Inovasi : Jurnal Sosial Humaniora dan Pendidikan
Volume. 4 Nomor. 2 Mei 2025
e-ISSN : 2809-0268; p-ISSN : 2809-0403, Hal. 815-825
DOI: https://doi.org/10.55606/inovasi.v4i2.4425
Available online at: https://journalcenter.org/index.php/inovasi

Ancaman Cybercrime di Indonesia: Tinjauan Sistematis dan Peran Cybersecurity pada E-Commerce dalam Hukum Pidana

Nanci Yosepin Simbolon *
Universitas Darma Agung, Indonesia
Email: nanciisimbolon123@gmail.com

Jl. DR. TD Pardede No.21, Petisah Hulu, Kec. Medan Baru, Kota Medan, Sumatera Utara
Korespondensi penulis: nanciisimbolon123@gmail.com *

Abstract. *The rapid development of information and communication technology in Indonesia brings serious challenges in the form of increasing cybercrime threats, especially in the e-commerce sector which is the backbone of the national digital economy. This research conducts a systematic review of various forms of cybercrime threats that threaten data security and e-commerce transactions in Indonesia, and examines the role of cybersecurity technology in mitigating these risks. In addition, this study examines the effectiveness of criminal law regulations, particularly the Electronic Information and Transaction Law (ITE Law), in tackling cybercrime. The review shows that cyber threats are increasingly complex with the emergence of artificial intelligence (AI) technology used for automated attacks and sophisticated scams such as deepfake and voice phishing. Cybersecurity plays an important role in protecting e-commerce platforms through the implementation of encryption technology, multi-factor authentication, and real-time system monitoring. However, criminal law enforcement against cybercrime still faces obstacles such as the anonymity of perpetrators and the cross-border nature of cybercrime. Therefore, a synergy between strengthening cybersecurity technology and harmonizing criminal law regulations is needed to create a safe and reliable e-commerce ecosystem in Indonesia. This research provides strategic recommendations for the government and business actors in strengthening national cyber resilience in the face of evolving threats. This theoretical study shows that the threat of cybercrime in Indonesia, especially in the e-commerce sector, is a complex phenomenon that requires a comprehensive criminal law approach and strong cybersecurity technology support. This theoretical study shows that the threat of cybercrime in Indonesia, especially in the e-commerce sector, is a complex phenomenon that requires a comprehensive criminal law approach and strong cybersecurity technology support. This research uses secondary data in the form of scientific articles, research reports, books, as well as laws and regulations related to cybercrime and cybersecurity in Indonesia, especially the ITE Law and the Criminal Code. In the context of e-commerce, cybercrime threatens customer data security, transaction integrity, and business reputation. Therefore, the role of cybersecurity becomes vital as the main fortress that protects e-commerce platforms through the implementation of encryption technology, intrusion detection systems, multi-factor authentication, and real-time monitoring.*

Keywords: *Criminal Law; Cybercrime Threat; E-Commerce Cybersecurity*

Abstrak. Perkembangan pesat teknologi informasi dan komunikasi di Indonesia membawa tantangan serius berupa meningkatnya ancaman cybercrime, khususnya pada sektor e-commerce yang menjadi tulang punggung ekonomi digital nasional. Penelitian ini melakukan tinjauan sistematis terhadap berbagai bentuk ancaman cybercrime yang mengancam keamanan data dan transaksi e-commerce di Indonesia, serta mengkaji peran teknologi cybersecurity dalam mitigasi risiko tersebut. Selain itu, penelitian ini menelaah efektivitas regulasi hukum pidana, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dalam menanggulangi kejahatan siber. Hasil tinjauan menunjukkan bahwa ancaman siber semakin kompleks dengan kemunculan teknologi kecerdasan buatan (AI) yang digunakan untuk serangan otomatis dan penipuan canggih seperti deepfake dan phishing suara. Cybersecurity berperan penting dalam melindungi platform e-commerce melalui penerapan teknologi enkripsi, otentikasi multi-faktor, dan pemantauan sistem secara real-time. Namun, penegakan hukum pidana terhadap cybercrime masih menghadapi kendala seperti anonimitas pelaku dan sifat lintas batas kejahatan siber. Oleh karena itu, sinergi antara penguatan teknologi keamanan siber dan harmonisasi regulasi hukum pidana diperlukan untuk menciptakan ekosistem e-commerce yang aman dan terpercaya di Indonesia. Penelitian ini memberikan rekomendasi strategis bagi pemerintah dan pelaku bisnis dalam memperkuat ketahanan siber nasional menghadapi ancaman yang terus berkembang. Kajian teoritis ini menunjukkan bahwa ancaman cybercrime di Indonesia, khususnya pada sektor e-commerce, merupakan fenomena kompleks yang membutuhkan pendekatan hukum pidana yang komprehensif dan dukungan teknologi

Received: Mei 13, 2025; Revised: Mei 27, 2025; Accepted: Juni 10, 2025; Published: Juni 16, 2025

cybersecurity yang kuat. Kajian teoritis ini menunjukkan bahwa ancaman cybercrime di Indonesia, khususnya pada sektor e-commerce, merupakan fenomena kompleks yang membutuhkan pendekatan hukum pidana yang komprehensif dan dukungan teknologi cybersecurity yang kuat. Penelitian ini menggunakan data sekunder berupa artikel ilmiah, laporan penelitian, buku, serta peraturan perundang-undangan terkait cybercrime dan cybersecurity di Indonesia, khususnya UU ITE dan KUHP. Dalam konteks e-commerce, cybercrime mengancam keamanan data pelanggan, integritas transaksi, serta reputasi bisnis. Oleh karena itu, peran cybersecurity menjadi sangat vital sebagai benteng pertahanan utama yang melindungi platform e-commerce melalui penerapan teknologi enkripsi, sistem deteksi intrusi, otentikasi multi-faktor, dan pemantauan secara real-time.

Kata Kunci: Ancaman Cybercrime; Cybersecurity E-Commerce; Hukum Pidana.

1. LATAR BELAKANG

Perkembangan pesat teknologi informasi dan komunikasi di Indonesia telah membawa dampak signifikan terhadap berbagai sektor, khususnya dalam bidang perdagangan elektronik (e-commerce). Namun, kemajuan ini juga diiringi dengan meningkatnya ancaman kejahatan siber (cybercrime) yang semakin kompleks dan beragam (Ketaren, 2017). Data terkini menunjukkan bahwa pada kuartal pertama tahun 2025, Indonesia menghadapi lebih dari 3 juta serangan siber berbasis web yang berhasil dideteksi dan diblokir, menjadikan Indonesia sebagai negara dengan tingkat serangan siber tertinggi kedua di Asia Tenggara. Jenis serangan yang paling banyak terjadi meliputi peretasan akun, phishing, ransomware, dan penyebaran informasi pribadi tanpa izin (doxing) (Sari, 2014). Korban dari serangan ini tidak hanya pelaku bisnis, tetapi juga pelajar, aktivis, dan masyarakat umum.

Ancaman cybercrime ini sangat mengancam stabilitas dan kepercayaan dalam ekosistem e-commerce, yang menjadi salah satu pilar utama perekonomian digital Indonesia. Kerugian akibat kejahatan siber diperkirakan akan mencapai triliunan rupiah, dengan pelaku kejahatan yang semakin terorganisir layaknya sebuah entitas bisnis profesional. Oleh karena itu, peran cybersecurity menjadi sangat krusial dalam melindungi transaksi dan data pelanggan di platform e-commerce agar dapat menciptakan lingkungan digital yang aman dan terpercaya (Artanto, 2023). Peran cybersecurity dalam melindungi platform e-commerce dari ancaman cyber sangat krusial dan mencakup berbagai aspek penting untuk menjaga keamanan data, transaksi, dan kepercayaan pelanggan. Cybersecurity merupakan fondasi utama dalam menjaga keamanan platform e-commerce dari ancaman cyber yang semakin kompleks, sehingga bisnis dapat beroperasi dengan aman dan pelanggan merasa terlindungi saat bertransaksi (Alshaikhi, 2023).

Penelitian ini bertujuan untuk melakukan tinjauan sistematis terhadap berbagai bentuk ancaman cybercrime yang terjadi di Indonesia, khususnya yang berdampak pada sektor e-commerce, serta mengkaji peran dan efektivitas strategi cybersecurity dalam menghadapi tantangan tersebut. Dengan memahami karakteristik ancaman dan langkah-langkah

perlindungan yang diterapkan, diharapkan dapat memberikan rekomendasi yang komprehensif bagi pemangku kepentingan dalam memperkuat keamanan digital di Indonesia. Latar belakang ini menggabungkan data statistik terbaru dan konteks penting terkait ancaman cybercrime dan cybersecurity di Indonesia, khususnya pada sektor e-commerce. Jika Anda ingin, saya juga dapat membantu menyusun bagian lain dari penelitian ini (Gultom, 2023).

2. KAJIAN TEORITIS

Cybercrime merupakan tindak pidana yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, khususnya internet, yang berbeda dengan kejahatan konvensional karena menggunakan kecerdasan dan teknik digital canggih sebagai alatnya. Dalam konteks e-commerce, cybercrime seringkali berupa pencurian uang elektronik (e-money) (Arroyabe et al., 2024), pembobolan rekening, penipuan transaksi online, dan penyalahgunaan data pelanggan. Kejahatan ini termasuk dalam kategori kejahatan ekonomi karena motif utamanya adalah merugikan harta benda secara finansial, yang berdampak langsung pada perekonomian nasional apabila tidak ditangani dengan serius.

Indonesia mengalami peningkatan signifikan dalam kasus cybercrime yang menargetkan platform e-commerce, seperti carding (penggunaan kartu kredit palsu), phishing, dan penipuan jual beli online (Anisa Fitri, 2022). Kejahatan ini tidak hanya merugikan konsumen, tetapi juga pelaku usaha dan sistem ekonomi digital secara keseluruhan. Penipuan dalam transaksi elektronik seringkali sulit diungkap karena pelaku berada di dunia maya dengan identitas yang tersembunyi, sehingga menimbulkan tantangan besar dalam penegakan hukum (Onwuadiamu, 2025a).

Hukum pidana Indonesia telah mengakomodasi tindak pidana cybercrime melalui beberapa regulasi, terutama Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan Undang-Undang No. 19 Tahun 2016. UU ITE memberikan dasar hukum yang lebih spesifik untuk menjerat pelaku kejahatan dunia maya, termasuk penipuan online dan pembobolan rekening e-commerce (Nabila A'yun et al., 2021). Meskipun KUHP masih digunakan untuk kasus penipuan konvensional, namun untuk tindak pidana yang terjadi di dunia maya, UU ITE lebih relevan karena mengatur secara khusus perbuatan yang dilarang di ranah digital.

Cybercrime di bidang e-commerce dikategorikan sebagai kejahatan ekonomi karena merugikan harta benda dan mengancam stabilitas ekonomi digital. Pelaku cybercrime memanfaatkan celah teknologi untuk melakukan pencurian uang elektronik dan penipuan transaksi yang dapat menurunkan kepercayaan masyarakat terhadap sistem pembayaran

digital dan transaksi online (Haerunnisa et al., 2021). Jika dibiarkan, hal ini dapat menghambat perkembangan ekonomi digital Indonesia dan menurunkan minat masyarakat untuk bertransaksi secara online. Cybersecurity berperan sebagai lini pertahanan utama dalam mencegah dan meminimalisasi dampak cybercrime di e-commerce. Dengan penerapan teknologi keamanan seperti enkripsi, firewall, sistem deteksi intrusi, dan otentikasi multi-faktor, platform e-commerce dapat melindungi data pelanggan dan transaksi dari serangan siber. Perlindungan ini tidak hanya mengurangi risiko kerugian finansial, tetapi juga memperkuat posisi hukum dalam menjerat pelaku karena adanya bukti digital yang dapat digunakan dalam proses penegakan hukum (Tubaishat & Alaleeli, 2024).

Kajian teoritis ini menunjukkan bahwa ancaman cybercrime di Indonesia, khususnya pada sektor e-commerce, merupakan fenomena kompleks yang membutuhkan pendekatan hukum pidana yang komprehensif dan dukungan teknologi cybersecurity yang kuat. Upaya harmonisasi antara regulasi hukum dan teknologi keamanan menjadi kunci dalam melindungi ekosistem digital dan mendorong pertumbuhan ekonomi digital yang sehat di Indonesia.

3. METODE PENELITIAN

Penelitian ini menggunakan metode tinjauan pustaka sistematis (Systematic Literature Review - SLR) untuk mengidentifikasi, menganalisis, dan mensintesis berbagai literatur yang relevan mengenai ancaman cybercrime di Indonesia, peran cybersecurity dalam e-commerce, serta aspek hukum pidana yang mengaturnya. Pendekatan ini dipilih karena memungkinkan peneliti memperoleh gambaran komprehensif dan terkini dari berbagai sumber terpercaya secara terstruktur dan objektif.

Penelitian ini bertujuan untuk mengetahui bentuk ancaman cybercrime yang mengancam e-commerce di Indonesia, serta menganalisis peran cybersecurity dalam menghadapi ancaman tersebut dari perspektif hukum pidana. Pencarian artikel, jurnal, dan dokumen hukum dilakukan melalui database akademik seperti Google Scholar, jurnal nasional dan internasional dengan kata kunci “cybercrime”, “cybersecurity”, “e-commerce”, dan “hukum pidana Indonesia”. Literatur yang dipilih adalah yang relevan dan terbaru, khususnya yang membahas aspek hukum dan teknologi keamanan siber di Indonesia (Purnama & Putri, 2021).

Artikel dan dokumen yang ditemukan diseleksi berdasarkan relevansi dan kualitasnya, kemudian disimpan dan dikelola menggunakan aplikasi manajemen referensi seperti Mendeley untuk memudahkan analisis. Data literatur dianalisis secara kualitatif dengan teknik deskriptif dan komparatif untuk mengidentifikasi pola, kesenjangan, dan

hubungan antara ancaman cybercrime, peran cybersecurity, dan regulasi hukum pidana yang berlaku. Analisis ini juga mengkaji efektivitas aturan hukum dalam menanggulangi kejahatan siber di sektor e-commerce serta tantangan penegakannya.

Penelitian ini menggunakan data sekunder berupa artikel ilmiah, laporan penelitian, buku, serta peraturan perundang-undangan terkait cybercrime dan cybersecurity di Indonesia, khususnya UU ITE dan peraturan pendukung lainnya. Penelitian ini terbatas pada kajian literatur dan tidak melakukan pengumpulan data primer seperti wawancara atau survei. Oleh karena itu, hasil penelitian lebih bersifat teoritis dan konseptual, yang dapat menjadi dasar untuk penelitian lanjutan dengan pendekatan empiris. Metode ini sesuai dengan praktik penelitian terkini dalam bidang keamanan siber dan hukum pidana di Indonesia, serta memberikan pendekatan holistik untuk memahami ancaman cybercrime dan solusi keamanan yang dapat diterapkan pada platform e-commerce.

4. HASIL DAN PEMBAHASAN

Ancaman Cybercrime di Indonesia terhadap E-Commerce

Indonesia menghadapi peningkatan signifikan ancaman cybercrime, terutama pada sektor e-commerce yang terus berkembang pesat. Berdasarkan data terbaru, pada kuartal I 2025, Indonesia mengalami lebih dari 3 juta serangan siber berbasis web yang berhasil diblokir, menunjukkan tingginya risiko terhadap platform digital. Ancaman ini meliputi serangan phishing yang meningkat hingga 350%, ransomware naik 150%, dan penipuan e-commerce melonjak 500%. Serangan-serangan ini tidak hanya merugikan secara finansial, tetapi juga mengancam data pribadi konsumen dan reputasi bisnis e-commerce (Novita et al., 2023).

Perkembangan teknologi seperti kecerdasan buatan (AI) juga membawa tantangan baru berupa AI agentik yang mampu melakukan serangan siber secara otomatis dan masif, serta teknik penipuan canggih seperti deepfake dan vishing (phishing suara). Serangan rantai pasokan (supply chain attack) juga menjadi perhatian karena dapat mengganggu operasional e-commerce melalui pihak ketiga, seperti vendor logistik, yang berdampak pada keamanan data pelanggan dan layanan. Menghadapi ancaman yang semakin kompleks dan canggih, peran cybersecurity menjadi sangat penting dalam menjaga keamanan platform e-commerce (Hu et al., 2018). Cybersecurity berfungsi untuk melindungi data pelanggan dan transaksi melalui berbagai teknologi dan kebijakan, seperti enkripsi data, firewall, sistem deteksi intrusi, otentikasi multi-faktor, serta pendekatan keamanan zero-trust. Selain itu, pemantauan sistem secara real-time dan pengujian penetrasi secara berkala menjadi strategi penting untuk mengidentifikasi dan menutup celah keamanan sebelum dimanfaatkan oleh pelaku kejahatan

siber.

Upaya edukasi dan peningkatan kesadaran keamanan siber di kalangan pelaku e-commerce dan konsumen juga menjadi bagian penting dalam membangun ekosistem digital yang aman dan terpercaya. Dengan demikian, cybersecurity tidak hanya berperan sebagai pelindung teknis, tetapi juga sebagai pilar utama dalam mempertahankan kepercayaan pelanggan dan kelangsungan bisnis e-commerce. Dalam konteks hukum pidana, Indonesia telah mengatur tindak pidana cybercrime melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang memberikan landasan hukum untuk menjerat pelaku kejahatan siber, termasuk penipuan online, pembobolan data, dan penyalahgunaan informasi elektronik. UU ITE menjadi instrumen utama dalam penegakan hukum terhadap cybercrime di Indonesia, melengkapi KUHP yang kurang spesifik mengatur kejahatan di ranah digital (Ghahtarani et al., 2020). Namun, penegakan hukum terhadap cybercrime menghadapi berbagai tantangan, seperti kesulitan mengidentifikasi pelaku yang beroperasi secara anonim di dunia maya, sifat lintas batas negara dari kejahatan siber, serta kebutuhan peningkatan kapasitas aparat penegak hukum dalam aspek teknis dan forensik digital. Oleh karena itu, sinergi antara kebijakan hukum, teknologi cybersecurity, dan kerja sama internasional sangat diperlukan untuk mengatasi ancaman ini secara efektif.

Ancaman cybercrime yang terus meningkat mengharuskan pelaku e-commerce dan pemerintah untuk memperkuat sistem keamanan dan regulasi. Penerapan teknologi cybersecurity mutakhir dan kebijakan keamanan yang ketat harus menjadi prioritas untuk melindungi data dan transaksi elektronik. Di sisi hukum, pembaruan regulasi dan peningkatan kapasitas penegak hukum dalam menangani kasus cybercrime sangat penting untuk memberikan efek jera kepada pelaku (Salsabila & Ispriyarso, 2023). Selain itu, kolaborasi antara sektor swasta, pemerintah, dan masyarakat dalam meningkatkan literasi keamanan siber serta kesadaran akan risiko cybercrime sangat dibutuhkan agar ekosistem e-commerce di Indonesia dapat berkembang dengan aman dan berkelanjutan. Pembahasan ini menggambarkan hubungan erat antara ancaman cybercrime yang terus berkembang, peran strategis cybersecurity dalam mitigasi risiko, serta pentingnya dukungan hukum pidana yang adaptif untuk melindungi sektor e-commerce di Indonesia secara menyeluruh (Didwal & Negi, 2022).

Regulasi Hukum Pidana Efektif Menanggulangi Ancaman Siber di Indonesia

Regulasi hukum pidana harus diperbarui secara berkala agar mampu mengakomodasi perkembangan teknologi baru seperti blockchain, cryptocurrency, kecerdasan buatan (AI), serta modus-modus kejahatan siber yang terus berkembang. Definisi dan sanksi terhadap kejahatan siber harus dibuat lebih jelas dan spesifik, termasuk untuk kejahatan baru seperti

penipuan berbasis AI dan deepfake. Penegak hukum perlu mendapatkan pelatihan khusus dalam forensik digital dan investigasi kejahatan siber agar dapat menangani kasus dengan efektif. Penggunaan teknologi canggih seperti AI untuk deteksi dan analisis ancaman secara real-time juga perlu diintegrasikan dalam proses penegakan hukum (Onwuadiamu, 2025b). Karena kejahatan siber bersifat lintas negara, harmonisasi hukum internasional dan perjanjian ekstradisi harus diperkuat untuk mempermudah penindakan pelaku kejahatan siber yang beroperasi antarnegara. Kolaborasi ini penting agar penegakan hukum tidak terhambat oleh batas wilayah negara.

Masyarakat dan pelaku bisnis harus diberikan edukasi mengenai risiko kejahatan siber dan cara pencegahannya. Kesadaran publik yang tinggi akan mengurangi kerentanan terhadap serangan siber dan meningkatkan partisipasi dalam pelaporan kejahatan siber. Regulasi juga harus mengatur mekanisme perlindungan dan pemulihan bagi korban kejahatan siber, termasuk kompensasi dan pemulihan data, sehingga memberikan rasa aman dan keadilan bagi masyarakat (Wissink et al., 2023). Penggunaan teknologi terbaru seperti sistem pemantauan otomatis, big data analytics, dan AI dapat membantu aparat penegak hukum dalam mendeteksi, melacak, dan mengungkap pelaku cybercrime dengan lebih efisien dan cepat (Dib et al., 2024).

Berikut adalah pasal-pasal hukum pidana yang efektif menanggulangi ancaman siber di Indonesia, khususnya yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) terbaru:

1. Pasal 27 ayat (1) - Kesusilaan, perjudian, penghinaan, dan pemerasan Melarang penyebaran konten asusila, perjudian online, pencemaran nama baik, dan pemerasan melalui media elektronik.
2. Pasal 28 - Berita bohong dan ujaran kebencian (SARA). Melarang penyebaran berita bohong yang dapat merugikan orang lain dan ujaran kebencian yang mengandung unsur SARA.
3. Pasal 30 - Akses ilegal (Peretasan). Mengatur larangan mengakses komputer atau sistem elektronik milik orang lain tanpa hak, dengan ancaman pidana penjara maksimal 6 tahun dan/atau denda sampai Rp600 juta.
4. Pasal 31 – Penyadapan. Melarang penyadapan secara ilegal terhadap informasi elektronik.
5. Pasal 32 - Modifikasi informasi, membuka rahasia. Melarang perubahan informasi elektronik secara tidak sah dan membuka rahasia elektronik.
6. Pasal 33 - Mengganggu atau mengacaukan sistem elektronik. Larangan tindakan yang mengganggu sistem elektronik seperti serangan DDoS.

7. Pasal 34 - Memfasilitasi kejahatan. Melarang membantu atau memfasilitasi tindak pidana siber.
8. Pasal 35 - Memalsukan informasi elektronik. Melarang pemalsuan informasi atau dokumen elektronik dengan ancaman pidana penjara hingga 12 tahun dan/atau denda maksimal Rp12 miliar.
9. Pasal 36 - Merugikan orang lain. Melarang perbuatan yang menyebabkan kerugian orang lain melalui sistem elektronik.

Pasal-Pasal Dalam KUHP Baru (UU No. 1 Tahun 2023)

1. Pasal 332 ayat (1) - Akses illegal.

   Setiap orang yang dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik milik orang lain dipidana penjara maksimal 6 tahun atau denda kategori V (sekitar Rp500 juta).
2. Pasal 332 ayat (3) - Akses ilegal dengan menerobos sistem pengamanan. Akses tanpa hak yang melanggar atau menjebol sistem pengamanan dipidana penjara maksimal 8 tahun atau denda kategori VI.
3. Pasal 335 - Penghilangan informasi rahasia pemerintah. Mengatur sanksi pidana maksimal 12 tahun bagi pelaku yang menghilangkan informasi elektronik rahasia pemerintah.

Pasal-pasal tersebut secara khusus mengatur berbagai bentuk tindak pidana siber, mulai dari akses ilegal, penyebaran konten negatif, pemalsuan data elektronik, hingga gangguan sistem elektronik (Afraji et al., 2025). Sanksi pidana yang cukup berat berupa penjara dan denda besar dirancang untuk memberikan efek jera dan melindungi masyarakat serta bisnis, termasuk sektor e-commerce, dari ancaman cybercrime (A Yassa et al., 2023).

5. KESIMPULAN

Ancaman cybercrime di Indonesia terus meningkat secara signifikan, terbukti dengan lebih dari 3 juta serangan siber berbasis web yang berhasil diblokir pada kuartal pertama 2025, menjadikan Indonesia sebagai negara dengan tingkat serangan siber tertinggi kedua di Asia Tenggara. Ancaman ini sangat beragam, mulai dari peretasan akun, phishing, ransomware, hingga penyebaran informasi pribadi tanpa izin, yang tidak hanya merugikan individu tetapi juga pelaku usaha e-commerce dan stabilitas ekonomi digital nasional.

Dalam konteks e-commerce, cybercrime mengancam keamanan data pelanggan, integritas transaksi, serta reputasi bisnis. Oleh karena itu, peran cybersecurity menjadi sangat vital sebagai benteng pertahanan utama yang melindungi platform e-commerce

melalui penerapan teknologi enkripsi, sistem deteksi intrusi, otentikasi multi-faktor, dan pemantauan secara real-time. Cybersecurity juga berkontribusi dalam menjaga kepercayaan konsumen dan kelangsungan bisnis di era digital.

Dari aspek hukum pidana, Indonesia telah mengatur tindak pidana cybercrime melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang memberikan dasar hukum untuk menjerat pelaku kejahatan siber secara spesifik. Namun, penegakan hukum masih menghadapi tantangan seperti sifat lintas batas kejahatan siber, anonimitas pelaku, dan keterbatasan kapasitas aparat penegak hukum. Oleh karena itu, harmonisasi regulasi, peningkatan kapasitas penegak hukum, serta kerja sama internasional sangat diperlukan untuk meningkatkan efektivitas penanganan cybercrime.

Penanggulangan ancaman cybercrime di Indonesia membutuhkan sinergi antara penguatan teknologi cybersecurity dan pembaruan hukum pidana yang adaptif. Langkah ini penting untuk menciptakan ekosistem e-commerce yang aman dan terpercaya, sekaligus menjaga stabilitas ekonomi digital Indonesia di tengah pesatnya transformasi teknologi informasi. Kesimpulan ini mengintegrasikan data terbaru tentang ancaman siber di Indonesia, peran teknologi keamanan, dan aspek hukum pidana yang relevan untuk memberikan gambaran komprehensif dan terkini.

DAFTAR REFERENSI

Jurnal

A Yassa, H., N Zakaria, R., & Z Abdellah, N. (2023). COVID-19 Pandemic Fuels Rise in Cybercrime. *Journal of Information Security and Cybercrimes Research*, *6*(1), 01–10. https://doi.org/10.26735/kuxw6317

Afraji, D. M. A. A., Lloret, J., & Peñalver, L. (2025). Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments. *Cyber Security and Applications*, *3*(September 2024), 100085. https://doi.org/10.1016/j.csa.2025.100085

Alshaikhi, K. I. S. (2023). Meningkatkan Kapasitas Nasional Cybersecurity Authority (NCA) Kerajaan Arab Saudi untuk Memperkuat Keamanan Digital Nasional. *Lembaga Ketahanan Nasional Rebuplik Indonesia*.

Anisa Fitri, N. (2022). Dampak E-Commerce terhadap Strategi Pemasaran (Studi Kasus Pada Platform Shopee). *Juli-Desember*, *01*(2), 67–77.

Arroyabe, M. F., Arranz, C. F. A., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers and Security*, *141*(February), 103826. https://doi.org/10.1016/j.cose.2024.103826

Artanto. (2023). Transformasi Media Massa Untuk Membangun Opini Positif Guna Meningkatkan Ketahanan Nasional. *Lembaga Ketahanan Nasional Republik Indonesia*.

Dib, O., Nan, Z., & Liu, J. (2024). Machine learning-based ransomware classification of Bitcoin transactions. *Journal of King Saud University - Computer and Information Sciences*, *36*(1), 101925. https://doi.org/10.1016/j.jksuci.2024.101925

Didwal, D. A., & Negi, D. R. (2022). Legal and Economic Perspective of the Consumer Protection Act, 2019 in India: An Overview. *International Journal of Scientific Research and Management*, *10*(08), 375–383. https://doi.org/10.18535/ijsrm/v10i08.lla01

Ghahtarani, A., Sheikhmohammady, M., & Rostami, M. (2020). The impact of social capital and social interaction on customers' purchase intention, considering knowledge sharing in social commerce context. *Journal of Innovation and Knowledge*, *5*(3), 191–199. https://doi.org/10.1016/j.jik.2019.08.004

Gultom, R. J. S. & E. R. (2023). Analisis Hukum terkait Melindungi Konsumen dalam Bertransaksi Digital di E Commerce Shopee. *Jurnal Pendidikan Dan Konseling*, *5*(19), 328–334.

Haerunnisa, Dwi Khaira Ramdhanni, & Ricky Firmansyah. (2021). Analisi Strategi Negosiasi Pada Platform Shopee. *ATRABIS: Jurnal Administrasi Bisnis (e-Journal)*, *7*(1), 29–38. https://doi.org/10.38204/atrabis.v7i1.602

Hu, S. K., Liou, J. J. H., Chuang, Y. C., & Tzeng, G. H. (2018). New hybrid fmadm model for mobile commerce improvement. *Technological and Economic Development of Economy*, *24*(5), 1801–1828. https://doi.org/10.3846/20294913.2017.1318311

Ketaren, E. (2017). Cybercrime, Cyber Space, Dan Cyber Law. *Jurnal TIMES*, *5*(2), 35–42. https://doi.org/10.51351/jtm.5.2.2016556

Nabila A'yun, Q. A., Chusma, N. M., Putri, C. N. A., & Latifah, F. N. (2021). Implementasi Etika Bisnis Islam Dalam Transaksi Jual Beli Online Pada E-Commerce Popular Di Indonesia. *JPSDa: Jurnal Perbankan Syariah Darussalam*, *1*(2), 166–181. https://doi.org/10.30739/jpsda.v1i2.998

Novita, A. P., Fatmanegara, F., Runtuwene, F. J. J., Samuela, J. T., & Syahbani, M. F. (2023). Cyber Security Threats; Analisis Dan Mitigasi Resiko Ransomware Di Indonesia. *Jurnal Ilmiah Sistem Informasi*, *3*(1), 160–169. https://doi.org/10.46306/sm.v3i1.91

Onwuadiamu, G. (2025a). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*(February), 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Onwuadiamu, G. (2025b). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*(December 2024), 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Purnama, N. I., & Putri, L. P. (2021). Analisis Penggunaan E-Commerce Di Masa Pandemi. *Seminar Nasional Teknologi Edukasi Dan Humaniora*, *1*(1), 553–558. http://jurnal.ceredindonesia.or.id/index.php/sintesa/article/view/357

Salsabila, D., & Ispriyarso, B. (2023). Efektivitas Keabsahan Kontrak Elektronik Berdasarkan Hukum Positif di Indonesia. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(2), 1343–1354. https://doi.org/10.37680/almanhaj.v5i2.3085

Sari, I. (2014). Perbedaan Bentuk Kejahatan Yang Dikategorikan Sebagai Cyber Crime Dan Cyber Warfare. *Jurnal Sistem Informasi Universitas Suryadarma*, *10*(1). https://doi.org/10.35968/jsi.v10i1.1002

Tubaishat, A., & Alaleeli, H. (2024). A Framework to Prevent Cybercrime in the UAE. *Procedia Computer Science*, *238*, 558–565. https://doi.org/10.1016/j.procs.2024.06.060

Wissink, I. B., Standaert, J. C. A., Stams, G. J. J. M., Asscher, J. J., & Assink, M. (2023). Risk factors for juvenile cybercrime: A meta-analytic review. *Aggression and Violent Behavior*, *70*(March), 101836. https://doi.org/10.1016/j.avb.2023.101836

Peraturan Undang-Undang

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor:27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik