Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 4, 2026
DOI: https://doi.org/10.61104/alz.v4i3.7300

Analisis Faktor Penyebab Meningkatnya Kejahatan Siber Di Indonesia

Trilestaria Simbolon[1], Suci Ramadani[2], Tri Sandi[3], Zefri Ansari[4]
Magister Ilmu Hukum, Universitas Pembangunan Panca Budi Medan, Indonesia[1-4]
Email Korespondensi: trilestarisimbolon05@gmail.com, suciramadani@dosen.pancabudi.ac.id, sanditri764@gmail.com, zefriansari86@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Maret 2026, Article published: 24 Juni 2026

ABSTRACT
The development of information technology and the internet in Indonesia has provided many benefits to society's daily life. However, it has also created threats in the form of increasing cybercrime. This study aims to identify the factors causing the rise of cybercrime in Indonesia and the government's efforts to overcome it. The method used is a literature study by reviewing various sources such as books, journals, and laws related to cybercrime. The discussion results show that the increase in cybercrime is influenced by the development of digital technology, low levels of digital literacy among the public, weak cybersecurity systems, and the economic motives of perpetrators. Common forms of cybercrime include online fraud, account hacking, personal data theft, and malware distribution. In addressing cybercrime, the government has undertaken various measures through the establishment of regulations such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law, strengthening the National Cyber and Crypto Agency (BSSN), law enforcement, improving digital literacy, and enhancing international cooperation. Therefore, cooperation between the government and society is needed to create better digital security in Indonesia.
Keywords: *Cybercrime, Cybersecurity, Digital Literacy, Personal Data Protection.*

ABSTRAK
Perkembangan teknologi informasi dan internet di Indonesia memberikan banyak manfaat dalam kehidupan masyarakat, namun juga menimbulkan ancaman berupa meningkatnya kejahatan siber (cyber crime). Penelitian ini bertujuan untuk mengetahui faktor penyebab meningkatnya kejahatan siber di Indonesia serta upaya pemerintah dalam menanggulanginya. Metode yang digunakan adalah studi kepustakaan dengan mengkaji berbagai sumber seperti buku, jurnal, dan peraturan perundang-undangan yang berkaitan dengan cyber crime. Hasil pembahasan menunjukkan bahwa meningkatnya kejahatan siber dipengaruhi oleh perkembangan teknologi digital, rendahnya literasi digital masyarakat, lemahnya sistem keamanan siber, serta motif ekonomi pelaku. Bentuk kejahatan siber yang sering terjadi meliputi penipuan online, peretasan akun, pencurian data pribadi, dan penyebaran malware. Dalam menanggulangi cyber crime, pemerintah melakukan berbagai upaya melalui pembentukan regulasi seperti UU ITE dan UU Perlindungan Data Pribadi, penguatan Badan Siber dan Sandi Negara (BSSN), penegakan hukum, peningkatan literasi digital, serta kerja sama internasional. Dengan demikian, diperlukan kerja sama antara pemerintah dan masyarakat untuk menciptakan keamanan digital yang lebih baik di Indonesia.
Kata Kunci: *Cyber Crime, Keamanan Siber, Literasi Digital, Perlindungan Data Pribadi.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa perubahan besar dalam kehidupan masyarakat Indonesia. Penggunaan internet yang semakin luas memberikan kemudahan dalam berbagai aktivitas, seperti komunikasi, pendidikan, perdagangan, hingga pelayanan publik. Namun, di balik kemajuan tersebut muncul ancaman baru berupa kejahatan siber (cyber crime). Kejahatan siber merupakan tindak kriminal yang memanfaatkan teknologi komputer, jaringan internet, maupun sistem elektronik sebagai sarana utama untuk melakukan tindakan melawan hukum (Hasri et al., 2025). Bentuk kejahatan ini meliputi peretasan, pencurian data pribadi, penipuan daring, penyebaran malware, hingga penyalahgunaan media sosial. Meningkatnya penggunaan internet di Indonesia turut berpengaruh terhadap meningkatnya angka kejahatan siber yang merugikan masyarakat maupun negara.

Kejahatan siber di Indonesia mengalami peningkatan karena berbagai faktor, salah satunya adalah rendahnya kesadaran masyarakat terhadap keamanan digital. Banyak pengguna internet yang masih kurang memahami pentingnya perlindungan data pribadi, penggunaan kata sandi yang aman, serta bahaya tautan atau aplikasi mencurigakan. Selain itu, kemajuan teknologi yang begitu cepat sering kali tidak diimbangi dengan kemampuan keamanan siber yang memadai. Perkembangan teknologi tanpa pengawasan dan rendahnya literasi digital menjadi faktor utama munculnya cyber crime di masyarakat (Laksana & Mulyani, 2023). Salah satu kejahatan siber yang paling sering terjadi adalah penipuan daring. Kasus penipuan online terus meningkat setiap tahun, bahkan hampir selalu memakan korban setiap minggunya,dimana tingkat penyelesaian kasus tersebut masih tergolong rendah (Laia et al., 2025).

Selain faktor rendahnya literasi digital, meningkatnya kejahatan siber juga dipengaruhi oleh motif ekonomi dan kemudahan akses teknologi. Pelaku cyber crime memanfaatkan internet karena dianggap lebih mudah, cepat, serta memiliki risiko tertangkap yang lebih kecil dibandingkan kejahatan konvensional. Sebagian besar pelaku kejahatan siber memiliki motivasi finansial, seperti pencurian data, penipuan daring, dan pembobolan akun digital(Peersman et al., 2022). Di Indonesia sendiri, maraknya penggunaan transaksi digital dan media sosial membuka peluang besar bagi pelaku untuk melakukan phishing, penipuan online, dan pencurian identitas.

Jenis kejahatan siber yang paling banyak ditemukan di Indonesia meliputi berbagai bentuk tindak kriminal berbasis digital, seperti penipuan daring, pembobolan akun media sosial, pencurian dan penyalahgunaan data pribadi, penyebaran informasi palsu atau hoaks, hingga serangan malware yang dapat merusak sistem perangkat pengguna. Salah satu bentuk kejahatan yang cukup marak terjadi adalah peretasan akun WhatsApp dengan memanfaatkan kode one time password (OTP) maupun fitur two factor authentication (2FA). Modus ini biasanya dilakukan dengan cara menipu korban agar memberikan kode verifikasi yang bersifat rahasia kepada pelaku. Faktor utama yang menyebabkan akun WhatsApp mudah diretas adalah kurangnya kewaspadaan pengguna dalam menjaga kerahasiaan kode verifikasi dan informasi pribadi mereka (Flora, 2025).

Banyak pengguna yang tanpa sadar memberikan kode OTP kepada pihak lain karena terjebak dalam berbagai bentuk rekayasa sosial atau social engineering. Selain itu, maraknya kebocoran data pribadi di masyarakat juga semakin memperbesar peluang terjadinya penyalahgunaan identitas.

Meningkatnya cyber crime di Indonesia menunjukkan bahwa keamanan siber masih menjadi tantangan besar bagi pemerintah dan masyarakat. Oleh karena itu, pemerintah Indonesia telah menetapkan berbagai regulasi untuk mengatur penggunaan teknologi informasi dan menindak pelaku kejahatan siber. Dasar hukum utama terkait cyber crime adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. UU ITE mengatur berbagai bentuk tindak pidana elektronik seperti akses ilegal, penyebaran informasi terlarang, manipulasi data elektronik, serta penipuan berbasis digital (Hasri et al., 2025). Selain itu, pemerintah juga mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) sebagai upaya memperkuat perlindungan data masyarakat di era digital.

Dalam upaya penanggulangan cyber crime, pemerintah melalui Badan Siber dan Sandi Negara (BSSN) terus meningkatkan sistem keamanan siber nasional melalui pengawasan, edukasi digital, dan kerja sama lintas lembaga. Pemerintah juga bekerja sama dengan Kepolisian Negara Republik Indonesia untuk melakukan penegakan hukum terhadap pelaku kejahatan siber. Selain penindakan hukum, langkah preventif seperti sosialisasi keamanan digital dan peningkatan literasi teknologi juga terus dilakukan untuk mengurangi risiko kejahatan siber di masyarakat.

Berdasarkan uraian tersebut, dapat dipahami bahwa meningkatnya kejahatan siber di Indonesia dipengaruhi oleh perkembangan teknologi, rendahnya kesadaran masyarakat terhadap keamanan digital, serta lemahnya perlindungan data pribadi. Cyber crime menjadi ancaman serius karena dapat merugikan individu, perusahaan, bahkan negara. Oleh sebab itu, diperlukan kerja sama antara pemerintah, aparat penegak hukum, dan masyarakat dalam meningkatkan keamanan siber agar tercipta ruang digital yang aman dan bertanggung jawab. Dengan demikian, penelitian mengenai faktor penyebab meningkatnya kejahatan siber di Indonesia menjadi penting untuk dikaji guna menemukan solusi yang efektif dalam menanggulangi cyber crime di masa mendatang.

METODE

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kualitatif dengan pendekatan studi kepustakaan (library research). Penelitian dilakukan dengan mengumpulkan berbagai data dan informasi dari sumber tertulis seperti buku, jurnal ilmiah, artikel, peraturan perundang-undangan, serta dokumen resmi yang berkaitan dengan kejahatan siber (cyber crime) di Indonesia. Pendekatan ini digunakan untuk memahami faktor-faktor penyebab meningkatnya kejahatan siber serta upaya pemerintah dalam menanggulanginya. Teknik pengumpulan data dilakukan melalui proses membaca, mencatat, dan menganalisis berbagai referensi yang relevan dengan topik penelitian. Data yang diperoleh kemudian dianalisis secara deskriptif untuk menjelaskan hubungan antara

perkembangan teknologi digital, rendahnya literasi digital masyarakat, lemahnya keamanan siber, dan penegakan hukum terhadap meningkatnya cyber crime. Melalui metode ini diharapkan diperoleh pemahaman yang lebih jelas mengenai kondisi kejahatan siber di Indonesia serta solusi yang dapat dilakukan untuk mengurangi risiko cyber crime di masyarakat.

HASIL DAN PEMBAHASAN

Faktor Penyebab Meningkatnya Kejahatan Siber

Perkembangan teknologi informasi dan internet di Indonesia menjadi salah satu faktor utama meningkatnya kejahatan siber (cyber crime). Kemudahan akses internet memungkinkan masyarakat melakukan berbagai aktivitas secara daring, seperti transaksi keuangan, komunikasi, dan pertukaran data. Namun, perkembangan tersebut juga dimanfaatkan oleh pelaku kejahatan untuk melakukan tindakan ilegal seperti peretasan, pencurian data, dan penipuan online. Perkembangan teknologi informasi tidak saja memberikan manfaat tetapi juga tidak luput dari dampak negatif (Pane & Situmeang, 2021). Meningkatnya penggunaan internet tanpa pengawasan keamanan yang memadai menyebabkan cyber crime semakin mudah terjadi.

Faktor berikutnya adalah rendahnya literasi digital masyarakat Indonesia. Banyak pengguna internet yang belum memahami pentingnya menjaga keamanan data pribadi, penggunaan kata sandi yang kuat, serta bahaya tautan mencurigakan. Kondisi ini membuat masyarakat mudah menjadi korban phishing, penipuan online, maupun pencurian identitas digital. Terdapat kekurangan yang signifikan dalam pemahaman konsep keamanan siber seperti phishing, malware, dan privasi data (Dananjoyo, 2024). Rendahnya kesadaran masyarakat terhadap keamanan digital menjadi faktor utama meningkatnya cyber crime. Selain itu, kurangnya edukasi mengenai etika dan keamanan digital memperbesar peluang penyalahgunaan teknologi oleh pihak yang tidak bertanggung jawab.

Kemajuan teknologi yang sangat cepat juga menjadi penyebab meningkatnya kejahatan siber di Indonesia. Perkembangan teknologi seperti cloud computing, Internet of Things (IoT), dan kecerdasan buatan memberikan peluang baru bagi pelaku kejahatan untuk menyerang sistem keamanan digital. Kejahatan dunia maya muncul seiring dengan perkembangan teknologi informasi yang begitu cepat (Alfian, 2017). Meningkatnya penggunaan perangkat digital dan jaringan pintar memperbesar risiko serangan siber apabila tidak diimbangi dengan sistem keamanan yang kuat. Pelaku cyber crime memanfaatkan kelemahan sistem teknologi untuk mencuri data, menyebarkan malware, dan melakukan sabotase digital.

Selain faktor teknologi, motif ekonomi juga menjadi penyebab utama meningkatnya kejahatan siber. Banyak pelaku melakukan cyber crime karena ingin memperoleh keuntungan finansial secara cepat dan mudah. Bentuk kejahatan yang sering dilakukan antara lain penipuan daring, pembobolan rekening bank, pencurian data kartu kredit, hingga ransomware. Digitalisasi sektor keuangan meningkatkan risiko phishing dan pencurian data nasabah (Wahyningtias, 2026).

Hal ini menunjukkan bahwa perkembangan ekonomi digital tanpa perlindungan keamanan yang baik dapat meningkatkan peluang terjadinya cyber crime.

Faktor lemahnya sistem keamanan siber nasional juga turut menyebabkan meningkatnya kejahatan siber di Indonesia. Banyak lembaga maupun perusahaan yang belum memiliki perlindungan data yang optimal sehingga rentan terhadap serangan hacker. Kebocoran data pribadi yang sering terjadi menunjukkan bahwa keamanan digital di Indonesia masih memiliki banyak kelemahan. Lemahnya sistem keamanan digital nasional dan keterbatasan kapasitas penegak hukum menjadi hambatan dalam pencegahan cyber crime (Dzaky & Edrisy, 2025). Oleh karena itu, diperlukan peningkatan sistem keamanan digital serta penguatan sumber daya manusia di bidang keamanan siber.

Meningkatnya kejahatan siber juga dipengaruhi oleh lemahnya penegakan hukum terhadap pelaku cyber crime. Walaupun Indonesia telah memiliki regulasi mengenai kejahatan siber, implementasi hukum sering menghadapi berbagai kendala seperti keterbatasan teknologi investigasi, kurangnya tenaga ahli digital forensik, dan sulitnya melacak pelaku lintas negara. Dasar hukum utama dalam penanganan cyber crime di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. Selain itu, terdapat Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang bertujuan melindungi data masyarakat dari penyalahgunaan digital. Namun, penerapan hukum tersebut masih memerlukan penguatan agar mampu mengikuti perkembangan modus cyber crime yang semakin kompleks.

Perkembangan masyarakat modern dan teknologi dapat melahirkan bentuk kriminalitas baru yang sulit dikendalikan apabila tidak diimbangi dengan pengawasan sosial yang baik. Faktor ekonomi, lingkungan sosial, dan perkembangan teknologi menjadi penyebab meningkatnya tindak kriminalitas dalam masyarakat modern. Pendapat tersebut relevan dengan kondisi cyber crime di Indonesia saat ini, di mana perkembangan teknologi digital yang pesat membuka peluang munculnya berbagai bentuk kejahatan baru di ruang siber. Dengan demikian, peningkatan cyber crime di Indonesia dipengaruhi oleh faktor teknologi, rendahnya literasi digital, motif ekonomi, lemahnya keamanan siber, dan kurang optimalnya penegakan hukum sehingga diperlukan kerja sama antara pemerintah dan masyarakat dalam meningkatkan keamanan digital nasional.

Upaya Pemerintah Dalam Menanggulangi Cyber Crime

Upaya pemerintah Indonesia dalam menanggulangi cyber crime dilakukan melalui pembentukan regulasi hukum yang mengatur penggunaan teknologi informasi dan transaksi elektronik. Pemerintah menyadari bahwa perkembangan teknologi digital membawa dampak positif sekaligus ancaman berupa meningkatnya kejahatan siber seperti peretasan, pencurian data, penipuan online, dan penyebaran malware. Oleh karena itu, pemerintah menetapkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. UU ITE menjadi dasar hukum utama dalam mengatur tindak pidana siber di Indonesia,

khususnya pada Pasal 27 sampai Pasal 37 mengenai perbuatan yang dilarang dalam ruang digital. UU ITE memberikan landasan hukum bagi aparat penegak hukum untuk menindak pelaku kejahatan siber dengan ancaman pidana penjara dan denda (Popal, 2023).

Selain melalui regulasi, pemerintah juga membentuk lembaga khusus yang menangani keamanan siber nasional, yaitu Badan Siber dan Sandi Negara. Lembaga ini dibentuk untuk meningkatkan perlindungan terhadap sistem elektronik nasional serta mencegah ancaman serangan siber. BSSN memiliki tugas melakukan deteksi, pencegahan, pemulihan, dan pengamanan sistem digital pemerintah maupun masyarakat. BSSN menggunakan strategi peningkatan kapasitas keamanan siber berdasarkan lima aspek, yaitu penguatan hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama internasional (Haryanto & Sutra, 2023). Pemerintah berharap keberadaan BSSN dapat memperkuat pertahanan siber nasional serta meningkatkan kesiapsiagaan menghadapi ancaman digital yang semakin kompleks.

Pemerintah juga melakukan penegakan hukum terhadap pelaku cyber crime melalui kerja sama antara kepolisian, kejaksaan, dan pengadilan. Kepolisian Republik Indonesia membentuk unit khusus cyber crime untuk menangani kasus kejahatan siber seperti penipuan online, penyebaran hoaks, dan peretasan data. Mabes Polri membentuk Cyber Troops atau pasukan dunia maya untuk melacak pelaku kejahatan siber serta mengawasi aktivitas digital yang berpotensi mengganggu keamanan masyarakat (Pratama, 2021). Langkah ini menunjukkan bahwa pemerintah berupaya meningkatkan pengawasan ruang digital agar lebih aman dan tertib.

Selain penegakan hukum, pemerintah melakukan upaya preventif melalui peningkatan literasi digital masyarakat. Edukasi mengenai keamanan digital dianggap penting karena banyak kasus cyber crime terjadi akibat rendahnya kesadaran masyarakat dalam melindungi data pribadi. Pemerintah melalui Kementerian Komunikasi dan Informatika secara rutin mengadakan program literasi digital untuk memberikan pemahaman mengenai penggunaan internet yang aman dan bijak. Keberhasilan penanggulangan cyber crime tidak hanya bergantung pada hukum, tetapi juga pada kesadaran masyarakat terhadap keamanan teknologi informasi (Sefitrios & Chandra, 2021). Oleh sebab itu, edukasi digital menjadi salah satu langkah penting untuk mencegah meningkatnya korban kejahatan siber.

Pemerintah juga memperkuat perlindungan data pribadi melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini bertujuan melindungi hak masyarakat atas keamanan data pribadi dari penyalahgunaan digital. Kebocoran data yang sering terjadi di Indonesia menjadi alasan penting lahirnya regulasi tersebut. Perlindungan data pribadi merupakan langkah penting dalam mengurangi risiko pencurian identitas dan penyalahgunaan informasi elektronik. Dengan adanya UU PDP, pemerintah memiliki dasar hukum yang lebih kuat untuk menindak pelaku penyalahgunaan data digital.

Upaya lain yang dilakukan pemerintah adalah meningkatkan kerja sama internasional dalam penanggulangan cyber crime. Kejahatan siber sering kali bersifat lintas negara sehingga membutuhkan koordinasi antarnegara dalam proses

penyelidikan dan penegakan hukum. Pemerintah Indonesia bekerja sama dengan berbagai organisasi internasional untuk memperkuat sistem keamanan siber nasional dan berbagi informasi mengenai ancaman digital global. Perkembangan cyber crime yang semakin kompleks memerlukan harmonisasi hukum dan kerja sama internasional agar penanganan kejahatan siber dapat berjalan efektif (Widijowati, 2022). Kerja sama ini penting karena pelaku cyber crime sering menggunakan jaringan internasional untuk menyembunyikan identitas dan lokasi mereka.

Perkembangan teknologi modern dapat memunculkan bentuk kriminalitas baru yang membutuhkan pengawasan sosial dan hukum yang lebih kuat. Kriminalitas berkembang seiring perubahan sosial dan kemajuan teknologi masyarakat. Pendapat tersebut menunjukkan bahwa pemerintah perlu terus menyesuaikan kebijakan dan sistem keamanan digital dengan perkembangan teknologi informasi. Dengan demikian, upaya pemerintah dalam menanggulangi cyber crime dilakukan melalui pembentukan regulasi hukum, penguatan lembaga keamanan siber, penegakan hukum, peningkatan literasi digital, perlindungan data pribadi, dan kerja sama internasional agar tercipta keamanan digital yang lebih baik di Indonesia.

SIMPULAN

Kesimpulan berdasarkan pembahasan di atas, dapat disimpulkan bahwa meningkatnya kejahatan siber di Indonesia disebabkan oleh perkembangan teknologi informasi yang sangat pesat, rendahnya literasi digital masyarakat, lemahnya sistem keamanan siber, serta motif ekonomi pelaku kejahatan. Kemudahan akses internet dan penggunaan transaksi digital membuka peluang terjadinya penipuan online, peretasan akun, pencurian data pribadi, hingga penyebaran malware. Kurangnya kesadaran masyarakat dalam menjaga keamanan data pribadi juga menjadi faktor utama meningkatnya cyber crime di Indonesia. Oleh karena itu, diperlukan peningkatan edukasi dan kesadaran masyarakat mengenai keamanan digital agar risiko kejahatan siber dapat diminimalkan. Selain itu, pemerintah telah melakukan berbagai upaya untuk menanggulangi cyber crime melalui pembentukan regulasi seperti UU ITE dan UU Perlindungan Data Pribadi, penguatan Badan Siber dan Sandi Negara (BSSN), serta penegakan hukum oleh kepolisian. Pemerintah juga meningkatkan literasi digital masyarakat dan menjalin kerja sama internasional untuk menghadapi ancaman siber lintas negara sehingga tercipta ruang digital yang aman dan bertanggung jawab.

DAFTAR RUJUKAN

Alfian, M. (2017). Penguatan Hukum Cyber Crime di Indonesia dalam Perspektif Peraturan Perundang-undangan. *Kosmik Hukum*, *17*(2). https://doi.org/10.30595/kosmikhukum.v17i2.2331

Dananjoyo, S. W. (2024). Literasi Digital Di Kalangan Masyarakat Pedesaan: Upaya Meningkatkan Kesadaran Keamanan Siber. *Jurnal Edutein*, *2*(1), 1–9.

Dzaky, M. A. T., & Edrisy, I. F. (2025). Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital.

PESHUM:JurnalPendidikan,SosialdanHumaniora, *4*(2), 3614–3625. https://doi.org/https://doi.org/10.56799/peshum.v4i2.8311

Flora, H. S. (2025). Faktor Penyebab Dan Penanggulangan Terjadinya Peretasan Whatsapp. *Jurnal Profil Hukum*, *3*(1), 1–11.

Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, *7*(1), 56–69. https://doi.org/https://doi.org/10.34010/gpsjournal.v7i1.8141

Hasri, H., Mashendra, M., Hayun, H., & Nisa, F. N. (2025). Kejahatan Cybercrime Dan Penanggulangannya Dalam Kerangka Sistem Hukum Nasional. *Indonesian Journal of Legality of Law*, *7*(2), 281–287. https://doi.org/https://doi.org/10.35965/ijlf.v7i2.6240

Laia, Y. R. N., Rahmayanti, R., Tampubolon, S. S., Gea, A. S., & Nasution, S. H. (2025). Implementasi Hukum terhadap Tindak Pidana Scammer. *JISPENDIORA :Jurnal Ilmu Sosial, Pendidikan Dan Humaniora*, *4*(1), 603–613. https://doi.org/https://doi.org/10.56910/jispendiora.v4i1.2504

Laksana, T. G., & Mulyani, S. (2023). Faktor – Faktor Mendasar Kejahatan Siber Terhadap Kemanusiaan. *Jurnal Hukum Prioris*, *11*(2), 136–160. https://doi.org/https://doi.org/10.25105/prio.v11i2.18960

Pane, M. D., & Situmeang, S. M. tua. (2021). Penegakan Hukum Cyber Crime Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi. *Journal of Community Services in Humanities and Social Sciences*, *2*(3), 93–105. https://doi.org/https://doi.org/10.32493/JLS.v3i2.p93-105

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). *Understanding motivations and characteristics of financially-motivated cybercriminals*. ArXiv. https://arxiv.org/abs/2203.08642

Popal, D. F. T. (2023). Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime). *Lex Administratum*, *11*(5).

Pratama, K. S. (2021). Upaya Pemerintah Dalam Menanggulangi Tindak Pidana Informasi Elektronik Yang Mengganggu Ketertiban Umum. *Lex Crimen*, *10*(4), 91–101.

Sefitrios, S., & Chandra, T. Y. (2021). The Process and Performance of Combating Cyber Crimes In Indonesia. *Jurnal Sosial Dan Budaya Syar-I*, *8*(8). https://doi.org/https://doi.org/10.15408/sjsbs.v8i4.21795

Wahyningtias, N. (2026). Analisis Normatif Perlindungan Hukum Terhadap Korban Kejahatan Siber Dalam Modus Phishing Rekening Bank Di Indonesia. *Judge: Jurnal Hukum*, *6*(6), 1972–1983. https://doi.org/https://doi.org/10.54209/judge.v6i06.1564

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, *2*(6), 597–606. https://doi.org/https://doi.org/10.54518/rh.2.6.2022.98

