *online* korban seringkali lebih menuntut ganti rugi yang bersifat materil kepada si pelaku agar mendapatkan haknya di kembalikan karena kerugian yang di dapatkan oleh korban itu sendiri dan bentuk pertanggungjawaban pelaku penipuan *online*. Akan tetapi hal itu belum sepenuhnya terealisasikan karena belum ada yang secara sah mengatur tentang bagaimana ganti rugi kepada korban penipuan *online* itu sendiri.

Sejalan dengan penuturan dari Alma Nursalsabila dan Diera A., bahwa sebagai korban, mereka tidak dapat meminta ganti rugi kepada pelaku dikarenakan pelaku langsung melakukan tindakan dengan menutup semua akses yang dimiliki dan mem-blokir nomor dan akun korban setelah berhasil melakukan tindakan penipuan terhadap korban (Alma Nursalsabila, 2025). Sehingga, korban tidak dapat meminta ganti rugi atau meminta uangnya kembali setelah penipuan itu terjadi dan uang yang sudah mereka *transfer* kepada pelaku tidak dapat kembali lagi (Diera A., 2025).

Pentingnya ganti rugi kepada korban penipuan transaksi *online* merupakan bentuk dari tercapainya hak-hak korban yaitu salah satunya bentuk keadilan. Dalam Undang-Undang ITE baik tahun 2008 maupun tahun 2016 dapat dilihat bahwa hanya ada satu pasal pidana pokok dan acaman pidana yang diberikan kepada pelaku tetapi belum menjelaskan bagaimana perlindungan kepada korban, perlindungan apa seperti apa yang bisa didapatkan korban setelah kasus selesai dengan kerugian materil dan imateril diderita oleh korban. Ganti rugi bagi korban yang dirugikan merupakan satu perlindungan hukum kepada korban dimana korban dapat mendapatkan kepastian, korban tidak hanya dilindungi dengan saksi hukum tetapi bagaimana tercapainya hak-hak korban setelahnya (Indrawan & Permatasari, 2022).

Maraknya kejahatan siber di era digital menuntut negara untuk tidak hanya hadir dalam bentuk regulasi, tetapi juga dalam pelaksanaan yang efektif demi memberikan perlindungan nyata bagi para korban. Meskipun Undang-Undang ITE telah menjadi payung hukum dalam menangani tindak pidana di ranah elektronik, namun belum sepenuhnya mengakomodasi kebutuhan korban, khususnya dalam aspek pemulihan hak, termasuk ganti rugi atas kerugian yang dialami. Perlindungan hukum seharusnya tidak berhenti pada pemberian sanksi pidana terhadap pelaku, tetapi juga mencakup pemulihan kondisi korban secara menyeluruh, baik secara materiil maupun imateriil. Dalam hal ini, diperlukan penguatan sistem hukum yang berpihak pada korban, termasuk peningkatan literasi digital, kejelasan mekanisme pengaduan, dan pemenuhan hak-hak korban sebagaimana yang telah diatur dalam UU Perlindungan Saksi dan Korban. Negara, sebagai pemegang mandat konstitusional untuk melindungi segenap warganya, wajib menjamin rasa aman dan keadilan, termasuk di dunia maya yang kini menjadi bagian tak terpisahkan dari kehidupan. *Cyber scam* adalah bentuk kejahatan digital yang dilakukan melalui internet dengan tujuan untuk menipu dan mendapatkan keuntungan dari korban. Istilah ini merujuk pada segala tindakan penipuan yang dirancang untuk mencuri uang, barang, atau data pribadi dari individu atau organisasi. masyarakat modern.

Dampak Tindak Pidana *Cyber Scam* terhadap Korban dalam Memicu Viktimisasi Sekunder

Tindak pidana adalah perbuatan yang dilarang oleh hukum dan dapat dikenai sanksi pidana. Dalam konteks hukum, istilah ini berasal dari bahasa Belanda "*strafbaar feit*" yang mencakup berbagai bentuk pelanggaran hukum baik yang bersifat aktif maupun pasif. Moeljatno menekankan bahwa tindak pidana adalah perbuatan yang dilarang dan diancam dengan sanksi pidana bagi siapa saja yang melanggarnya (P.A.F., Lamintang, 2011). Seiring dengan perkembangan teknologi dan dinamika sosial yang semakin kompleks, bentuk-bentuk tindak pidana pun mengalami transformasi.

Perkembangan teknologi informasi yang terjadi kini telah mencapai titik puncaknya. Hal ini dapat dilihat dari pesatnya inovasi dan fitur-fitur yang terus berkembang dalam ranah teknologi digital, khususnya teknologi komputer berbasis internet. Dampak dari kemajuan ini membuat "dunia" semakin mengecil, di mana batasan jarak dan waktu semakin tidak berarti (Nooryanto, Prihatin, & Dewi, 2023). Kemudahan ini tidak hanya meningkatkan produktivitas individu, tetapi juga membuka peluang baru bagi kolaborasi dan inovasi di berbagai sektor. Perkembangan teknologi informasi bukan hanya sekadar kemajuan teknis, tetapi juga sebuah revolusi dalam cara kita berinteraksi, bekerja, dan menjalani kehidupan sehari-hari. Transformasi ini mengubah paradigma sosial dan ekonomi secara mendalam yang menjadikan dunia semakin terhubung dan saling bergantung satu sama lain. Namun, tidak dapat dipungkiri bahwa tetap terdapat celah dalam transformasi teknologi saat ini, termasuk kejahatan berbasis digital.

Kejahatan siber atau yang lebih dikenal dengan istilah *cyber crime* adalah tindak kejahatan yang dilakukan secara *online* melalui jaringan internet. *Cyber scam* merupakan bentuk kejahatan digital yang dilakukan melalui internet dengan tujuan untuk menipu dan mendapatkan keuntungan dari korban. Istilah ini merujuk pada segala tindakan penipuan yang dirancang untuk mencuri uang, barang, atau data pribadi dari individu atau organisasi. Fenomena ini menjadi semakin kompleks seiring dengan perkembangan teknologi informasi yang pesat. Tujuan dari kejahatan siber sangat beragam. Beberapa pelaku mungkin melakukannya hanya untuk iseng atau untuk membuktikan kemampuan teknis mereka, sementara yang lain memiliki niat jahat yang lebih serius, seperti pencurian identitas, penipuan finansial, atau bahkan sabotase terhadap sistem informasi perusahaan (Malunsenge, Massie, & Rorie, 2022). Para pelaku kejahatan siber biasanya adalah individu yang memiliki keahlian tinggi dalam berbagai teknik peretasan dan pemrograman. Mereka sering kali memanfaatkan celah keamanan dalam sistem untuk mengakses data sensitif atau melakukan tindakan merugikan salah satunya *cyber scam*.

Dalam praktiknya, *cyber scam* sering kali muncul dalam berbagai bentuk, seperti penawaran investasi yang tidak nyata, phishing, atau penipuan e-commerce, di mana pelaku berpura-pura sebagai penjual untuk menerima pembayaran tanpa mengirimkan barang. Para pelaku *cyber scam*, yang dikenal sebagai scammer, menggunakan teknik yang canggih dan sering kali tampak meyakinkan, sehingga banyak orang yang menjadi korban. Modus operandi mereka termasuk menciptakan rasa urgensi dengan penawaran yang terlalu menggiurkan atau meminta informasi pribadi dengan dalih tertentu (Warsiti & Markoni, 2023).

Bentuk-bentuk kejahatan siber (*cybercrime*) di Indonesia dapat dikaitkan dengan ketentuan hukum pidana Indonesia, baik ketentuan KUHP maupun ketentuan pidana dalam peraturan perundang-undangan di luar KUHP yaitu UU No. 11 Tahun 2008 *Jo* UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Meskipun demikian, ada perbedaan konsepsi antara hukum pidana Indonesia dengan karakteristik kejahatan siber (*cybercrime*). Tindak pidana penipuan merupakan tindak pidana yang sangat dekat dengan orang-orang, selain dekat bahkan tidak sedikit orang yang menyadari bahwa dirinya telah ditipu (Rachmat, 2023).

Kejahatan ini diatur dalam Pasal 378 sampai dengan Pasal 394 Kitab Undang-Undang Hukum Pidana (KUHP) yang menyatakan bahwa penipuan yang dimaksud dalam pasal tersebut dikenakan sanksi pidana penjara selama empat tahun. Bentuk dari penipuan *online* tersebut dapat beragam dan dapat dilakukan dalam berbagai celah yang ada seiring dengan perkembangan teknologi yang semakin canggih seperti saat ini. Seperti kasus yang telah terjadi kepada Alma Nursalsabila yang menjadi korban dari tindak pidana *cyberscam* dan mengalami kerugian yang cukup besar, ia mengalami tindak pidana *cyberscam* tersebut dalam bentuk penipuan dalam platform whatsapp yang di mana pelaku ini berpura-pura akan membeli pulsa kepada korban menggunakan identitas palsu dan menyamar menjadi guru SMA nya dulu. Korban awalnya tidak menaruh kecurigaan sama sekali terhadap transaksi tersebut, dikarenakan korban mengira pelaku merupakan guru SMA korban. Transaksi tersebut terjadi berulang kali mencapai 6 (enam) kali transaksi dan korban mengalami kerugian sebesar 2 juta rupiah (Alma Nursalsabila, 2025).

Selain itu, bentuk dari *cyberscam* yang lain pun dialami oleh Diera A. yang menjadi korban dari *cyberscam* penipuan tiket konser *online* pada *platform* sosial media instagram. Pelaku pada awalnya menghubungi korban pada salah satu kolom komentar penjualan tiket *online* di instagram dengan harga yang jauh lebih murah dari harga *official* dari penyelenggaraan event konser tersebut. Korban merasa tertarik untuk membeli dan awalnya percaya pada pelaku dikarenakan pelaku memalsukan data pribadi di instagramnya sebagai bagian dari *event* konser tersebut (*volunteer*). Namun, setelah transaksi terjadi dan korban sudah mentransfer sejumlah uang yang diminta, respon dari pelaku lambat dan sempat menghilang beberapa waktu dan pada akhirnya pelaku memberikan tiket kepada korban, tapi tiket yang diberikan berbeda dan tidak sesuai dengan tiket *event* konser yang dijanjikan oleh pelaku. Hal tersebut tentunya merugikan korban dari tindak pidana *cyberscam*. Kejadian yang dialami oleh Alma Nursalsabila dan Diera A. ini menunjukkan betapa pentingnya regulasi yang mampu melindungi masyarakat dari kejahatan di dunia maya (Diera A., 2025).

Saat ini Indonesia telah memiliki Undang-undang yang khusus untuk mengatur mengenai *cyber crime* atau kejahatan mayatara, yaitu Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang selanjutnya disebut dengan UU ITE. UU ITE dirasa perlu untuk diberlakukan dan terus diperbaharui. Pasal 28 Ayat (1) UU ITE telah mengatur mengenai perbuatan yang dilarang dalam transaksi elektronik, yang berisi mengenai setiap orang dilarang untuk menyebarkan berita bohong dan menyesatkan secara sengaja dan tanpa hak yang dapat merugikan konsumen dalam transaksi elektronik, sedangkan mengenai sanksi pidana yang diberikan atas perbuatan pada Pasal 28 Ayat (1) UU ITE tersebut diatur dalam ketentuan pidana yang terdapat pada Pasal 45A Ayat (1) UU ITE (Ismail, 2018). Dalam hal ini Undang-Undang Informasi dan Transaksi Elektronik Tahun 2016 mengatur tentang delik-delik yang belum sepenuhnya direformasi dalam Undang-Undang Informasi dan Transaksi Elektronik, seperti belum memperbarui pasal-pasal tentang transaksi elektronik. (Annisa Hesti Kurniawati, Dara Pustika Sukma, & Yulio Iqbal Cahyo Arsetyo, 2023)

Di era globalisasi dimana canggihnya teknologi membuat mudahnya kejahatan yang bersifat modern ini terjadi dan berdampak lebih besar dari pada kejahatan konvensional, *cyber scam* ini dapat di bercirikan beberapa hal diantaranya penjahatnya bisa siapa saja orang umum yang berpendidikan atau juga orang awam yang berpendidikan) dan alat yang digunakan sederhana saja dan kejahatannya tidak perlu menggunakan suatu keahlian, kejahatan dapat dilakukan secara transnasional yaitu melintasi batas negara. (Dermawan, Amalia, Ramdhan, Tiara, & Alfina, 2024)

Maraknya kasus *cyber* ini banyak memakan korban, Perlindungan terhadap korban kejahatan merupakan elemen penting dalam sistem peradilan yang adil dan manusiawi. Selama ini, fokus penegakan hukum lebih diarahkan pada pelaku, sementara korban tindak pidana diabaikan. Pemulihan kerugian korban merupakan bagian dari perlindungan hukum terhadap korban sehingga dapat dikaji melalui kajian viktimologi. Jika sudah berkaitan dengan pemulihan kerugian korban hal itu menjadi penting sebab termasuk ke dalam suatu respon terhadap suatu viktimisasi sekunder. Hal ini bisa berupa sikap menyalahkan korban (*victim blaming*), pengulangan proses pelaporan yang menyakitkan atau ketidakpedulian terhadap kebutuhan psikologis dan emosional korban. (Mawby, R.I & Walkate, S. 1994)

Korban sudah menderita karena menjadi target kejahatan, ini disebut viktimisasi primer. Tetapi setelah itu, ia malah dipersulit, disalahkan atau diabaikan oleh orang-orang atau sistem yang seharusnya membantunya, itulah viktimisasi sekunder. Contoh bentuk viktimisasi

sekunder yaitu korban disalahkan oleh masyarakat atau aparat, dimana korban penipuan *online* sering dikatai "bodoh" atau "gampang ketipu". Pertanyaan yang menyudutkan saat pelaporan yaitu polisi atau pihak berwenang menganggap laporan korban "tidak penting" atau "sulit di buktikan". Minimnya perlindungan atau bantuan hukum, korban tidak mendapat informasi, pendampingan atau kejelasan tentang proses hukum. Paparan di media sosial atau media massa, identitas korban diungkap atau cerita mereka dipakai sebagai bahan sindiran atau olok-olok. Tidak adanya dukungan psikologis yaitu korban tidak diberi ruang untuk pulih, bahkan seringkali harus berjuang sendiri.

Sejalan dengan pernyataan tersebut, Alma Nursalsabila dan Diera A. pun merasakan hal yang sama, di mana mereka disalahkan oleh orang-orang terdekatnya dikarenakan mereka dianggap tidak teliti dan gampang untuk dibodoh-bodohi oleh seseorang. Hal tersebut tentunya menimbulkan rasa kepercayaan korban terhadap dirinya sendiri dan justru akan menyalahkan dirinya sendiri karena telah bertindak "bodoh". Selain itu, viktimisasi sekunder yang dialaminya pun membuat mereka enggan untuk melapor ke pihak yang berwenang dikarenakan khawatir akan mendapatkan respon yang sama. Padahal, korban seharusnya mendapatkan perlindungan dan perhatian dari orang sekitar, aparat penegak hukum, dll.

Viktimisasi sekunder merupakan hal yang penting dibahas karena hal ini bisa memperparah trauma korban, membuat korban enggan melapor, merusak kepercayaan terhadap sistem hukum dan sosial serta menghambat proses pemulihan secara psikologis dan sosial. Viktimisasi sekunder dapat memperparah luka psikologis korban *cyber scam*, yaitu menghambat proses pemulihan dan menurunkan kepercayaan terhadap sistem hukum dan sosial. Oleh karena itu, penting bagi aparat penegak hukum, media dan masyarakat untuk lebih empatik, suportif dan tidak menyalahkan korban, agar tidak menambah beban korban yang sudah menjadi pihak yang dirugikan.

Korban kejahatan ini tidak hanya mengalami kerugian ekonomi sebagai bentuk viktimisasi primer, tetapi juga menghadapi penderitaan tambahan dari sistem sosial dan hukum yang tidak responsif atau bahkan menyudutkan korban. Beberapa dampak viktimisasi *cyber scam* yang memanifestasikan diri dalam beberapa bentuk yaitu, Pertama, Respon aparat yang tidak memadai, banyak korban yang merasa diabaikan atau tidak dipercaya saat melaporkan kejahatan *cyber*. Karena pelaku bisa saja berada di luar negeri atau luar pulau, menggunakan identitas palsu, korban kerap mendapat jawaban bahwa kasusnya "sulit ditindak lanjuti"(Sudiyawati & Mertha, 2022)

Kedua, korban seringkali disalahkan oleh lingkungan sosial dengan pernyataan seperti "kok bisa ketipu?", "harusnya hati-hati dong". Hal ini menambah rasa malu, bersalah dan

membuat korban menarik diri dari lingkungan sosial. (Maulida & Romdoni, 2024) Ketiga, Minimnya dukungan psikologis dan hukum, memang tidak semua korban mendapat pendampingan hukum atau psikososial. Padahal, dampak psikologis dari penipuan daring bisa sangat dalam. Beberapa dampak yang dialami korban *cyber scam* dapat mempengaruhi korban dalam segi apapun termasuk kepercayaan nya terhadap sistem hukum, takut akan reviktimisasi melalui proses hukum atau takut akan melalui proses hukum yang panjang dan melelahkan, dimana mereka akan mengulang kembali pengalaman traumatis mereka tanpa adanya jaminan keadilan atau kompensasi.

Selain itu, tingkat kepercayaan korban terhadap transaksi jual beli *online* menjadi menurun dan bahkan mengalami trauma untuk tidak lagi melakukan transaksi jual beli *online* karena kasus penipuan *online* yang dialaminya. Hal tersebut pun dialami oleh Alma Nursalsabila dan Diera A. setelah menjadi korban dari tindak pidana *cyberscam*. Namun menurut Diera A., kejadian tersebut pun memiliki dampak positifnya yaitu korban menjadi lebih waspada dan penuh kehati-hatian dalam setiap transaksi yang ia lakukan, baik itu transaksi *online* maupun transaksi secara langsung.

Timbul pertanyaan, bisa saja kasus *cyber scam* memang terjadi karena kelalaian atau kurangnya kewaspadaan korban, namun meskipun korban lalai, beban moral dan hukum seharusnya tidak serta merta dibalikkan seluruhnya kepada mereka, sebab dalam perspektif hukum, kelalaian bukan alasan pembenar sebuah kejahatan. Prinsip dasar nya adalah "Tidak ada kejahatan tanpa kesalahan, dan tidak ada hukuman tanpa perbuatan pidana" sekalipun korban lalai (misalnya memberikan OTP, mengklik tautan berbahaya atau mentransfer uang) pelaku tetap bertanggung jawab secara hukum karena telah melakukan penipuan atau manipulasi. Kelalaian korban bisa saja memperberat resiko, tapi tidak menghapus tanggung jawab pidana pelaku. "Kecerobohan korban tidak dapat menghilangkan unsur perbuatan melawan hukum yang dilakukan pelaku penipuan siber" (Sulastri & Wahyuni, 2023)

Dalam perspektif viktimologi modern, korban tetaplah korban, status korban tidak boleh dibatalkan hanya karena mereka lalai. Viktimology tidak hanya menelaah bagaimana korban mengalami kerugian, tetapi juga bagaimana sistem memperlakukan mereka setelah itu. Bahkan jika korban melakukan kesalahan, tugas sistem hukum dan sosial adalah memberikan perlindungan dan pemulihan, bukan menyalahkan.

4. KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa perlindungan hukum terhadap korban tindak pidana *cyber scam* di Indonesia belum terlaksana secara maksimal. Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur sanksi terhadap pelaku, namun belum secara menyeluruh memberikan perlindungan yang memadai bagi korban, terutama terkait pemulihan hak-hak korban seperti ganti rugi materiil maupun immateriil. Ketentuan yang ada lebih berfokus pada penindakan pelaku, sementara perlindungan terhadap korban masih bersifat umum dan belum implementatif. Banyak korban *cyber scam* tidak mengetahui cara melaporkan kejahatan yang mereka alami, sehingga pelaku sering kali lolos dari hukuman. Hal ini menunjukkan perlunya peningkatan literasi digital masyarakat serta penyediaan mekanisme pelaporan yang lebih mudah diakses.

Di sisi lain, korban kejahatan *cyber scam* juga kerap mengalami viktimisasi sekunder, yaitu penderitaan lanjutan yang timbul bukan dari pelaku kejahatan, melainkan dari respon negatif aparat penegak hukum, media, dan masyarakat. Hal ini terjadi dalam bentuk pengabaian laporan, sikap menyalahkan korban, minimnya pendampingan hukum dan psikologis, serta kurangnya perhatian terhadap pemulihan korban secara utuh. Dampak tersebut tidak hanya memperparah trauma korban, tetapi juga melemahkan kepercayaan terhadap sistem hukum.

Sebagai langkah strategis, pemerintah perlu melakukan revisi dan penyempurnaan terhadap UU ITE agar lebih menitikberatkan pada perlindungan korban, termasuk penyediaan mekanisme ganti rugi yang jelas dan tegas. Aparat penegak hukum, media, dan masyarakat juga perlu diberikan pelatihan dan edukasi untuk membangun pemahaman yang lebih empatik terhadap korban kejahatan digital guna menghindari terjadinya viktimisasi sekunder. Pendekatan yang berbasis pada korban harus menjadi bagian integral dari sistem peradilan pidana. Selain itu, peningkatan literasi digital secara menyeluruh di kalangan masyarakat menjadi sangat penting agar individu lebih waspada terhadap modus kejahatan siber serta memahami langkah-langkah hukum yang dapat ditempuh ketika menjadi korban. Hal ini penting demi mewujudkan sistem hukum yang adil, manusiawi, dan berpihak pada korban di era digital.

REFERENSI

- Abdulkadir Muhammad. (2004). *Hukum dan Penelitian Hukum*. Bandung: Citra Aditya Bakti.
- Alma Nursalsabila. (2025). *Hasil Wawancara Pribadi*.
- Annisa Hesti Kurniawati, Dara Pustika Sukma, & Yulio Iqbal Cahyo Arsetyo. (2023).

- Perlindungan Hukum Atas Korban Kejahatan Penipuan Berbasis Online Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Secara Viktimologi. *Jurnal Cakrawala Ilmiah*, 2(9), 3465–3474. <https://doi.org/10.53625/jcijurnalcakrawailmiah.v2i9.5661>
- Arikunto, S. (2012). *Prosedur Penelitian Suatu Pendekatan Praktek*. Jakarta: Rineka Cipta.
- Astri, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Jurnal Hukum Kris*, 15.
- Berita Keamanan Siber. (2025). Ancaman Siber 2025: Indonesia Harus Waspada AI Agentik. Retrieved April 14, 2025, from <https://csirt.bpip.go.id/posts/ancaman-siber-2025-indonesia-harus-waspada-ai-agentik>
- Dermawan, A. (2019). Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi. *Journal of Science and Social Research*, 4307(2), 39–46.
- Dermawan, A., Amalia, A., Ramdhan, W., Tiara, A., & Alfina, C. (2024). Viktimologi Hukum Bagi Korban Tindak Pidana Kejahatan Digitalisasi. *Jurnal Bangun Abdimas*, 3(1), 245–250. <https://doi.org/10.56854/ba.v3i1.336>
- Didik M, & Arief, M. (2005). *Cyber Law, Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.
- Diera A. (2025). *Hasil Wawancara Pribadi*.
- ERLYNA, & Isnawati, M. (2024). Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Transaksi Jual Beli Pada Marketplace. *Perspektif Hukum*, 26–44. <https://doi.org/10.30649/ph.v24i1.263>
- Indrawan, M., & Permatasari, P. (2022). Perlindungan Hukum Korban Penipuan Transaksi Jual Beli Online Melalui Ganti Rugi. *Jurnal Kewarganegaraan*, 6(3), 6487–6494. Retrieved from <http://journal.upy.ac.id/index.php/pkn/article/view/4157>
- Ismail, M. (2018). Kebijakan Hukum Pidana Cyberpornography. *Jurnal Hukum Ekonomi Syariah*, 1(2), 129.
- Karolus Charlaes, B., Aziz, F. R., Rahmad, R. A., & Sunarto4, H. B. (2025). Tindak Pidana Cybercrime : Tantangan Hukum Pidana Menanggulangi Kejahatan di Dunia Maya (Desember 2024). *Jurnal Kolaboratif Sains*, 8(1), 506–511. <https://doi.org/10.56338/jks.v8i1.6740>
- Madinah Mokobombang, Zulfikri Darwis, & Sabil Mokodenseho. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum Dan HAM Wara Sains*, 2(6), 517–525. <https://doi.org/10.58812/jhhws.v2i6.447>
- Malunsenge, L. M., Massie, C. D., & Rorie, R. E. (2022). Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia. *Lex Crimen*, 11(3), 1–10.

- Maulida, G., & Romdoni, M. (2024). Perlindungan Hukum Terhadap Korban Pelecehan Seksual Yang Mengalami Viktimisasi Sekunder di Media Sosial. *Southeast Asian Journal of Victimology*, 2(1), 59. <https://doi.org/10.51825/sajv.v2i1.25445>
- Maya Sri Novita. (2025). Pentingnya Perlindungan Hukum Bagi Korban Tindak Pidana Penipuan dalam Proses Transaksi Jual Beli Secara Online (E- Commerce). *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, 2(2). <https://doi.org/doi.org/10.62383/desentralisasi.v2i2.690>
- Narbuko, C., & Achmadi, A. (2001). *Metodologi Penelitian*. Jakarta: Bumi Aksara.
- Nooryanto, F. H., Prihatin, L., & Dewi, C. C. (2023). Kajian Hukuman Bagi Pelaku dan Perlindungan Hukum Bagi Korban dalam Tindak Pidana Bullying dan Cyber Bullying. *JHIP - Jurnal Ilmiah Ilmu Pendidikan*, 6(1), 169–177. <https://doi.org/10.54371/jhip.v6i1.1363>
- P.A.F., Lamintang. (2011). *Dasar-Dasar Hukum Pidana Indonesia* (Cetakan Ke). Bandung: P.T.Citra Aditya Bakti.
- Rachmat, L. A. A. (2022). Perlindungan Hukum terhadap Korban Tindak Pidana Penipuan melalui Media Sosial. *Indonesia Berdaya*, 3(4), 771–778. <https://doi.org/10.47679/ib.2022326>
- Rachmat, L. A. A. (2023). Viktimisasi dan Perlindungan Hukum terhadap Korban Tindak Pidana Penipuan Melalui Media Sosial. *Indonesia Berdaya*, 4(2), 629–644. <https://doi.org/10.47679/ib.2023468>
- Saputra, F., Soesanto, E., & Cahyaningtyas, K. I. (2024). Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo. *IJM: Indonesian Journal of Multidisciplinary*, 2, 146–154.
- Sedau, K. S., Masu, R. R., & Tungga, I. A. (2023). Penggunaan Dokumen Elektronik Sebagai Alat Bukti Oleh Hakim Dalam Pertimbangan Putusan Perkara Pornografi (Studi Putusan Nomor 16/PID SUS/2021/PN Kupang dan Putusan Nomor 162/PID.SUS/2020/PN Kupang). *Jurnal Indonesia Sosial Teknologi*, 4(6), 726–740. <https://doi.org/https://doi.org/10.59141/jist.v4i6.631>
- Simon Kemp. (2025). Digital 2025: Indonesia. Retrieved April 14, 2025, from <https://datareportal.com/reports/digital-2025-indonesia>
- Sudiyawati, N. P. L., & Mertha, I. K. (2022). Kejahatan Siber (Cybercrime) Dalam Konteks Kekerasan Seksual Berbasis Gender Online Di Indonesia. *Kertha Semaya: Journal Ilmu Hukum*, 10(4), 850. <https://doi.org/10.24843/ks.2022.v10.i04.p11>
- Tanthawi, Dahlan Ali, S. (2017). Perlindungan Korban Tindak Pidana Cyber Crime Dalam Sistem Hukum Pidana Indonesia. *Ilmu Hukum*, 2(1), 32–40.
- Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban KejahatanCyber Crime Di Indonesia. *Jurnal Ilmu Hukum Jambi*, 4(1), 98–113.
- Waluyo, B. (2002). *Penelitian Hukum dalam Praktek* (Cet. 3). Jakarta: Sinar Grafika.

- Warsiti, T., & Markoni, M. (2023). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Berbentuk Phising Dalam Transaksi Perdagangan Internasional. *Jurnal Multidisiplin Indonesia*, 2(6), 1109–1125. <https://doi.org/10.58344/jmi.v2i6.262>
- Yunus Darmono. (2023). Perlindungan Hukum Terhadap Korban Tindak Pidana Cyber Crime di Indonesia. *Journal UNIBA*, 35(1), 43. <https://doi.org/10.36722/jmih.v2i1.740>