HARISA: Jurnal Hukum, Syariah, dan Sosial, 02 (1), 2025: 67-80
ISSN: XXXX-XXXX, E-ISSN: XXXX-XXXX
DOI:

Kajian Kritis Efektivitas Sanksi Pidana dalam Kejahatan Siber Menurut Hukum Positif

Andri Ebenezer Nainggolan
Prodi Ilmu Hukum Universitas Terbuka, Indonesia.
E-mail:Ebenezer.ee32@gmail.com
*corresponding author

Abstract

Cybercrime is a global phenomenon that continues to evolve alongside technological advancements, yet the effectiveness of criminal sanctions in addressing it remains debatable. This study aims to critically examine the effectiveness of criminal sanctions in deterring cybercrime from the perspective of positive law, particularly in Indonesia. The research employs a normative juridical approach, analyzing legislation, court decisions, and relevant literature. The findings reveal that although Indonesian positive law, such as the ITE Law and the Criminal Code (KUHP), provides criminal sanctions for cybercrime, their implementation faces challenges, including unclear definitions, evidentiary difficulties, and low enforcement rates. Furthermore, the existing sanctions are deemed insufficient in creating a deterrent effect for perpetrators. This study recommends policy reforms, including regulatory updates, enhanced law enforcement capacity, and restorative justice approaches to complement conventional criminal sanctions. The findings contribute to academic discourse on cyber criminal law and provide insights for policymakers.
Keywords: *Criminal sanctions; cybercrime; positive law; effectiveness; ITE Law.*

Abstrak

Kejahatan siber (cybercrime) merupakan fenomena global yang terus berkembang seiring kemajuan teknologi, sementara efektivitas sanksi pidana dalam menanggulanginya masih menjadi perdebatan. Penelitian ini bertujuan untuk mengkaji secara kritis efektivitas sanksi pidana dalam menekan kejahatan

siber berdasarkan perspektif hukum positif, khususnya di Indonesia. Metode penelitian menggunakan pendekatan yuridis normatif dengan analisis terhadap peraturan perundang-undangan, putusan pengadilan, serta literatur terkait. Hasil penelitian menunjukkan bahwa meskipun hukum positif Indonesia, seperti UU ITE dan KUHP, telah mengatur sanksi pidana untuk kejahatan siber, implementasinya masih menghadapi tantangan seperti ketidakjelasan definisi, kesulitan pembuktian, dan rendahnya tingkat penindakan. Selain itu, sanksi yang ada dinilai belum sepenuhnya memiliki efek jera (deterrent effect) bagi pelaku. Studi ini merekomendasikan perlunya reformasi kebijakan yang mencakup pembaruan regulasi, peningkatan kapasitas penegak hukum, dan pendekatan restoratif untuk melengkapi sanksi pidana konvensional. Temuan ini memberikan kontribusi akademis dalam diskursus hukum pidana siber serta menjadi bahan evaluasi bagi pembuat kebijakan.

Kata Kunci: Sanksi Pidana; Kejahatan Siber; Hukum Positif; Efektivitas; UU ITE.

Pendahuluan

Perkembangan teknologi digital yang pesat telah melahirkan bentuk-bentuk kejahatan baru di ruang siber *(cybercrime)*(Mahira Dewantoro & Dian Alan Setiawan S.H., M.H., 2023). Kejahatan ini tidak lagi mengenal batas wilayah dan telah menjadi ancaman serius bagi keamanan global. Menurut data INTERPOL (2023), terjadi peningkatan lebih dari 300% kasus kejahatan siber dalam dekade terakhir, dengan kerugian ekonomi mencapai triliunan dolar AS(Muhammad et al., 2024). Fenomena ini menunjukkan bahwa kejahatan siber telah berkembang menjadi masalah sistemik yang membutuhkan penanganan serius dari perspektif hukum pidana(Madinah Mokobombang et al., 2023).

Di Indonesia, kejahatan siber mengalami pertumbuhan yang mengkhawatirkan. Laporan BSSN (2023) mencatat lebih dari 1,2 miliar serangan siber sepanjang tahun 2022, dengan dominasi kasus penipuan digital, kebocoran data, dan penyebaran konten ilegal. Kondisi ini mempertanyakan efektivitas kerangka hukum yang ada,

terutama UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, dalam menanggulangi masalah ini(Awaluddin et al., 2024; Putri, 2022).

Hukum positif Indonesia menghadapi beberapa tantangan mendasar dalam mengatur kejahatan siber. Pertama, ketidaksesuaian antara karakteristik kejahatan siber yang dinamis dengan sifat rigid dari peraturan perundang-undangan. Kedua, adanya dualisme pengaturan antara KUHP sebagai hukum pidana umum dan UU ITE sebagai hukum khusus. Ketiga, perbedaan interpretasi yuridis terhadap berbagai bentuk kejahatan siber yang terus berkembang(Najwa, 2024; Nicodemus, 2023).

Persoalan utama terletak pada efektivitas sanksi pidana yang diatur dalam hukum positif. Beberapa penelitian terdahulu (Hadisuprapto, 2021; Santoso, 2022) menunjukkan bahwa sanksi pidana konvensional seperti penjara dan denda belum memberikan efek jera yang optimal. Pelaku kejahatan siber cenderung menganggap risiko hukum sebagai cost of business yang dapat dikalkulasi, bukan sebagai deterrent yang efektif(Sari et al., 2024).

Implementasi sanksi pidana untuk kejahatan siber menghadapi kendala operasional yang kompleks. Mulai dari kesulitan dalam proses penyidikan akibat keterbatasan teknologi dan SDM aparat penegak hukum, hingga masalah pembuktian elektronik yang membutuhkan keahlian khusus. Selain itu, kerjasama internasional yang masih lemah dalam penanganan kejahatan siber lintas negara turut memperparah kondisi ini(Sihombing et al., 2023).

Penelitian ini memiliki urgensi akademis dan praktis. Secara akademis, studi ini mengisi celah literatur mengenai evaluasi kritis terhadap efektivitas sanksi pidana dalam konteks kejahatan siber. Secara praktis, temuan penelitian dapat menjadi bahan pertimbangan bagi pembuat kebijakan dalam melakukan reformasi hukum pidana siber di Indonesia.

Berdasarkan latar belakang tersebut, penelitian ini akan menjawab pertanyaan: (1) Bagaimana efektivitas sanksi pidana dalam UU ITE dan KUHP dalam menanggulangi kejahatan siber? (2) Apa faktor-faktor yang menghambat efektivitas sanksi pidana tersebut? (3) Bagaimana model ideal sanksi pidana untuk kejahatan siber dalam sistem hukum positif Indonesia?

Metode

Penelitian ini menggunakan pendekatan yuridis normatif dengan metode analisis deskriptif-analitis terhadap bahan hukum primer meliputi UU ITE, KUHP, dan putusan pengadilan terkait kejahatan siber, serta bahan hukum sekunder berupa literatur hukum pidana siber, jurnal internasional, dan dokumen kebijakan. Teknik pengumpulan data dilakukan melalui studi dokumen dan analisis putusan pengadilan, kemudian dianalisis secara kualitatif melalui content analysis untuk mengidentifikasi efektivitas sanksi pidana. Validasi data dilakukan melalui triangulasi sumber dengan membandingkan temuan dari berbagai dokumen hukum dan literatur terkait.

Hasil dan Pembahasan

Efektivitas Sanksi Pidana dalam UU ITE dan KUHP dalam Menanggulangi Kejahatan Siber

UU ITE dan KUHP merupakan dasar hukum utama dalam penanganan kejahatan siber di Indonesia. UU ITE secara khusus mengatur delik-delik siber, sementara KUHP menjadi payung umum hukum pidana. Namun, keduanya belum sepenuhnya mampu mengikuti dinamika kejahatan siber yang terus berkembang(Rahmawati, 2017).

UU ITE mengenakan sanksi pidana penjara maksimal 12 tahun dan denda hingga Rp12 miliar untuk berbagai tindak pidana siber, seperti penyebaran konten ilegal, akses tanpa izin, atau pemalsuan data elektronik. Meski demikian, sanksi ini seringkali tidak proporsional dengan dampak kejahatan yang ditimbulkan. KUHP mengatur sanksi pidana umum seperti penjara dan denda yang dapat diterapkan untuk kejahatan siber melalui analogi. Namun, ketiadaan definisi eksplisit tentang kejahatan siber dalam KUHP menimbulkan ketidakpastian hukum dalam penegakannya(Faridi, 2019; Setiawan, 2019).

Data menunjukkan bahwa sanksi pidana dalam UU ITE dan KUHP belum sepenuhnya menimbulkan efek jera. Pelaku kejahatan siber seringkali mengulangi tindakannya karena menganggap sanksi yang diberikan tidak sebanding dengan keuntungan yang diperoleh.

Proses pembuktian kejahatan siber memerlukan keahlian teknis yang tinggi. Banyak kasus gagal diadili karena kurangnya alat bukti elektronik yang sah atau ketidaksiapan aparat penegak hukum dalam menghadapi kompleksitas teknologi(Meha Middlyne Simbolon et al., 2021).

Penegakan hukum terhadap kejahatan siber cenderung tidak merata. Beberapa kasus besar mendapatkan perhatian media dan penanganan serius, sementara banyak kasus serupa justru diabaikan karena keterbatasan sumber daya. Perkembangan kejahatan siber seperti deepfake, cryptojacking, atau serangan ransomware belum sepenuhnya terakomodasi dalam UU ITE dan KUHP. Hal ini menciptakan celah hukum yang dimanfaatkan pelaku kejahatan(Muhammad, 2022).

Laporan BSSN (2023) menunjukkan bahwa hanya sekitar 15% laporan kejahatan siber yang berhasil diselesaikan melalui proses hukum. Sebagian besar kasus terbengkalai karena kesulitan teknis dan administratif. Terdapat ketimpangan dalam penerapan sanksi, di mana pelaku individu seringkali dihukum lebih berat dibandingkan korporasi yang melakukan kejahatan serupa. Hal ini menunjukkan inkonsistensi dalam penegakan hukum(Syah, 2023).

Sanksi pidana konvensional seperti penjara dinilai kurang efektif untuk kejahatan siber. Diperlukan sanksi alternatif seperti pemblokiran akses, pemulihan nama baik, atau kerja sosial di bidang teknologi untuk meningkatkan efek preventif. Beberapa negara seperti Singapura dan Amerika Serikat telah mengadopsi sistem sanksi yang lebih progresif, termasuk denda tinggi dan kewajiban pelatihan siber bagi pelaku. Model semacam ini patut dipertimbangkan untuk diterapkan di Indonesia(Davis Mahardika, 2020).

Reformasi hukum pidana siber harus mencakup pembaruan definisi kejahatan, penyederhanaan proses pembuktian, dan peningkatan kapasitas aparat. Tanpa perubahan struktural, efektivitas sanksi pidana akan tetap rendah. Sanksi pidana dalam UU ITE dan KUHP belum optimal dalam menanggulangi kejahatan siber. Diperlukan pendekatan holistik yang menggabungkan pembaruan regulasi, peningkatan kapasitas penegak hukum, dan penerapan sanksi yang lebih inovatif untuk menciptakan efek jera yang lebih besar.

Analisis Mendalam Faktor Penghambat Efektivitas Sanksi Pidana untuk Kejahatan Siber

Sistem hukum Indonesia menghadapi tantangan kompleks dalam menciptakan sanksi pidana yang efektif untuk kejahatan siber, yang bersumber dari akar masalah multidimensional. Fundamentalnya, kerangka hukum yang ada dibangun atas konsep kejahatan konvensional sehingga gagal mengakomodasi karakteristik unik kejahatan digital yang bersifat borderless, cepat berkembang, dan sangat teknis. UU ITE sebagai payung hukum utama justru mengandung pasal-pasal multitafsir yang dalam praktiknya lebih sering digunakan untuk kriminalisasi aktivitas digital biasa daripada memerangi kejahatan siber yang sesungguhnya(DM et al., 2022).

Problem mendasar terletak pada epistemologi hukum yang masih memandang kejahatan siber melalui lensa tradisional. Pendekatan legal-formalistik dalam KUHP dan UU ITE tidak menyediakan instrumen memadai untuk menjangkau dimensi virtual yang menjadi ruang operasi kejahatan siber. Ketiadaan definisi operasional tentang aspek-aspek krusial seperti otentikasi elektronik, jejak digital, atau sistem elektronik dalam undang-undang menciptakan ambiguitas yuridis yang dimanfaatkan pelaku untuk menghindari jeratan hukum(Bhakti, 2025).

Dari sisi penegakan hukum, terjadi diskoneksi antara kebutuhan investigasi digital dengan kapasitas institusi penegak hukum. Proses penyidikan kasus siber seringkali terhambat oleh ketiadaan standard operating procedure yang komprehensif untuk pengumpulan dan preservasi bukti digital, sementara mekanisme mutual legal assistance untuk kasus lintas yurisdiksi berjalan lamban dan birokratis. Padahal, karakter kejahatan siber justru menuntut respons cepat dan koordinasi real-time(M. Syafiih et al., 2024).

Aspek teknis-yuridis pembuktian menjadi bottleneck dalam efektivitas sanksi. Ketentuan tentang alat bukti elektronik dalam UU ITE dan KUHAP belum sepenuhnya mengakomodasi perkembangan teknologi digital mutakhir seperti blockchain, dark web, atau enkripsi canggih. Hakim yang kurang melek teknologi seringkali gagal memahami kompleksitas bukti digital yang diajukan, berujung pada putusan yang tidak mencerminkan beratnya dampak kejahatan siber.

Dinamika kejahatan siber yang evolutif bertolak belakang dengan sifat hukum pidana yang statis. Modus operandi baru seperti AI-enabled cybercrime atau quantum computing attacks sudah muncul sementara pembaruan undang-undang membutuhkan proses legislasi yang panjang. Celah ini dimanfaatkan pelaku untuk mengembangkan varian kejahatan yang belum diatur dalam ketentuan hukum positif yang ada(Ayman & Nurhadiyanto, 2024).

Secara struktural, fragmentasi kewenangan antarlembaga menciptakan inefisiensi penanganan kasus. Kewenangan BSSN, Polri, dan Kominfo yang tumpang tindih dalam penanganan insiden siber sering berujung pada passing the buck atau duplikasi upaya. Sementara itu, ketiadaan special cyber crime court memperparah ketidakkonsistenan penafsiran hukum terhadap kasus-kasus serupa(Saputra, 2024).

Dimensi ekonomi-politik turut mempengaruhi efektivitas sanksi. Korporasi besar pelaku pelanggaran data seringkali lolos dari sanksi maksimal melalui berbagai cara mulai dari lobi hukum hingga penyelesaian di luar pengadilan. Sebaliknya, pelaku individu dengan sumber daya terbatas justru menjadi sasaran empuk penegakan hukum yang tidak proporsional(Kemit et al., 2023).

Pendekatan sanksi yang terlalu mengandalkan hukuman penjara dan denda terbukti tidak efektif untuk konteks kejahatan siber. Sanksi seperti ini gagal menciptakan efek jera karena tidak menyentuh akar masalah seperti motivasi ekonomi pelaku atau kerentanan sistem. Di banyak yurisdiksi, model sanksi restoratif seperti mandatory cybersecurity training atau asset forfeiture justru menunjukkan hasil lebih baik(Agung, 2022).

Budaya hukum masyarakat digital yang masih rendah memperparah situasi. Kesadaran tentang konsekuensi hukum aktivitas digital di kalangan pengguna internet Indonesia masih minim, sementara edukasi literasi digital yang menyertakan aspek hukum belum menjadi prioritas kebijakan. Kondisi ini menciptakan lingkungan yang subur bagi proliferasi kejahatan siber(Ramadha, 2021).

Solusi fundamental menuntut rekonstruksi paradigma hukum pidana siber yang holistik. Tidak cukup dengan revisi pasal per pasal, tetapi perlu membangun sistem hukum yang responsif terhadap perkembangan teknologi, didukung institusi penegak hukum khusus dengan kompetensi tinggi, dan mengintegrasikan pendekatan

multistakeholder dalam pencegahan maupun penindakan. Tanpa perubahan sistemik, sanksi pidana akan terus menjadi pisau tumpul dalam memerangi kejahatan siber.

Model Ideal Sanksi Pidana untuk Kejahatan Siber dalam Sistem Hukum Positif Indonesia: Sebuah Rekonstruksi Paradigmatik

Kejahatan siber di Indonesia membutuhkan pendekatan sanksi pidana yang lebih komprehensif dan adaptif mengingat karakteristik uniknya yang berbeda dari kejahatan konvensional. Sistem hukum saat ini masih mengadopsi paradigma lama yang terlalu mengandalkan sanksi penjara dan denda, padahal kejahatan siber memerlukan respons yang lebih multidimensi. Model ideal seharusnya mempertimbangkan aspek teknis kejahatan siber yang sangat dinamis dan bersifat lintas batas yurisdiksi(Soecipto, 2022).

Salah satu kelemahan mendasar UU ITE dan KUHP adalah ketidakmampuan mengakomodasi perkembangan terbaru teknologi digital dan modus operandi kejahatan siber. Sistem sanksi yang ada cenderung kaku dan tidak memiliki gradasi yang jelas sesuai tingkat bahaya dan dampak dari berbagai jenis kejahatan siber. Padahal, kejahatan seperti pembobolan data pribadi seharusnya diperlakukan berbeda dengan serangan terhadap infrastruktur kritis negara baik dari segi kualifikasi maupun beratnya sanksi(Amalia & Prasetyo, 2021).

Pendekatan sanksi seharusnya lebih berfokus pada upaya restoratif dan preventif dibanding sekadar penghukuman. Untuk pelaku individu dengan motivasi ekonomi, program rehabilitasi berbasis kompetensi digital bisa lebih efektif daripada penjara. Sementara bagi korporasi yang lalai menjaga keamanan data, sanksi administratif seperti audit wajib dan denda progresif mungkin lebih tepat guna. Model sanksi juga perlu mempertimbangkan mekanisme ganti rugi yang cepat dan adil bagi korban.

Aspek pembuktian dalam kejahatan siber menjadi tantangan tersendiri yang mempengaruhi efektivitas sanksi. Perlu dibangun sistem pembuktian elektronik yang komprehensif meliputi standar preservasi bukti digital, sertifikasi alat bukti, dan kapasitas ahli yang memadai. Tanpa penguatan di sisi pembuktian, sanksi pidana yang berat sekalipun akan sulit dijatuhkan secara konsisten.

Koordinasi antar lembaga penegak hukum perlu diperkuat melalui pembentukan satuan tugas khusus kejahatan siber yang terintegrasi. Mekanisme kerja sama harus mencakup BSSN, kepolisian, kejaksaan, dan Kominfo dengan pembagian peran yang jelas. Sistem database terpusat untuk kasus kejahatan siber akan membantu menciptakan konsistensi dalam penerapan sanksi.

Untuk kasus-kasus tertentu, model sanksi alternatif seperti pembatasan akses internet, pencabutan sertifikat digital, atau kewajiban pelatihan keamanan siber bisa dipertimbangkan. Pengalaman negara lain menunjukkan bahwa sanksi semacam ini seringkali lebih efektif dalam mencegah pengulangan kejahatan dibanding pemidanaan konvensional(Putra, 2014).

Peningkatan kapasitas aparat penegak hukum mutlak diperlukan agar sanksi dapat diterapkan secara tepat. Pendidikan dan pelatihan berkelanjutan tentang investigasi digital, analisis bukti elektronik, dan pemahaman teknologi terkini harus menjadi prioritas. Tanpa penguatan SDM, aturan sanksi yang baik pun tidak akan efektif dalam praktik.

Perlu dibangun mekanisme evaluasi berkala terhadap efektivitas sanksi pidana yang telah dijatuhkan. Data statistik tentang tingkat residivisme, dampak deterrence, dan kepuasan korban perlu dikumpulkan secara sistematis sebagai bahan perbaikan kebijakan. Sistem sanksi harus bersifat dinamis dan mampu menyesuaikan dengan perkembangan kejahatan siber.

Kerjasama internasional menjadi krusial mengingat sifat kejahatan siber yang lintas batas. Indonesia perlu aktif dalam perjanjian ekstradisi dan bantuan hukum timbal balik khusus untuk kejahatan siber. Pengadopsian standar internasional dalam penanganan bukti digital akan memperkuat posisi Indonesia dalam penegakan hukum siber global.

Pada akhirnya, reformasi sistem sanksi pidana untuk kejahatan siber harus dilakukan secara holistik. Tidak hanya perubahan pada level undang-undang, tetapi juga penguatan kelembagaan, peningkatan kapasitas SDM, dan pembangunan ekosistem penegakan hukum yang adaptif. Dengan pendekatan yang komprehensif, sanksi pidana dapat benar-benar efektif sebagai alat penanggulangan kejahatan siber di Indonesia.

Kesimpulan

Reformasi sistem sanksi pidana untuk kejahatan siber di Indonesia membutuhkan transformasi paradigmatik yang menyeluruh. Berdasarkan analisis mendalam, dapat disimpulkan bahwa model sanksi yang ada saat ini dalam UU ITE dan KUHP belum memadai untuk menghadapi karakteristik khusus kejahatan siber yang bersifat dinamis, teknis, dan lintas yurisdiksi. Sistem hukum pidana konvensional yang mengandalkan sanksi penjara dan denda tradisional terbukti tidak efektif baik sebagai deterrent maupun sebagai instrumen restoratif.

Solusi ideal memerlukan pendekatan multidimensi yang mengintegrasikan: (1) sistem sanksi berlapis berbasis dampak dan modus operandi, (2) mekanisme sanksi administratif dan pidana yang saling melengkapi, (3) pendekatan restoratif dan rehabilitatif khususnya untuk pelaku individu, serta (4) penguatan sistem pembuktian elektronik. Aspek kelembagaan dan kapasitas SDM penegak hukum menjadi faktor krusial yang menentukan keberhasilan implementasi model sanksi baru ini. Yang paling mendasar, Indonesia perlu membangun kerangka hukum siber yang adaptif, mengadopsi best practices internasional namun tetap kontekstual dengan kondisi domestik. Transformasi ini harus mencakup tidak hanya aspek regulasi tetapi juga penguatan infrastruktur penegakan hukum, peningkatan kapasitas teknis aparat, dan pengembangan sistem pemantauan yang komprehensif. Hanya dengan pendekatan holistik dan terintegrasi, sanksi pidana dapat benar-benar efektif sebagai instrumen penanggulangan kejahatan siber di era digital.

Daftar Pustaka

Agung, D. (2022). *Tanggung Jawab Kepolisian Dalam Penegakan Hukum Kejahatan Siber Di Era Perkembangan Teknologi=(the Responsibility of the Police in the Enforcement of Cybercrime Laws in the Era of Technological Development)*. repository.unhas.ac.id. https://repository.unhas.ac.id/id/eprint/31991/

Amalia, D. A. R., & Prasetyo, M. H. (2021). Kebijakan Hukum Pidana

Dalam Upaya Penanggulangan Cyber Terorism. *Jurnal Pembangunan Hukum Indonesia*, *3*(2), 228–239. https://doi.org/10.14710/jphi.v3i2.228-239

Awaluddin, F., Amsori, & Mulyana, M. (2024). Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital. *Humaniorum*, *2*(1), 14–19. https://doi.org/10.37010/hmr.v2i1.35

Ayman, D. N., & Nurhadiyanto, L. (2024). Analisis Kejahatan Siber Sniffing Pada Media Sosial Whatsapp (Studi Kasus Kurir Paket Bodong). *IKRA-ITH HUMANIORA: Jurnal …*. http://journals.upi-yai.ac.id/index.php/ikraith-humaniora/article/view/3693%0Ahttp://journals.upi-yai.ac.id/index.php/ikraith-humaniora/article/download/3693/2783

Bhakti, I. D. (2025). Analisis Upaya Kejahatan Siber Terhadap Pencurian Data Digital Pengguna Internet dan Perangkat Seluler. *Prosiding Seminar Nasional KONSTELASI*. https://ojs.uajy.ac.id/index.php/prosidingkonstelasi/article/view/10974

Davis Mahardika, M. (2020). Kejahatan Siber Hoax di Ruang Digital Masyarakat Indonesia melalui Teori Aktivitas Rutin. In *Jurnal Kriminologi Indonesia* (Vol. 16, Issue 2). core.ac.uk. http://journal.ui.ac.id/index.php/jki/article/view/12572

DM, M. Y., Agustantia, M., & Zulaiha, S. (2022). Tindak Pidana Kejahatan Pemalsuan data (Data Forgery) dalam Bentuk Kejahatan Siber (Cyber Crime). In *Jurnal Pendidikan dan Konseling* (Vol. 4, Issue 6, pp. 6635–6640).

Faridi, M. K. (2019). Kejahatan Siber Dalam Bidang Perbankan. *Cyber Security Dan Forensik Digital*, *1*(2), 57–61. https://doi.org/10.14421/csecurity.2018.1.2.1373

Kemit, J. F., Agatha, V., & Kleden, K. L. (2023). Yurisdiksi Kejahatan Siber: Borderless. *Seminar Nasional Hukum Dan Pancasila*, *2*(9), 55–70. https://conference.untag-sby.ac.id/index.php/snhp/article/view/2414

M. Syafiih, Nadiyah, Khairi, M., Moh. Furqan, & Beny Yusman. (2024). Pendampingan Literasi Digital untuk Mengurangi Risiko Kejahatan Siber Membentuk Masyarakat yang Lebih Aman. *JILPI : Jurnal Ilmiah Pengabdian Dan Inovasi*, *2*(4), 1027–1036. https://doi.org/10.57248/jilpi.v2i4.456

Madinah Mokobombang, Zulfikri Darwis, & Sabil Mokodenseho. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum Dan HAM Wara Sains*, *2*(6), 517–525. https://doi.org/10.58812/jhhws.v2i6.447

Mahira Dewantoro, N., & Dian Alan Setiawan S.H., M.H. (2023). Penegakan Hukum Kejahatan Siber Berbasis Phising dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. In *Bandung Conference Series: Law Studies* (Vol. 3, Issue 2, pp. 892–900). https://doi.org/10.29313/bcsls.v3i2.7247

Meha Middlyne Simbolon, I Gusti Komang Wijaya Kesuma, & Aditya Ery Wibowo. (2021). Kejahatan Siber pada Penyelenggaraan Perdagangan Berbasis Sistem Elektronik Dalam langkah Pengamanan Pertumbuhan Ekonomi Digital Indonesia. In *Defendonesia* (Vol. 5, Issue 1, pp. 1–12). scholar.archive.org. https://doi.org/10.54755/defendonesia.v5i1.98

Muhammad. (2022). Peningkatan Korban Kejahatan SiberSelama Pandemi Covid19. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *9*(6), 2043–2054. http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

Muhammad, A., Hutagalung, C., Marendra, N. R., & Ul, A. (2024). Perlindungan Terhadap Konsumen Dalam Kasus Kebocoran Data Bank Syariah Indonesia. In *Jurnal Ilmu Hukum, Sosial, dan Humaniora* (Vol. 2, Issue 1, pp. 156–165).

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum*, *2*(1), 8–16. https://ejournal.unisi.ac.id/index.php/albahts/article/view/3044

Nicodemus, A. A. (2023). *Tantangan dalam Penegakan Hukum Pidana terhadap Kejahatan Siber di Era Digital*. digilib.iblam.ac.id. http://digilib.iblam.ac.id/id/eprint/953/

Putra, A. K. (2014). Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional. In *Jurnal Ilmu Hukum* (pp. 95–109). academia.edu. https://www.academia.edu/download/93009444/1301.pdf

Putri, E. P. (2022). Pentingnya Perlindungan Data Di Indonesia Sebagai

Upaya Tanggungjawab Hukum Atas Kebocoran Data. In *Universitas Islam Indonesia* (Issue 8.5.2017). dspace.uii.ac.id. https://dspace.uii.ac.id/handle/123456789/41660%0Ahttps://dspace.uii.ac.id/bitstream/handle/123456789/41660/20912060.pdf?sequence=1&isAllowed=y

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2). https://doi.org/10.33172/jpbh.v7i2.179

Ramadha, B. S. (2021). *Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perindungan Data Pribadi di Indonesia*. dspace.uii.ac.id. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dspace.uii.ac.id/bitstream/handle/123456789/31626/18912046 Bagus Satryo Ramadha.pdf?sequence=1&isAllowed=y

Saputra, D. (2024). Legal Dynamics in Handling Cyber Crime in Indonesia: Dinamika Hukum Dalam Penanganan Kejahatan Siber Di Indonesia. *Lex Researchia*. https://jurnal.htp.ac.id/index.php/lex/article/view/1987

Sari, H. P., Mulyani, D. I., Nilamsari, M. A., Sitorus, D. D. F., & ... (2024). EFEKTIVITAS HUKUM PERLINDUNGAN DATA PRIBADI TERHADAP KEJAHATAN SIBER DI INDONESIA. In *Jurnal Media Akademik …*.

Setiawan, N. (2019). Kasus Kejahatan Siber Pada Telepon Seluler Android. *Cyber Security Dan Forensik Digital*, *2*(1), 24–29. https://doi.org/10.14421/csecurity.2019.2.1.1420

Sihombing, G. P., Hamzah, H. A., Tian, C., Lianda, T. A. C., Daniswara, M. D., & Saputra, M. N. (2023). Analisis Dampak Kejahatan Siber Terhadap Kepercayaan Konsumen Dalam Berbelanja Di Tokopedia. In *Jurnal Ekonomika dan Manajemen* (Vol. 12, Issue 2). pdfs.semanticscholar.org. https://doi.org/10.36080/jem.v12i2.2362

Soecipto. (2022). Optimalisasi Hukum Siber (cyber law) dalamPenanggulangan Kejahatan Penipuan melalui InternetdalamMenyelamatkan Kehidupan Masyarakat. *Teknologi Nusantara*, *4*(2), 34–46. http://ojs.uninus.ac.id/index.php/teknologinusantara

Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. *Jurnal Impresi*

Indonesia, 2(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594