Jurnal Legal Dialogica
Volume I Issue 2 Tahun 2026

Kejahatan Siber Ancaman Nyata di Era Digial Indonesia

Auliya Nilwanda Safitri[1], Nurul Qamar[2], Muhammad Azham Ilham[3]

[123] Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

Email Koresponden : aulyans@gmail.com

Abstrak: Penelitian ini bertujuan untuk menganalisis pengaturan hukum positif Indonesia dalam menanggulangi kejahatan siber di era digitalisasi serta mengidentifikasi faktor-faktor yang berperan dalam upaya antisipatif dari perspektif kriminologi. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Bahan hukum yang dianalisis meliputi bahan hukum primer berupa Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Kitab Undang-Undang Hukum Pidana, Undang-Undang Perlindungan Data Pribadi, serta peraturan terkait keamanan siber; bahan hukum sekunder berupa buku dan jurnal ilmiah; serta bahan hukum tersier sebagai pendukung. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan, kemudian dianalisis secara kualitatif dengan menafsirkan norma hukum dan teori kriminologi yang relevan. Hasil penelitian menunjukkan bahwa pengaturan hukum positif Indonesia dalam penanggulangan kejahatan siber telah berkembang secara komprehensif melalui kombinasi hukum pidana umum, hukum pidana khusus, regulasi administratif, serta penguatan kelembagaan seperti peran Badan Siber dan Sandi Negara. Selain itu, pendekatan kebijakan kriminal tidak hanya bersifat represif, tetapi juga preventif melalui kewajiban pengamanan sistem elektronik, perlindungan data pribadi, dan pelaporan insiden siber. Faktor-faktor yang memengaruhi efektivitas antisipasi kejahatan siber meliputi kualitas regulasi, kapasitas aparat penegak hukum, infrastruktur teknologi, kerja sama nasional dan internasional, literasi digital masyarakat, serta tanggung jawab sektor swasta. Rekomendasi penelitian ini menekankan perlunya penguatan harmonisasi kebijakan hukum siber dalam sistem hukum pidana nasional melalui pendekatan preventif, edukatif, dan teknologi-adaptif tanpa mengesampingkan prinsip perlindungan hak asasi manusia, kepastian hukum, proporsionalitas sanksi, serta keadilan sosial di ruang digital.

Kata Kunci:Kejahatan Siber, Kriminologis, Hukum Pidana, Digitalisasi.

Abstract: *This study aims to analyze Indonesia's positive legal regulations in dealing with cybercrime in the digitalization era and to identify factors that play a role in anticipatory efforts from a criminology perspective. This study uses a normative legal research method with a statutory and conceptual approach. The legal materials analyzed include primary legal materials in the form of the Electronic Information and Transactions Law and its amendments, the Criminal Code, the Personal Data Protection Law, and regulations related to cybersecurity; secondary legal materials in the form of books and scientific journals; and tertiary legal materials as supporting materials. The legal materials were collected through a literature study, then analyzed qualitatively by interpreting relevant legal norms and criminological theories. The research*

results show that Indonesia's positive legal arrangements for combating cybercrime have developed comprehensively through a combination of general criminal law, special criminal law, administrative regulations, and institutional strengthening, such as the role of the National Cyber and Crypto Agency. Furthermore, the criminal policy approach is not only repressive but also preventive, through mandatory security of electronic systems, personal data protection, and reporting of cyber incidents. Factors influencing the effectiveness of cybercrime prevention include regulatory quality, law enforcement capacity, technological infrastructure, national and international cooperation, public digital literacy, and private sector responsibility. This research recommendation emphasizes the need to strengthen the harmonization of cyber law policies within the national criminal justice system through a preventive, educational, and technology-adaptive approach, without neglecting the principles of human rights protection, legal certainty, proportional sanctions, and social justice in the digital space.
Keywords: Cybercrime, Criminology, Criminal Law, Digitalization.

PENDAHULUAN

Arus globalisasi saat ini telah membawa dunia ke dalam era yang sangat dipengaruhi oleh teknologi digital. Kemajuan teknologi informasi dan komunikasi memicu perubahan besar dalam berbagai aspek kehidupan, termasuk ekonomi, sosial, budaya, dan hukum. Digitalisasi telah menciptakan keterhubungan global tanpa batas, sehingga negara-negara dapat bebas berinteraksi secara ekonomi dan sosial melewati batas geografis tradisional. Di satu sisi, hal ini memberi peluang besar dalam hal akses informasi dan kemajuan ekonomi, namun di sisi lain membuka ruang bagi berbagai bentuk konflik baru seperti konflik energi, pangan, bahkan keamanan informasi di dunia digital. Fenomena tersebut merupakan konsekuensi alami globalisasi yang didorong oleh dinamika teknologi modern.[1]

Perkembangan teknologi informasi tidak hanya mempermudah komunikasi dan transaksi jarak jauh, tetapi juga memungkinkan pelaku kriminal memanfaatkan celah digital untuk melakukan kejahatan. Evolusi teknologi jaringan dan perangkat lunak telah memungkinkan munculnya kejahatan canggih seperti cybercrime, yang tidak lagi terbatas pada pelanggaran konvensional tetapi meluas ke pelanggaran digital yang kompleks.[2]

Indonesia sebagai negara dengan jumlah pengguna internet yang besar telah merespon dinamika digital ini melalui regulasi baru. Salah satu regulasi penting

adalah Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang berlaku sejak 2 Januari 2024. UU ini merupakan pembaruan penting dalam menghadapi tantangan hukum di ranah digital dengan tujuan menciptakan ruang digital yang bersih, sehat, produktif, beretika, serta memberikan kepastian hukum dan keadilan bagi masyarakat.

Penambahan pasal-pasal baru dalam UU ITE memperjelas lingkup hukum digital, termasuk perlindungan terhadap anak dalam ekosistem digital dan kewajiban penyelenggara sistem elektronik dalam menjaga keamanan dan etika penggunaan ruang digital.[3]

Kesenjangan antara hukum ideal dan realitas hukum memperlihatkan bahwa sistem hukum pidana Indonesia belum sepenuhnya adaptif terhadap perubahan teknologi. Secara ideal, hukum pidana seharusnya responsif terhadap dinamika teknologi, menjamin keadilan, memberikan efek jera, dan mampu melindungi masyarakat dari ancaman kriminal digital. Namun kenyataannya, regulasi yang ada masih mengalami keterlambatan harmonisasi, kurangnya kapasitas aparat, serta rendahnya literasi hukum masyarakat terkait keamanan digital. Permasalahan tersebut menjadi bukti bahwa penegakan hukum digital membutuhkan pembaruan normatif dan peningkatan kapasitas kelembagaan secara komprehensif.[4]

METODE PENELITIAN

Penelitian normatif ini berfokus pada kajian mendalam terhadap peraturan perundang-undangan, asas-asas hukum, serta doktrin-doktrin hukum yang berkaitan dengan penegakan hukum pidana terhadap kejahatan siber di Indonesia. Penelitian hukum normatif menempatkan hukum sebagai norma atau kaidah yang mengatur perilaku manusia dalam kehidupan bermasyarakat, sehingga objek utama kajian adalah hukum tertulis sebagaimana tertuang dalam peraturan perundang-undangan yang berlaku. Dalam konteks ini, penelitian dilakukan dengan menelaah berbagai ketentuan hukum yang relevan, seperti undang-undang, peraturan pelaksana, serta putusan pengadilan yang memiliki keterkaitan dengan tindak pidana siber.

Pendekatan normatif digunakan karena permasalahan yang diteliti bersifat konseptual dan normatif, yakni berkaitan dengan bagaimana hukum mengatur, mengkualifikasikan,

dan memberikan sanksi terhadap kejahatan siber. Penelitian ini tidak menitikberatkan pada pengumpulan data empiris di lapangan, melainkan pada analisis sistematis terhadap norma hukum yang berlaku serta konsistensi penerapannya dalam sistem hukum pidana Indonesia. Selain itu, pendekatan ini memungkinkan peneliti untuk mengkaji kesesuaian antara peraturan yang ada dengan asas-asas hukum pidana, seperti asas legalitas, kepastian hukum, dan keadilan. Dengan demikian, penelitian normatif diharapkan mampu memberikan pemahaman yang komprehensif mengenai kerangka hukum penegakan pidana terhadap kejahatan siber serta mengidentifikasi potensi permasalahan atau kekosongan hukum yang ada.

PEMBAHASAN

Berdasarkan data yang diperoleh penulis dari bahan hukum normatif, termasuk hal-hal berikut:

1. **Pengaturan Hukum Posittif di Indonesia dalam Menanggulangi Kejahatan Siber di Era Digitalisasi**

   Dalam era digital yang semakin berkembang pesat, perlindungan data pribadi menjadi salah satu isu hukum yang sangat penting untuk diperhatikan. Penelitian ini mengungkapkan bahwa kejahatan siber yang melibatkan pelanggaran terhadap privasi data, menunjukkan tren peningkatan signifikan di Indonesia. Kejahatan seperti pencurian data, penyalahgunaan informasi pribadi, hingga pemalsuan identitas digital tidak hanya merugikan individu tetapi juga berdampak pada kepercayaan masyarakat terhadap sistem digital. Hukum pidana sebagai instrumen penegakan hukum menghadapi tantangan besar dalam mengimbangi kemajuan teknologi yang memungkinkan terjadinya kejahatan tersebut.[5]

   Perubahan terakhir melalui UU No. 1 Tahun 2024 dilakukan antara lain untuk memperjelas rumusan delik, menyeimbangkan perlindungan kebebasan berekspresi dengan kepentingan ketertiban umum, serta memperkuat mekanisme penegakan hukum dalam ruang digital.[6]

   Selain UU ITE, penguatan pengaturan kejahatan siber juga terlihat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).[7] Undang-undang ini menjadi respon terhadap meningkatnya kasus kebocoran dan penyalahgunaan data pribadi yang kerap terjadi melalui sistem elektronik. UU PDP mengkriminalisasi perbuatan memperoleh, mengungkapkan, atau menggunakan data

pribadi secara melawan hukum, serta menetapkan tanggung jawab pidana bagi korporasi yang lalai dalam melindungi data subjek hukum.[8]

Kehadiran UU PDP memperluas rezim hukum siber dari sekadar perlindungan sistem elektronik menjadi perlindungan hak privasi warga negara dalam ruang digital.[9] Kesadaran masyarakat terkait pentingnya melindungi data pribadi mereka masih rendah. Banyak individu yang dengan mudah memberikan informasi pribadi kepada pihak ketiga tanpa memahami risiko yang mungkin timbul, seperti penyalahgunaan data untuk kepentingan komersial atau tindakan kriminal lainnya. Edukasi publik mengenai perlindungan data pribadi dan literasi digital harus menjadi prioritas dalam upaya pencegahan kejahatan siber. Dalam konteks ini, pemerintah perlu berkolaborasi dengan sektor swasta, khususnya penyedia layanan digital, untuk meningkatkan kesadaran dan pemahaman masyarakat mengenai pentingnya menjaga keamanan data pribadi.[10]

Di luar regulasi khusus tersebut, hukum pidana umum juga tetap berperan dalam menanggulangi kejahatan siber. Kitab Undang-Undang Hukum Pidana (KUHP), termasuk KUHP baru yang diundangkan melalui Undang-Undang Nomor 1 Tahun 2023, dapat digunakan untuk menjerat pelaku apabila unsur-unsur tindak pidana konvensional seperti penipuan, pemerasan, atau perbuatan yang menyebabkan kerugian dilakukan dengan menggunakan sarana elektronik. Hal ini menunjukkan bahwa hukum positif Indonesia menganut pendekatan komplementer, yakni memadukan hukum pidana umum dengan undang-undang khusus di bidang teknologi informasi.[11]

Dari sisi kelembagaan, penanggulangan kejahatan siber juga diperkuat melalui pembentukan dan peran Badan Siber dan Sandi Negara (BSSN) yang bertugas menjaga keamanan siber nasional serta mendukung penegakan hukum dalam hal pencegahan dan mitigasi serangan siber. Keberadaan institusi ini mencerminkan bahwa pengaturan hukum positif tidak hanya bersifat represif melalui pemidanaan, tetapi juga preventif melalui peningkatan ketahanan sistem digital nasional.[12]

Dengan demikian, dapat disimpulkan bahwa pengaturan hukum positif Indonesia dalam menanggulangi kejahatan siber di era digitalisasi telah berkembang ke arah yang lebih komprehensif. Hal ini tercermin dari adanya regulasi khusus melalui UU ITE dan UU PDP, dukungan hukum pidana umum, serta penguatan kelembagaan di bidang keamanan siber. Meskipun demikian, efektivitas pengaturan tersebut tetap

bergantung pada kapasitas aparat penegak hukum, kerja sama lintas negara, serta kesadaran hukum masyarakat dalam menggunakan teknologi digital secara bertanggung jawab.[13]

Selain mengatur jenis-jenis perbuatan yang dikualifikasikan sebagai tindak pidana, hukum positif Indonesia juga mengatur aspek prosedural penegakan hukum siber. Ketentuan mengenai penyidikan, penyitaan alat elektronik, penggeledahan sistem, serta penggunaan alat bukti elektronik diatur dalam UU ITE dan diperkuat oleh ketentuan dalam KUHAP. Pengakuan terhadap informasi elektronik dan/atau dokumen elektronik sebagai alat bukti yang sah merupakan terobosan penting karena menyesuaikan hukum acara pidana dengan realitas digital, di mana jejak kejahatan sering kali hanya tersimpan dalam bentuk data.[14]

Lebih lanjut, pengaturan hukum positif Indonesia juga menunjukkan kecenderungan mengikuti standar internasional dalam menghadapi kejahatan siber yang bersifat lintas negara. Meskipun Indonesia belum meratifikasi *Budapest Convention on Cybercrime*, substansi beberapa norma dalam UU ITE seperti kriminalisasi akses ilegal, intersepsi tanpa hak, serta gangguan terhadap sistem elektronik sejalan dengan prinsip-prinsip yang dianut dalam konvensi tersebut. Hal ini menunjukkan adanya proses harmonisasi hukum nasional dengan rezim hukum global guna meningkatkan efektivitas kerja sama internasional dalam penanggulangan kejahatan siber.[15]

Dalam kerangka kebijakan kriminal (*criminal policy*), pengaturan hukum siber di Indonesia tidak hanya bersifat represif, tetapi juga diarahkan pada pendekatan preventif dan administratif. Hal ini tampak dari kewajiban penyelenggara sistem elektronik untuk menjaga keamanan data, menerapkan standar perlindungan sistem, serta melaporkan insiden kebocoran data. Ketentuan tersebut menunjukkan bahwa hukum positif Indonesia tidak semata-mata berorientasi pada pemidanaan pelaku, melainkan juga pada pencegahan melalui penguatan tata kelola keamanan digital.[16]

2. Faktor-Faktor dalam Mengantisipasi Kejahatan Siber

Menentukan keberhasilan antisipasi kejahatan siber adalah kekuatan kerangka regulasi hukum. Peraturan perundang-undangan seperti UU ITE, UU Perlindungan Data Pribadi, serta KUHP baru menyediakan dasar normatif bagi negara untuk melakukan penindakan maupun pencegahan. Kejelasan rumusan delik,

proporsionalitas sanksi, serta pengakuan alat bukti elektronik merupakan unsur penting agar hukum mampu merespons modus kejahatan berbasis teknologi yang terus berkembang. Dalam perspektif kebijakan hukum pidana, regulasi yang baik harus bersifat progresif dan terbuka terhadap pembaruan agar tidak tertinggal oleh inovasi digital.[17]

Terletak pada kapasitas aparat penegak hukum. Penyidik, jaksa, dan hakim dituntut memiliki kompetensi teknis di bidang forensik digital, analisis data elektronik, serta pemahaman terhadap pola kejahatan siber modern. Tanpa sumber daya manusia yang terlatih, penerapan hukum positif akan menghadapi kesulitan dalam pembuktian dan pelacakan pelaku yang menggunakan teknologi enkripsi atau jaringan lintas negara. Oleh karena itu, pelatihan berkelanjutan dan pembentukan unit khusus kejahatan siber menjadi kebutuhan strategis dalam sistem peradilan pidana.[18]

Selain itu, dukungan infrastruktur dan teknologi keamanan siber merupakan faktor penting dalam pencegahan. Negara melalui lembaga seperti Badan Siber dan Sandi Negara (BSSN) berperan dalam memperkuat sistem pertahanan siber nasional, melakukan deteksi dini terhadap serangan, serta membangun standar keamanan bagi penyelenggara sistem elektronik. Infrastruktur keamanan yang kuat memungkinkan terjadinya mitigasi risiko sebelum serangan berkembang menjadi tindak pidana yang merugikan masyarakat luas.[19]

Faktor berikutnya adalah kerja sama nasional dan internasional.

Mengingat kejahatan siber kerap bersifat transnasional, penegakan hukum memerlukan koordinasi antar-lembaga di dalam negeri serta kolaborasi dengan negara lain melalui mekanisme bantuan hukum timbal balik (*mutual legal assistance*), pertukaran informasi intelijen, dan kerja sama kepolisian internasional. Harmonisasi hukum dengan standar global juga menjadi bagian dari strategi antisipatif agar Indonesia tidak menjadi celah bagi pelaku kejahatan siber lintas negara.[20]

Di samping faktor struktural tersebut, kesadaran dan literasi digital masyarakat juga memegang peranan penting. Banyak kejahatan siber, seperti penipuan daring atau pencurian identitas, berhasil dilakukan karena rendahnya pemahaman pengguna terhadap keamanan digital. Program edukasi publik mengenai perlindungan data pribadi,

verifikasi informasi, serta keamanan transaksi elektronik merupakan bagian dari strategi preventif non-penal yang sejalan dengan pendekatan kriminologis dalam pencegahan kejahatan.[21]

Faktor peran sektor swasta dan penyelenggara sistem elektronik tidak dapat diabaikan. Korporasi yang mengelola platform digital memiliki tanggung jawab untuk menerapkan standar keamanan informasi, melindungi data pengguna, serta bekerja sama dengan aparat penegak hukum ketika terjadi insiden siber. Dalam konteks ini, kewajiban hukum yang diatur dalam UU Perlindungan Data Pribadi dan regulasi turunan di bidang sistem elektronik menjadi instrumen penting untuk mendorong kepatuhan dan akuntabilitas pelaku usaha digital.[22]

KESIMPULAN

Dapat disimpulkan bahwa pengaturan hukum positif di Indonesia dalam menanggulangi kejahatan siber di era digitalisasi telah mengalami perkembangan yang semakin sistematis dan komprehensif, terutama setelah diberlakukannya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor

11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini memperbarui dan mempertegas pengaturan mengenai berbagai bentuk tindak pidana siber, seperti akses ilegal terhadap sistem elektronik, gangguan terhadap data dan sistem, penyebaran konten yang melanggar hukum, penipuan berbasis digital, serta penguatan perlindungan hak-hak pengguna di ruang siber. Penguatan tersebut juga dikomplementasi oleh keberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menitikberatkan pada perlindungan hak privasi warga negara serta pengaturan pertanggungjawaban pidana, termasuk bagi korporasi yang lalai menjaga keamanan data pribadi. Oleh karena itu, diperlukan aparat penegak hukum untuk memperoleh peningkatan kapasitas secara berkelanjutan melalui pendidikan dan pelatihan khusus di bidang forensik digital, analisis data elektronik, serta kerja sama internasional.

REFERENSI

[1] M. R. Habibi and I. Liviani, “Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia,” *Al-Qanun J. Pemikir. dan*

Pembaharuan Huk. Islam, vol. 23, no. 2, pp. 400–426, 2020, doi: 10.15642/alqanun.2020.23.2.400-426.

[2] Y. I. Kurniawan, A. Rahmawati, N. Chasanah, and A. Hanifa, "Application for determining the modality preference of student learning," *J. Phys. Conf. Ser.*, vol. 1367, no. 1, 2019, doi:
10.1088/1742-6596/1367/1/012011.

[3] M. Idris, S. Aprita, and M. Nurlani, "PENGATURAN DAN PENEGAKAN HUKUM KEJAHATAN DUNIA MAYA (CYEBER CRIME) : HARMONISASI REVISI
UNDANG-UNDANG ITE DAN KUHP LATAR BELAKANG Globalisasi dan segala perkembangannya menawarkan janji-janji yang sangat menarik manusia . 396–411, doi: 10.28946/lexl.v6i3.4266.

[4] M. Djarawula, N. Alfiani, and H. Mayasari, "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *J. Cakrawala Ilm.*, vol. 2, no. 10, pp. 3799–3806, 2023, [Online]. Available: http://bajangjournal.com/index.php/JCI

[5] A. P. Wardana, "Hukum Pidana dan Perlindungan Data Pribadi: Upaya Menanggulangi Kejahatan Siber di Era Digital di Indonesia," *Pustaka Law J.*, pp. 20–25, 2024, [Online]. Available: https://ojs.pustakapublisher.com/index.php/plj/article/view/18%0Ahttps://ojs.pustakapubli sher.com/index.php/plj/article/download/18/21

[6] M. Apandi, K. Rahayu, W. Agus Prayugo, and L. Ariany, "Kekaburan Norma dalam Kebebasan Berekspresi di Era Digital: Analisis Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik," *J. Huk. Lex Gen.*, vol. 5, no. 12, 2025, doi: 10.56370/jhlg.v5i12.1007.

[7] D. Anjheli, "Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023," *Staatsr. J. Huk. Kenegaraan dan Polit. Islam*, vol. 4, no. 1, pp. 165–189, 2025, [Online]. Available: https://ejournal.uin-suka.ac.id/syariah/Staatsrecht/article/view/3964

[8] R. S. Silalahi, "Analisis Hukum Tindak Pidana Cyber Data Breach Di Era Digital Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik (Studi Putusan Nomor 2447/Pid.Sus/2024/Pn Mdn)," vol. 4, no. 9, pp. 2425–2440, 2025.

[9] Z. J. Fernando *et al.*, "KONSTITUSIONALISME DIGITAL DI INDONESIA : PEMBATASAN KEKUASAAN NEGARA DAN PLATFORM DALAM PERLINDUNGAN HAK KONSTITUSIONAL WARGA DI RUANG SIBER".

[10] V. P. Putri, S. F. Rahmawati, and A. Z. Zelda, "Kajian Terhadap Penggunaan Internet Terkait Etika Bersosial Media Dengan Melihat Hukum Di Indonesia Dalam Melindungi Masyarakatnya," *Das Soll. J. Kaji. Kontemporer Huk. dan Masy.*, vol. 2, no.

1, pp. 1–25, 2023, doi: 10.11111/dassollen.xxxxxxx.

[11] D. Parindo, Y. Daeng, A. S. Atmaja, H. R. Putra, and H. Berson, "Penerapan Konsep Dasar HAM dan Pembaharuan Tiga Pilar Utama Hukum Pidana dalam KUHP Baru UU No. 01 Tahun 2023," *J. Huk. Indones.*, vol. 3, no. 3, pp. 129–142, 2024, doi: 10.58344/jhi.v3i3.796.

[12] Y. Ginanjar, "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara," *J. Din. Glob.*, vol. 7, no. 02, pp. 291–312, 2022, doi: 10.36859/jdg.v7i02.1187.

[13] H. Wildanah and A. Rivai, "Harmonisasi Lex Specialis UU ITE dan KUHP dalam Penegakan Cybercrime serta Validitas Transaksi Elektronik di Indonesia general provisions in the Criminal Code and specific provisions in the Electronic Information and Transaction Law (EIT Law), in addition to the need for legal certainty regarding the validity of legal actions based on qualitatively and prescriptively . The results of the study show that : (1) the cybercrime enforcement regime in Indonesia places the ITE Law as lex specialis that complements the Criminal Code ; (2) electronic transactions," vol. 4, no. 2, pp. 106–127, 2025.

[14] "Tesis analisis hukum terhadap media sosial dalam pembuktian tindak pidana informasi dan transaksi elektronik," 2023.

[15] A. R. Agma, "Kebijakan Hukum Pidana Dalam Penanggulangan Cybercrime Di Indonesia," *J. Huk. Pidana dan Kriminologi*, vol. 1, no. 1, pp. 22–29, 2025, [Online]. Available: https://ejournal.pustakabangsaindonesia.com/index.php/jhpk

[16] D. J. H. Dame and J. Hukum, ", Wina Erni," vol. 1, no. 1, pp. 1–23, 2025.

[17] H. Djanggih and N. Qamar, "Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *Pandecta Res. Law J.*, vol. 13, no. 1, pp. 10–23, 2018, doi: 10.15294/pandecta.v13i1.14020.

[18] M. A. Gustawinata, L. Abubakar, and E. Rahmawati, "Jurnal Tana Mana," *J. Tana Mana*, vol. 2, no. 1, pp. 46–48, 2021, [Online]. Available: https://ojs.staialfurqan.ac.id/jtm/article/download/736/452/

[19] Satya Muhammad Sutra and Agus Haryanto, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," *Glob. Polit. Stud. J.*, vol. 7, no. 1, pp. 56–69, 2023, doi: 10.34010/gpsjournal.v7i1.

[20] K. Hukum *et al.*, "Aulia Mawaddah Matondang dan Andryan Universitas Muhammadiyah Sumatera Utara," vol. 6, no. 1, pp. 1–14, 2025.

[21] M. Arisanty *et al.*, "Cerdas Dan Aman Bermedia Digital : Peningkatan," *J. Abdimas Patikala*, vol. 4, no. 4, pp. 1407–1418, 2025.

[22] Alaikha Annan, "Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022," *J. Ilm. Multidisiplin*, vol. 1, no. 4, pp. 247–254, 2024, [Online]. Available: https://e-journal.naureendigition.com/index.php/sjim