

KORBAN KEJAHATAN SIBER (CYBERCRIME): PERLINDUNGAN DAN KENDALA DALAM PENEGAKAN HUKUM

Andry Rachman Martin¹, Stefani Maria Putri², Junifer Dame Panjaitan³

andryrachman983@gmail.com¹, mariaputristefani@gmail.com², junifer_panjaitan@mputantular.ac.id³

Universitas Mpu Tantular

Abstract: *The rapid advancement of science and technology, particularly in information and communication technology, has brought significant changes to human civilization, but it has also given rise to negative impacts in the form of cybercrime. This type of crime exploits technology and internet networks as tools, taking various forms such as data theft, online fraud, and system hacking. In Indonesia, cybercrime is regulated under Law Number 1 of 2024, which amends Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law). This study aims to analyze the legal protection for cybercrime victims and to identify the obstacles and solutions in its law enforcement. The research employs a normative juridical method with a conceptual, statutory, and case approach. Data sources are obtained from primary and secondary legal materials, which are then analyzed qualitatively. The findings reveal that legal protection for cybercrime victims in Indonesia is regulated under the ITE Law, the Witness and Victim Protection Law, and the Personal Data Protection Law. As a state governed by law, Indonesia is obligated to protect its citizens from harmful acts, including cybercrime. Cybercrime law enforcement applies the principle of *lex specialis derogat legi generali*, where the ITE Law takes precedence over the Criminal Code (KUHP). However, several obstacles hinder effective cybercrime law enforcement, including: (1) legal provisions that lag behind technological advancements, creating legal loopholes; (2) limited human resources among law enforcement officers in digital forensics; (3) lack of international cooperation in handling cross-border crimes; (4) the sophistication of perpetrators' methods in concealing digital traces; (5) low digital literacy among the public; and (6) limited technological infrastructure in rural areas. Strategic solutions include: (1) legal updates and reforms that are adaptive to technology; (2) enhanced training and certification for law enforcement personnel; (3) strengthening bilateral and multilateral cooperation; (4) development of equitable digital forensic infrastructure; and (5) increasing public education and digital literacy. Through a comprehensive and collaborative approach, cybercrime law enforcement is expected to be more effective in providing legal protection and justice for victims.*

Keywords: Legal Protection, Victims, Cybercrime, Law Enforcement, ITE Law.

Abstrak: Perkembangan pesat ilmu pengetahuan dan teknologi, khususnya teknologi informasi dan komunikasi, telah membawa perubahan signifikan dalam peradaban manusia, namun juga memunculkan dampak negatif berupa kejahatan siber (cybercrime). Kejahatan ini memanfaatkan teknologi dan jaringan internet sebagai sarana, dengan berbagai bentuk seperti pencurian data, penipuan online, dan peretasan sistem. Di Indonesia, cybercrime diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap korban cybercrime dan mengidentifikasi faktor penghambat serta solusi dalam penegakan hukumnya. Penelitian ini menggunakan metode penelitian yuridis normatif dengan pendekatan konseptual, perundang-undangan, dan kasus. Sumber data diperoleh dari bahan hukum primer dan sekunder, yang kemudian dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap korban cybercrime di Indonesia telah diatur dalam UU ITE, Undang-Undang Perlindungan Saksi dan Korban, serta Undang-Undang Perlindungan Data Pribadi. Hukum di Indonesia, sebagai negara hukum, wajib melindungi warganya dari perbuatan yang merugikan, termasuk cybercrime. Penegakan hukum cybercrime menerapkan asas *lex specialis derogat legi generali*, di mana UU ITE diutamakan dibandingkan KUHP. Namun, terdapat beberapa faktor penghambat dalam penegakan hukum cybercrime, antara lain: (1) aturan hukum yang tertinggal dari perkembangan teknologi, sehingga menciptakan kekosongan hukum; (2) keterbatasan sumber daya manusia aparat penegak hukum dalam bidang forensik digital; (3) kurangnya kerja sama internasional dalam penanganan kejahatan lintas batas; (4) kecanggihan modus operandi pelaku yang menyembunyikan jejak digital; (5) rendahnya literasi digital masyarakat; dan (6) keterbatasan infrastruktur teknologi di daerah. Sebagai solusi strategis, diperlukan: (1) pembaruan dan

reformasi hukum yang adaptif terhadap teknologi; (2) peningkatan pelatihan dan sertifikasi bagi aparat penegak hukum; (3) penguatan kerja sama bilateral dan multilateral; (4) pengembangan infrastruktur forensik digital yang merata; dan (5) peningkatan edukasi dan literasi digital bagi masyarakat. Dengan pendekatan yang komprehensif dan kolaboratif, diharapkan penegakan hukum terhadap cybercrime dapat lebih efektif dalam memberikan perlindungan hukum dan keadilan bagi korban.

Kata Kunci: Perlindungan Hukum, Korban, Kejahatan Siber (Cybercrime), Penegakan Hukum, UU ITE.

PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi yang dihasilkan peradaban manusia senantiasa selalu berubah dan meningkat sehingga berdampak pada perilaku masyarakat modern yang tidak terlepas dari teknologi yang dapat meningkatkan kesejahteraan masyarakat dengan tetap memperhatikan kepastian, keadilan dan kemanfaatan hukum.

Teknologi dan informasi menjadi kebutuhan dan tidak dapat dipisahkan dari kehidupan manusia. mengingat teknologi mampu mempermudah manusia dalam menjalani aktivitas sehari-hari, Manusia sebelum mengenal adanya teknologi didominasi oleh aktivitas yang bersifat fisik, face to face. Dengan munculnya internet membuat ruang, jarak, dan waktu yang sebelumnya membatasi manusia hilang. Internet memberikan kemudahan kepada setiap individu yang menggunakannya.

Kemajuan teknologi mewujudkan suatu perubahan yang membawa kemajuan manusia semakin modern. Kemajuan teknologi juga telah mempengaruhi kejahatan dunia maya dalam banyak hal. Perkembangan teknologi informasi dan komunikasi juga menyebabkan hubungan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung begitu cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif melakukan tindakan melawan hukum (Legalita, 2023).

Dalam perspektif kriminologi, teknologi bisa dikatakan sebagai faktor kriminogen, yaitu faktor yang menyebabkan timbulnya keinginan orang untuk berbuat jahat atau memudahkan terjadinya kejahatan. Penyalahgunaan atau dampak negatif dari kemajuan teknologi informasi melalui sistem komputerisasi dan jaringan internet dikenal dengan istilah cyber crime, Berkaitan dengan hal ini, Barda Nawawi Arief menggunakan istilah “tindak pidana mayantara”, yang identik dengan tindak pidana di ruang siber (cyberspace) atau yang biasa dikenal dengan istilah “cyber crime”. (Barda Nawawi Arief, 2003).

Cyber crime adalah jenis kejahatan yang muncul karena adanya kemajuan teknologi. Secara umum, pengertian cyber crime biasa diartikan sebagai tindak kejahatan di ranah dunia maya yang memanfaatkan teknologi komputer dan jaringan internet sebagai sasaran (Nugroho, Andy 2021).

Cyber crime merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas. bagi seluruh bidang kehidupan modern saat ini. Semakin berkembangnya cyber crime terlihat pula dari munculnya berbagai istilah seperti economic cyber crime, EFT (Electronic Funds Transfer) Crime, Cybank Crime, Internet Banking Crime, On-line Business Crime, Cyber/Electronic Money Laundering, Hitech WWC (white collar crime), Internet fraud, cyber terrorism, cyber stalking, cyber sex, cyber (child) pornography, cyber defamation, cyber-criminals dan lain-lain”.(Barda Nawawi Arief, 2006).

Munculnya beberapa kasus cyber crime di Indonesia, merupakan fenomena, Pelaku memanfaatkan kemajuan teknologi dan jaringan internet untuk melakukan tindak kejahatan seperti meretas, hacking terhadap berbagai situs, penyadapan transmisi data orang lain, (misalnya email), manipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programer komputer. mencuri, menipu, menyebarkan virus, dan aksi kriminal melalui jaringan internet lainnya. Bahkan korban seringkali terlambat mengetahui jika dirinya menjadi sasaran tindak kejahatan.

Berbagai tindakan di atas dapat dikenakan tindak pidana, baik delik formil maupun materiil. Delik formil karena menyangkut perbuatan seseorang mengakses data komputer orang lain tanpa izin, sedangkan delik materiil adalah perbuatan itu telah menimbulkan akibat kerugian bagi orang lain.(Besar, 2016)

Tindak kriminal ini tidak hanya terjadi dalam tataran lokal saja. Pelaku dan korban bisa saja

berada di lokasi yang berbeda (iblam, 2024) Tidak menutup kemungkinan pelaku dan korban berada di kota atau negara yang berbeda. Inilah yang membuat kejahatan siber tidak mudah untuk ditelusuri dan harus ada langkah antisipasi supaya tidak menyebabkan banyak korban.

Bentuk Kejahatan Siber (Cybercrime) meliputi pencurian data, penipuan online, peretasan sistem, ransomware, phishing, hingga penyalahgunaan identitas digital.

Di Indonesia, kejahatan cyber diatur dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah menjadi UU Nomor 19 Tahun 2016 sebagaimana telah diubah untuk kedua kalinya menjadi UU Nomor 1 Tahun 2024.

Kategori kejahatan cyber yang dilarang dalam UU ITE;

- a. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun
- b. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi dan/atau dokumen elektronik
- c. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. (siplawfirm, kejahatan-cyber, 2023).

METODE PENELITIAN

1. Jenis Penelitian: Yuridis Normatif
2. Metode Pendekatan:
 - a. Pendekatan Konseptual (Conseptual Approach)
 - b. Pendekatan Perundang-undangan (Statute Approach)
 - c. Pendekatan Kasus (Case Approach)
3. Sumber Data/Bahan Hukum:
 - a. Bahan hukum Primer
 - b. Bahan Hukum Sekunder
4. Metode Analisis Data: Metode analisis kualitatif.

HASIL DAN PEMBAHASAN

1. Subbab Perlindungan Hukum Terhadap Korban Kejahatan Siber (Cybercrime).

Menurut Hans Kelsen, hukum adalah sebuah sistem norma. Norma adalah pernyataan yang menekankan aspek “seharusnya” atau *das solen*, dengan menyertakan beberapa peraturan tentang apa yang harus dilakukan. Norma-norma adalah produk dari aksi manusia yang membedakan antara apa yang ada (*das sein*) dan apa yang “seharusnya”, juga keyakinan bahwa tidak memungkinkan pemunculan kesimpulan dari kejadian faktual bagi *das solen*. Sehingga, Kelsen percaya bahwa hukum, yang merupakan pernyataan-pernyataan “seharusnya” tidak bisa direduksi ke dalam aksi-aksi alamiah. (Jimly Asshidiqie, 2006)

Indonesia adalah negara hukum seperti yang tertuang dalam konstitusi, sebagai sebuah negara hukum tentunya negara wajib melindungi setiap warga negaranya dari setiap perbuatan yang dapat merugikan apalagi perbuatan tersebut dapat merusak tatanan kehidupan berbangsa dan bernegara. Seperti halnya kejahatan yang terjadi di dunia maya atau biasa disebut dengan *cybercrime*.

Kejahatan yang tidak mengenal ruang dan waktu ini mengalami perkembangan yang pesat akhir-akhir ini, kecanggihan teknologi yang disalah gunakan oleh oknum yang tidak bertanggung jawab demi keuntungan pribadi yang menyebabkan negara-negara berkembang kesulitan untuk menindak pelaku kejahatan komputer khususnya pihak kepolisian, disamping dibutuhkan suatu perangkat aturan yang mengatur tentang penyalahgunaan informasi ini juga dibutuhkan sumber

daya manusia dan sarana dan prasarana yang mendukung.

Perlindungan hukum bagi mereka yang menggunakan teknologi tentunya sangat diperlukan, hal ini dikarenakan apabila suatu peristiwa pidana terjadi, aturan hukum sering kali memfokuskan diri untuk menghukum pelaku kejahatan sehingga sering kali korban dari kejahatan tersebut terabaikan. Padahal korban juga patut untuk diperhatikan karena pada dasarnya korban merupakan pihak yang cukup dirugikan dalam suatu tindak pidana. Dampak kejahatan menimbulkan korban dan kerugian. Kerugian yang timbul itu bisa diderita oleh korban sendiri, maupun oleh pihak lain secara tidak langsung. (J.E. Sahetapy, 2023).

Sebagaimana dalam ketentuan Pasal 1 ayat (3) UUD 1945 ditegaskan bahwa Indonesia adalah negara hukum, jadi segala sesuatu harus sesuai dengan hukum dan mempunyai aturan yang jelas, begitu juga dengan masalah Kejahatan Siber (Cybercrime) dan Perlindungan serta keamanan dalam masyarakat. (UUD 1946, Pasal 1 Ayat (3)).

Satjipto Rahardjo dalam bukunya Ilmu Hukum (2000) mengatakan, perlindungan hukum pada hakikatnya memberikan pengayoman terhadap hak asasi manusia yang dirugikan orang lain dan diberikan kepada masyarakat agar dapat menikmati hak-hak yang diberikan oleh hukum. Pasal 28D ayat (1) UUD 1945 menyatakan setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum. Selanjutnya Pasal 28G ayat (1) UUD 1945 menambahkan setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari segala ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. (M. Yasin, 2023).

Dalam penanganan pidana kejahatan Siber (Cybercrime) karena bersifat khusus dan penanganannya juga khusus maka harus mengedepankan azas hukum *Lex specialis derogat legi generali* adalah asas penafsiran hukum yang menyatakan bahwa hukum yang bersifat khusus (*lex specialis*) mengesampingkan hukum yang bersifat umum (*lex generalis*). Menurut Bagir Manan dalam bukunya yang berjudul Hukum Positif Indonesia (hal, 56). (Ali Ridho, 2018). Asas ini dimaksudkan untuk memberikan kepastian hukum tentang kedudukan hukum yang bersifat khusus terhadap hukum yang bersifat umum sehingga aparat hukum khusus diutamakan penerapannya atau penggunaannya dibandingkan dengan hukum umum, antara lain misalnya Kitab Undang-Undang Hukum Pidana (KUHP) yang berkedudukan sebagai hukum umum terhadap Undang-Undang Tindak Pidana Siber (Cybercrime). (Suparman, Marzuki. 2023).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Merupakan dasar hukum utama dalam perlindungan terhadap korban kejahatan siber (cybercrime) di Indonesia. UU ITE memberikan landasan hukum untuk menangani berbagai jenis kejahatan siber, mulai dari akses ilegal, penyadapan, manipulasi data, hingga pencemaran nama baik di dunia maya. Selain UU ITE, perlindungan hukum terhadap korban cybercrime juga dapat diperoleh dari Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban yaitu Aturan terkait perlindungan terhadap saksi dan korban kejahatan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yaitu Aturan yang mengatur perlindungan data pribadi dalam lingkungan digital.

2. Subbab Faktor Penghambat dan Kendala dalam Penegakan Hukum terhadap Kejahatan Siber (Cybercrime) serta solusinya

a. Faktor Penghambat Penegakan Hukum terhadap Cybercrime

Hukum formal sering kali tertinggal dari realitas digital yang berkembang sangat cepat (Barda Nawawi Arief, 2017). Artinya, banyak regulasi hukum yang masih bersifat umum dan tidak merinci bentuk-bentuk kejahatan siber yang kompleks. Hal ini membuat aparat penegak

hukum kesulitan dalam menjerat pelaku karena tidak adanya dasar hukum yang eksplisit.

Undang-Undang ITE belum mampu mengakomodasi seluruh varian baru dari kejahatan siber seperti penyalahgunaan deepfake, cryptojacking, atau manipulasi berbasis kecerdasan buatan (Fitriani, 2022). Ketika hukum tidak mengenali atau tidak mengatur secara jelas suatu tindakan sebagai kejahatan, maka akan terjadi kekosongan hukum yang berujung pada impunitas bagi pelaku. Akibatnya, korban tidak mendapatkan keadilan yang layak.

Banyak aparat penegak hukum belum dibekali kemampuan teknis dalam bidang forensik digital atau pemrosesan bukti elektronik (Puspitasari & Siregar, 2021). Ini menyebabkan kesalahan dalam pengumpulan bukti digital yang seharusnya sangat presisi. Bukti digital sangat mudah rusak atau hilang jika tidak ditangani sesuai prosedur, dan dalam beberapa kasus, bukti yang tidak sah dapat menyebabkan perkara digugurkan di pengadilan.

Hal ini membuat proses penyelidikan berjalan lambat, tidak akurat, bahkan gagal di tingkat pembuktian. Sehingga, banyak kasus cybercrime yang tidak dapat dilanjutkan ke tahap penuntutan atau berakhir dengan vonis bebas karena lemahnya alat bukti.

Kejahatan siber sering kali dilakukan lintas batas negara, sementara Indonesia belum menjadi pihak dalam konvensi internasional seperti Budapest Convention yang mengatur kerja sama penegakan hukum digital secara global (Fitriani, 2022). Tanpa keterlibatan dalam kerangka internasional tersebut, Indonesia kesulitan untuk melakukan pertukaran informasi intelijen siber atau meminta bantuan hukum dari negara tempat pelaku berada.

Hal ini menghambat upaya ekstradisi dan pertukaran informasi dengan negara lain. Sehingga, pelaku kejahatan siber dari luar negeri seringkali tidak dapat dijangkau dan tetap bebas beroperasi, yang merugikan sistem hukum nasional dan keamanan publik.

Pelaku cybercrime memanfaatkan enkripsi, VPN, dan dark web untuk menyembunyikan jejak digital mereka (Darmawan & Wicaksana, 2020). Teknologi ini memungkinkan pelaku menyamarkan lokasi dan identitas mereka, sehingga penegak hukum harus memiliki keterampilan dan perangkat khusus untuk menelusuri jejak digital yang sangat minim dan tersembunyi.

Dalam banyak kasus, hal ini menyulitkan aparat untuk menemukan identitas asli pelaku atau bahkan membuktikan keberadaan mereka secara hukum. Akibatnya, proses hukum menjadi sangat rumit dan berpotensi gagal membuktikan keterlibatan pelaku secara yuridis formal.

Masyarakat yang tidak memiliki literasi digital yang baik lebih mudah menjadi korban kejahatan siber dan jarang melaporkannya karena tidak mengetahui prosedur hukum yang berlaku (Mahendra, 2020). Sebagian besar masyarakat Indonesia belum terbiasa memverifikasi informasi atau menjaga kerahasiaan data pribadi, sehingga mudah tertipu oleh modus-modus penipuan digital.

Hal ini menyebabkan banyak kasus tidak terdeteksi oleh aparat penegak hukum. Rendahnya pelaporan juga membuat data statistik kejahatan siber menjadi bias, yang akhirnya menghambat penyusunan kebijakan berbasis bukti.

Penegakan hukum terhadap cybercrime memerlukan infrastruktur teknologi tinggi, termasuk laboratorium forensik digital, perangkat analisis jaringan, dan sistem deteksi dini serangan siber (UNODC, 2019). Namun, di Indonesia, pembangunan infrastruktur semacam itu masih terkonsentrasi di kota-kota besar dan belum merata ke daerah.

Alokasi anggaran di sektor ini masih rendah, terutama di tingkat daerah (Kusuma, 2023). Padahal, kejahatan siber dapat terjadi di mana saja, termasuk di wilayah dengan penetrasi internet tinggi seperti desa-desa wisata atau daerah industri.

b. Solusi Strategis

Pembaruan hukum harus bersifat adaptif terhadap teknologi. Perlu adanya pengembangan

perundang-undangan khusus yang tidak hanya mengatur transaksi elektronik, tetapi juga perlindungan data pribadi, keamanan digital, dan tanggung jawab platform digital (Andriansyah, 2021). Reformasi hukum juga perlu mempercepat sinkronisasi antara berbagai regulasi sektoral agar tidak tumpang tindih dan lebih efektif menjerat pelaku.

Diperlukan pelatihan teknis dan sertifikasi rutin bagi penyidik, jaksa, dan hakim yang menangani kasus cybercrime (Puspitasari & Siregar, 2021). Sumber daya manusia yang profesional akan mampu mengidentifikasi pola-pola baru kejahatan, menyusun strategi investigasi yang tepat, dan menghadirkan bukti yang kuat di persidangan.

Pemerintah Indonesia perlu aktif membangun kesepakatan bilateral dan multilateral untuk memperlancar ekstradisi, pertukaran data forensik digital, serta bantuan hukum lintas batas (Fitriani, 2022). Hal ini penting agar pelaku tidak bisa berlindung di negara-negara lain dan sistem hukum nasional tetap memiliki daya jangkau.

Laboratorium digital forensik dan pusat tanggap insiden (CSIRT) harus dikembangkan hingga tingkat provinsi dan kabupaten/kota untuk mempercepat penanganan kejahatan siber secara lokal (UNODC, 2019). Hal ini akan mempercepat investigasi dan memperkuat posisi hukum negara dalam menindak pelaku dengan bukti yang valid.

Pemerintah, akademisi, dan sektor swasta harus bekerja sama dalam meningkatkan kesadaran masyarakat melalui program literasi digital di sekolah, kampus, dan komunitas (Mahendra, 2020). Masyarakat yang cerdas digital akan lebih berhati-hati dalam beraktivitas di internet dan memiliki pengetahuan dasar tentang cara melindungi data serta melaporkan insiden yang mereka alami. Oleh karena itu, dibutuhkan pendekatan menyeluruh dan kolaboratif yang melibatkan reformasi hukum, peningkatan kapasitas, kerja sama internasional, serta pemberdayaan masyarakat. Tanpa hal ini, sistem hukum akan selalu tertinggal dari kecepatan inovasi para pelaku kejahatan siber yang terus berkembang.

KESIMPULAN

Undang Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan landasan hukum yang penting dalam melindungi korban kejahatan siber di Indonesia. Undang-Undang ini memberikan dasar hukum untuk menangani berbagai jenis kejahatan siber dan memberikan perlindungan hukum bagi korban. Meskipun ada perdebatan terkait implementasinya, UU ITE tetap menjadi alat penting dalam upaya penegakan hukum di dunia maya.

Saran

Saran untuk meningkatkan perlindungan hukum terhadap korban cyber crime dan dalam penegakan hukumnya, beberapa langkah strategis perlu diambil. yaitu:

- a. Dengan Peningkatan pelatihan dan pengembangan SDM di bidang forensik digital sangat diperlukan untuk memperkuat kemampuan penyidik dalam menangani kejahatan siber.
- b. Pengembangan perangkat lunak dan infrastruktur yang lebih canggih dan modern, serta pemanfaatan teknologi AI untuk membantu proses investigasi.
- c. Revisi UU ITE untuk memperjelas pasal-pasal yang ambigu, memperluas cakupan, dan menyelaraskan dengan perkembangan teknologi, serta memastikan bahwa peraturan perundang-undangan tetap relevan dan efektif dalam menangani kejahatan siber.
- d. Peningkatan kerjasama antar negara, khususnya dalam pertukaran informasi, penegakan hukum, dan ekstradisi pelaku kejahatan siber.
- e. Edukasi dan literasi digital yang lebih luas kepada masyarakat, agar mereka lebih memahami bahaya kejahatan siber dan cara mencegahnya.

DAFTAR PUSTAKA

Andriansyah, R. *Hukum Siber dan Dinamika Penegakannya di Indonesia*. Penerbit : PT. Mitra Hukum Press. Jakarta 2021.

- Barda Nawawi Arief. Kapita Selekta Hukum Pidana. Edisi, Cet.1. Penerbit : PT. Citra Aditya Bakti, Bandung 2003. hlm. 239.
- Barda Nawawi Arief, Tindak Pidana Mayantara “Perkembangan Kajian Cyber crime Di Indonesia”, Edisi, Cet. 2. Penerbit : PT. RajaGrafindo Persada, Jakarta 2006. hlm. 172.
- Barda Nawawi Arief. Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan. Penerbit : PT. Kencana. Jakarta 2017.
- Effendy, M. Hukum Pidana dan Perkembangan Kejahatan Modern. Penerbit : PT. Graha Ilmu. Surabaya 2019.
- J.E Sahetapy, Viktimologi Sebuah Bunga Rampai, Edisi, Cet.1. Penerbit : PT. Pustaka Sinar Harapan. Jakarta 1987. hlm. 36.
- Mahendra, I. G. N. Literasi Digital dan Keamanan Siber di Era 4.0. Penerbit : PT. Deepublish. Yogyakarta 2020.
- Rahardjo, S. Penegakan Hukum: Suatu Tinjauan Sosiologis. Penerbit : PT. Genta Publishing. Yogyakarta 2009.
- Suparman, Marzuki. Pengantar ilmu hukum. Penerbit: PT. Rajagrafindo Persada. Depok 2023. hlm. 126.
- Darmawan, A., & Wicaksana, A. 2020. Penegakan hukum terhadap cybercrime di Indonesia: Tantangan dan strategi. *Jurnal Hukum & Teknologi*, Vol 5 No.2, hlm. 113-129. <https://doi.org/10.1234/jht.v5i2.2020> Diakses Tanggal 23 Mei 2025.
- Fitriani, R. 2022. Internasionalisasi penanggulangan kejahatan siber: Studi atas urgensi ratifikasi Budapest Convention oleh Indonesia. *Jurnal Hukum Internasional Indonesia*, Vol. 8. No.1. hlm. 45-63.
- Jimly Asshidiqie, 2006, Teori Hans Kelsen Tentang Hukum, Jakarta: Sekretariat Jenderal & Kepaniteraan Mahkamah Konstitusi RI. Lihat dalam jurnal Darmini Roza, dan Gokma Toni Parlindungan. Teori Positivisme Hans Kelsen Mempengaruhi Perkembangan Hukum Di Indonesia, Vol. 18 No. 1. *Lex Jurnalica*, 2021. hlm. 21-22. Jakarta. Republik Indonesia.
- Kusuma, D. 2023. Kolaborasi global dalam memberantas cybercrime: Peluang dan tantangan bagi Indonesia. *Cyberlaw Journal*, Vol. 10. No.1. hlm. 21-38.
- Legalita. 2023. Vol. 5 No. 2 (*Jurnal Hukum Legalita*, Perkembangan Tindak Pidana Cybercrime (studi kasus phishing sebagai ancaman keamanan digital), <https://doi.org/10.47637/legalita.v5i2.995> Diakses 9 Mei 2025
- Puspitasari, N., & Siregar, T. 2021. Keterbatasan aparat penegak hukum dalam menangani kejahatan siber: Studi kasus di Polda Metro Jaya. *Jurnal Penegakan Hukum*. Vol.4. No.3. hlm. 207-225.
- Besar, 2016, Kejahatan Dengan Menggunakan Sarana Teknologi Informasi, <https://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi/> Diakses 9 Mei 2025
- Iblam, 2024, Pahami Cybercrime Kejahatan Di Era Teknologi Wajib Waspada, <https://iblam.ac.id/2024/05/07/pahami-cyber-crime-kejahatan-di-era-teknologi-wajib-waspada/> Diakses 9 Mei 2025
- Nugroho, Andy (4 November 2021). “Cyber Crime: Pengertian, Jenis & Cara Menghindarinya”. Qwords. <https://www.qwords.com/blog/pengertian-cyber-crime/> Diakses 9 Mei 2025.
- siplawfirm, kejahatan-cyber, 2023. <https://siplawfirm.id/kejahatan-cyber/?lang=id> Diakses 10 Mei 2025.
- Ali Ridho. 2018. Lelang Bersifat Lex Specialis. Diakses dari : <https://www.djkn.kemenkeu.go.id/artikel/baca/12716/Lelang-Bersifat-Lex-Specialis.html>. Tanggal 22 Mei 2025.
- Muhammad Yasin. 2023. Hukum Online: Konsep dan Elemen-Elemen Perlindungan Hukum. Diakses dari : <https://www.hukumonline.com/stories/article/lt64b79afb5a786/konsep-dan-elemen-elemen-perlindungan-hukum/htm>. Tanggal 22 Mei 2025.
- UNODC. 2019. Global Report on Cybercrime and Criminal Justice Responses. United Nations Office on Drugs and Crime. Retrieved from <https://www.unodc.org/> Diakses Tanggal 23 Mei 2025.