

Tindak Pidana Ekonomi melalui Kejahatan Siber: Analisis terhadap Putusan Pengadilan

Andini Khoirunnisa¹, Devina Tri Aulia², Sarip Hidayat³

^{1,2,3}Fakultas Hukum, Universitas Kuningan, Indonesia

Email: 20231410060@uniku.ac.id¹, 20231410009@uniku.ac.id², sarip.hidayat@uniku.ac.id³

Abstrak

Perkembangan teknologi informasi dan komunikasi telah memunculkan berbagai bentuk kejahatan siber yang berdampak pada aspek sosial, ekonomi, dan hukum. Di Indonesia, kejahatan siber tidak hanya menyebabkan kerugian ekonomi, tetapi juga mengancam keamanan transaksi elektronik dan kepercayaan publik. Penelitian ini bertujuan menganalisis peran Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam penanganan kejahatan siber serta penerapannya dalam putusan pengadilan. Metode yang digunakan adalah yuridis normatif dengan pendekatan studi kasus, menggunakan bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, serta bahan hukum sekunder dari literatur dan jurnal ilmiah. Hasil penelitian menunjukkan bahwa UU ITE berperan penting sebagai dasar hukum dalam menindak pelaku kejahatan siber, seperti penipuan elektronik, penyebaran informasi bohong, dan pencemaran nama baik. Namun, efektivitas penerapannya masih menghadapi kendala pembuktian digital, keterbatasan infrastruktur, serta rendahnya literasi hukum dan digital masyarakat.

Kata kunci: Tindak Pidana; Ekonomi; Putusan Pengadilan

Abstract

The rapid development of information and communication technology has led to the emergence of various forms of cybercrime that affect social, economic, and legal aspects of society. In Indonesia, cybercrime not only causes economic losses but also threatens the security of electronic transactions and public trust. This study aims to analyze the role of the Electronic Information and Transactions Law (ITE Law) in addressing cybercrime and its implementation in court decisions. The research employs a normative juridical method with a case study approach, utilizing primary legal materials in the form of legislation and court decisions, as well as secondary legal materials derived from literature and scientific journals. The findings indicate that the ITE Law plays a significant role as a legal basis for prosecuting cybercrime offenders, particularly in cases involving electronic fraud, the dissemination of false information, and defamation. However, its effectiveness remains constrained by challenges in digital evidence, limited infrastructure, and the low level of legal and digital literacy among the public.

Keywords: Criminal Acts; Economics; Court Decisions

A. Pendahuluan

Peraturan perundang-undangan terkait kejahatan siber telah berkembang pesat di berbagai negara belahan dunia. Peraturan ini berfokus pada harmonisasi hukum Internasional bertujuan menangani ancaman digital yang melintasi batas negara.¹ Di Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) menjadi dasar utama, yang diperkuat oleh peraturan turunan seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.² Namun, di dalamnya terdapat tantangan muncul dalam penerapan hukum, seperti kejahatan siber yang sering melibatkan yurisdiksi lintas negara. Regulasi ITE di Indonesia juga perlu disesuaikan dengan

¹ Heryanto Kawisen et al., "Analisis Efektivitas Dan Tantangan Hukum Internasional Dalam Penanggulangan Kejahatan Siber Lintas Negara Secara Global," *JATI (Jurnal Mahasiswa Teknik Informatika)* 9, no. 5 (2025): 8613–18.

² Dwi Erna Susilowati, Muhammad Muhtarom, dan Amir Junaidi, "Analisis yuridis keabsahan tanda tangan digital dalam transaksi e-commerce di Indonesia," *Jurnal Penelitian Serambi Hukum* 18, no. 01 (2025): 17–26.

standar internasional seperti *Konvensi Budapest* tentang Kejahatan Siber untuk meningkatkan efektivitas penegakan hukum.³

Kejahatan siber telah meningkat secara drastis dengan dilihat data dari Interpol melaporkan lonjakan serangan ransomware dan phishing sebesar 300% (tiga ratus persen) selama pandemi COVID-19.⁴ Di tingkat global, kondisi ini diperburuk oleh ketergantungan pada teknologi digital, di mana perusahaan dan individu menjadi sasaran utama. Pada negara-negara berkembang seperti Indonesia menghadapi tantangan infrastruktur yang lemah, sehingga memerlukan adanya penelitian lebih lanjut tentang pola kejahatan siber untuk mengembangkan strategi pencegahan yang lebih efektif.⁵

Kebaruan dari tulisan ini terletak pada pendekatan integratif yang menggabungkan analisis regulasi hukum dengan studi kasus penerapan di era digital saat ini, termasuk dampak kecerdasan buatan dalam kejahatan siber. Berbeda dari penelitian sebelumnya yang fokus pada aspek teknis, artikel ini menekankan interaksi antara peraturan dan praktik penegakan hukum. Pendekatan ini menawarkan wawasan baru tentang bagaimana regulasi dapat disesuaikan dengan evolusi teknologi, seperti penggunaan *AI* dalam deteksi kejahatan, yang belum banyak dieksplorasi dalam literatur terkini.⁶ Kejahatan siber menyebabkan kerugian ekonomi global mencapai triliunan dolar pertahun, Indonesia sebagai salah satu negara terdampak tinggi akibat serangan terhadap sektor keuangan dan pemerintah.⁷ Permasalahan utama meliputi kesenjangan antara regulasi yang ada dan kemampuan penegakan, serta kurangnya koordinasi internasional. Terdapat fakta dan dengan data menunjukkan bahwa 70% (tujuh puluh persen) serangan siber tidak dilaporkan, sehingga memperburuk masalah dalam pengumpulan bukti dan penuntutan di pengadilan.⁸ Di tingkat internasional, peraturan seperti General Data Protection Regulation (GDPR) di Uni Eropa dan Cybercrime Convention telah mempengaruhi pembentukan hukum nasional, termasuk di Asia Tenggara. Namun, penerapan di Indonesia masih menghadapi hambatan seperti interpretasi hukum yang beragam dan kurangnya sumber daya manusia terlatih. bagaimana regulasi ini perlu diperkuat

³ Joni Laksito, Maulana Fahmi Idris, dan Agus Waryanto, "Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif," *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 4 (2024): 774–90.

⁴ Jansen Chandra, Vincent Tanaka, dan Ricky Banke, "Peran Interpol dalam Menangani dan Menanggulangi Kejahatan Siber di Indonesia," *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora* 4, no. 3 (2025): 4710–19.

⁵ Mukum Syahrir, "Efektivitas Hukuman bagi Pelaku Kejahatan Siber di Indonesia: Analisis Kriminologi dengan Metode Content Analysis," *Perkara: Jurnal Ilmu Hukum dan Politik* 3, no. 1 (2025): 694–711.

⁶ Sitti Fatimah dan Ludfi Ludfi, "Navigasi Hukum Di Era Fintech Syariah: Tinjauan Literatur Dan Regulasi," *IDEALITA: Jurnal Pendidikan Dan Sosial Keagamaan* 4, no. 1 (2024): 41–52.

⁷ Isro'Kurniawan Rahakbauw dan Ika Arini Batubara, "Analisis Potensi Ancaman Siber pada Bidang Ekonomi di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional* 7, no. 1 (2024): 5.

⁸ Rasya Arafah dan Irwan Triadi, "Analisis Peran Hukum Internasional Dalam Mencegah Perdagangan Manusia Di Indonesia," *Media Hukum Indonesia (MHI)* 3, no. 3 (2025).

melalui kerja sama regional, seperti ASEAN Cyber Security Cooperation, untuk mengatasi kejahatan siber lintas batas yang semakin kompleks. Kondisi terkini menunjukkan peningkatan kejahatan siber yang melibatkan *deepfake* dan serangan terhadap infrastruktur kritis, dengan laporan dari *Cybersecurity and Infrastructure Security Agency (CISA)* AS mencatat ribuan insiden perbulan. Penelitian pendahuluan ini mengungkapkan bahwa sektor kesehatan dan energi menjadi target utama, dengan dampak yang merusak. kondisi ini memerlukan penelitian interdisipliner untuk memahami dinamika sosial dan teknis kejahatan siber.⁹

Artikel ini mengusulkan model baru untuk evaluasi efektivitas regulasi berdasarkan indikator seperti tingkat penuntutan dan tingkat kesadaran Masyarakat dengan menggunakan sistem hukum. Penelitian ini semakin mendesak dengan munculnya ancaman baru seperti *cyber warfare* dan eksploitasi data pribadi, yang dapat mengancam stabilitas nasional. Permasalahan yang dibahas meliputi ketidakmampuan regulasi untuk mengimbangi inovasi teknologi, serta isu etika dalam pengawasan digital.¹⁰ Melalui analisis kasus, menunjukkan bahwa tanpa reformasi regulasi, kejahatan siber akan terus berkembang, memerlukan tindakan kolektif dari pemerintah, industri, dan masyarakat. Penelitian ini berfokus pada analisis peran Undang-Undang Informasi dan Transaksi Elektronik (ITE) dalam penanganan kasus kejahatan siber, serta mengkaji bagaimana penerapan hukum terhadap pelaku kejahatan siber dalam berbagai putusan pengadilan. Kajian ini bertujuan untuk memahami efektivitas UU ITE sebagai dasar hukum dalam menanggulangi kejahatan siber dan menilai implementasi penegakan hukum oleh aparat penegak hukum dan lembaga peradilan terhadap pelaku tindak pidana siber.

B. Metode Penelitian

Penelitian ini menggunakan pendekatan yuridis normatif dengan metode studi kasus untuk menganalisis implementasi penegakkan hukum terhadap kejahatan siber dalam putusan-putusan pengadilan. Jenis penelitian kualitatif deskriptif analitis, dengan sumber data primer berupa putusan pengadilan dan Undang – Undang tentang informasi dan Transaksi Elektronik, serta sumber sekunder dari jurnal ilmiah. Teknik pengumpulan data melalui studi dokumen, diikuti analisis isi dan yuridis untuk mengidentifikasi tema seperti peran hukum, tantangan, dan rekomendasi.

⁹ Muhammad Arafat dan Alexander Tito Enggar Wirasto, “Kebijakan kriminal dalam penanganan siber di era digital: Studi kasus di Indonesia,” *Equality: Journal of Law and Justice* 1, no. 2 (2024): 220–41.

¹⁰ Akhmad Zaki Yamani, “Analisis Tantangan Dalam Penyusunan Rancangan Undang-Undang Di Era Transformasi Digital: Antara Regulasi, Inovasi, Dan Perlindungan Hak,” *Journal Of Law And Nation* 4, no. 2 (2025): 312–24.

C. Hasil dan Pembahasan

1. Peran Peraturan Undang-Undang tentang Informasi dan Transaksi Elektronik (ITE) dalam kasus Kejahatan Siber

Globalisasi jadi salah satu pemicu teknologi memasuki sendi kehidupan masyarakat bangsa Indonesia, ini tidak terlepas dari adanya interaksi global yang menyebabkan akselerasi dan perubahan.¹¹ Perkembangan teknologi informasi telah membawa dampak positif dalam berbagai aspek kehidupan, tetapi juga memicu peningkatan kejahatan ekonomi berbasis digital. Kejahatan ini meliputi berbagai bentuk pelanggaran, seperti penipuan online, pencurian data pribadi, dan pencucian uang melalui jaringan internet, yang semakin meningkat sejalan dengan semakin besarnya peran internet dalam kehidupan sehari-hari. Jenis kejahatan ini memiliki konsekuensi yang serius, baik bagi individu yang kehilangan data atau dana, perusahaan yang mengalami kerugian akibat serangan siber, maupun negara yang dirugikan oleh hilangnya potensi pendapatan. Berdasarkan hukum di Indonesia, beberapa tindak kejahatan ini melanggar Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 19 Tahun 2016 Pasal 28 ayat (1), yang mengatur tentang larangan penyebaran informasi yang menyesatkan atau penipuan melalui media elektronik.¹² Pemerintah Indonesia telah melakukan pembaruan regulasi melalui Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) yang menggantikan UU Nomor 19 Tahun 2016. Pembaruan ini dilatarbelakangi oleh kebutuhan akan kerangka hukum yang lebih komprehensif dan adaptif dalam menghadapi evolusi ancaman siber, khususnya cyberterrorism yang semakin canggih dan terorganisir. Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam pencegahan cyberterrorism sangat bergantung pada alat dan sarana yang digunakan dalam implementasinya.¹³ Alat dan sarana yang dimaksud meliputi, Teknologi Pemantauan Siber yaitu Pemerintah melalui instansi seperti Badan Siber dan Sandi Negara (BSSN) telah menggunakan perangkat pemantauan berbasis kecerdasan buatan (AI) dan analitik big data untuk mendeteksi aktivitas mencurigakan di dunia maya. Alat ini membantu dalam identifikasi ancaman potensial, seperti penyebaran propaganda radikal dan komunikasi yang berpotensi terorisme. Sistem

¹¹ Zainudin Hasan Dan Ahmad Mahardika, "Peranan Cyber Law Dalam Penanganan Tindak Pidana" 2, no. 5 (2024): 337–45.

¹² Andi Ahmad Munajat dan Hudi Yusuf, "Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus : Studi Tentang Kejahatan Keuangan Berbasis Digital The Role of Information Technology in the Prevention and Disclosure of Special Economic Crimes : A Study of Digital-Based Financial Crimes," no. November (2024): 4853–65.

¹³ Muhammad Arkhan et al., "Evaluasi Efektivitas Undang-Undang No. 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik dalam Pencegahan Cyberterrorism Evaluation of the Effectiveness of Law No. 1 of 2024 on Information and Electronic Transactions in Preventing Cyberterrorism" 5681, no. 2 (2024): 430–43.

Deteksi dan Respon Ancaman di UU ITE memberikan dasar hukum bagi penggunaan sistem deteksi dini (early warning system) yang terintegrasi dengan pusat data nasional. Sistem ini mampu memberikan peringatan dini kepada otoritas terkait untuk mencegah eskalasi ancaman, Infrastruktur Hukum Digital yaitu dengan Keberadaan portal aduan online yang dikelola oleh Kementerian Komunikasi dan Informatika (Kominfo) memungkinkan masyarakat melaporkan aktivitas siber yang mencurigakan. Sarana ini memperkuat partisipasi masyarakat dalam mendukung implementasi UU ITE.¹⁴

Hukum bersifat progresif ketika hukum dapat mengikuti perkembangan masyarakat. Saat ini telah lahir suatu rezim hukum baru yang dikenal sebagai Hukum Siber. Hukum Siber didefinisikan sebagai padanan kata dari Cyber Law, Informasi dan Transaksi Elektronik atau dikenal dengan UU ITE merupakan salah satu langkah kepedulian pemerintah terhadap perkembangan dan pemanfaatan teknologi informasi agar dapat diakses secara aman serta memberikan kepastian hukum terutama dalam menanggulangi cyber crime hal ini dibuktikan dengan dimasukkannya UU ITE kedalam Kitab Undang-Undang Hukum Pidana.¹⁵ Pertanggungjawaban hukum terkait penyebarluasan data pribadi yang tersimpan pada barcode dapat berupa tanggung jawab pidana dan perdata antara lain : 1) Tanggung Jawab Pidana : Pelaku yang menyebarkan data pribadi tanpa izin dapat dikenakan sanksi pidana berdasarkan Pasal 45 ayat (1) UU ITE. Sanksi ini mencakup pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah). Selain itu, Pasal 30 UU ITE juga mengatur tentang akses ilegal ke sistem elektronik yang dapat dikenakan sanksi pidana; 2) Tanggung Jawab Perdata : Korban penyebarluasan data pribadi dapat mengajukan gugatan perdata berdasarkan Pasal 26 ayat (2) UU ITE. Gugatan ini dapat diajukan untuk mendapatkan ganti rugi atas kerugian yang dialami akibat penyebarluasan data pribadi tanpa izin. Selain itu, korban juga dapat menuntut pemulihan nama baik.¹⁶

Upaya Preventif dalam melakukan upaya preventif ini pihak kepolisian khususnya unit cyber crime polisi telah melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik.¹⁷ Tantangan Implementasi di Lapangan Meskipun

¹⁴ H Ajamalus dan Agung Cucu Purnawirawan, "Perkembangan Hukum Cyber di Indonesia: Tantangan dan Peluang," *Bulletin of Community Engagement* 4, no. 3 (2024): 109–16.

¹⁵ Indah Meisyana Suci et al., "Perlindungan Hak Kekayaan Intelektual Di Era Digital Melalui Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE)," n.d.

¹⁶ Ilham Muhammad dan Akbar Muhammad, "Pelaku Penyebaran Data Pribadi Yang Tersimpan Pada Barcode Ditinjau Dari Undang-Undang Informasi Transaksi," 2024, 43–52, <https://doi.org/10.47709/ijbl.v3i1.4281>.

¹⁷ Erine Nur Maulidya et al., "Strategi Penanggulangan Informasi Hoax dan Terorisme di Media Sosial Oleh Unit Polisi Virtual Provinsi Lampung," *Jurnal Dakwah dan Komunikasi* 8, no. 1 (2023): 139–56.

undang-undang ini cukup komprehensif, tantangan terbesar yang dihadapi adalah implementasi yang tidak merata. Beberapa daerah dan sektor masih kesulitan dalam menerapkan regulasi ini dengan maksimal. Keterbatasan anggaran dan kurangnya infrastruktur teknologi yang memadai di beberapa bagian negara menjadi hambatan besar. Peran Penyuluhan dalam Meningkatkan Kesadaran Keamanan Penyuluhan yang lebih masif dan program edukasi terkait pencegahan cyberterrorism sangat penting untuk membangun kesadaran di kalangan masyarakat dan organisasi. Walaupun ada upaya dalam penyuluhan, tingkat pemahaman masyarakat tentang pentingnya menjaga keamanan data dan informasi masih rendah, yang membuka celah bagi potensi serangan.¹⁸ Rendahnya pemahaman terhadap validitas alat bukti digital sering kali menyebabkan kasus siber tidak dapat dilanjutkan ke tahap penyidikan, karena tidak terpenuhinya syarat formil dan materiil pembuktian. Oleh karena itu, kegiatan ini merekomendasikan pentingnya pendampingan hukum bagi korban kejahatan siber, khususnya dalam aspek perolehan dan penyusunan bukti digital yang sah. Pendampingan ini diharapkan dapat memberikan rasa keadilan.¹⁹ demikian, UU ITE dapat mencapai tujuannya secara optimal, yakni sebagai landasan hukum yang kuat untuk melindungi kepentingan nasional dan masyarakat di era teknologi informasi yang terus berkembang.²⁰

Perkembangan globalisasi dan kemajuan teknologi informasi telah membawa perubahan fundamental dalam struktur sosial, ekonomi, dan hukum di Indonesia. Transformasi digital yang masif telah mendorong masyarakat untuk bergantung pada sistem elektronik dalam berbagai aktivitas, mulai dari transaksi ekonomi hingga komunikasi sehari-hari.²¹ Namun, di balik kemudahan tersebut, muncul berbagai bentuk kejahatan ekonomi digital yang semakin kompleks dan sulit dideteksi. Penelitian mutakhir menunjukkan bahwa kejahatan siber kini tidak lagi bersifat sporadis, melainkan terorganisir, sistematis, dan sering kali melibatkan jaringan lintas negara yang memanfaatkan celah hukum serta kelemahan sistem keamanan digital.²²

¹⁸ Markus, Novita Alfiani, Dan Hanita 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" 2, no. 10 (2023): 3799–3806.

¹⁹ Uut Rahayuningsih dan Bayu Prasetyo, "Sosialisasi Pembuktian Cyber Crime dalam KUHAP dan UU ITE" 4, no. 3 (2025): 649–58.

²⁰ Astri Aprilianti, "Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi" 15 (2024).

²¹ Jayanti Armida Sari dan Bambang Agus Diana, "Dampak Transformasi Digitalisasi terhadap Perubahan Perilaku Masyarakat Pedesaan," *Jurnal Pemerintahan dan Politik* 9, no. 2 (2024): 88–96.

²² Deva Wira Pramudya dan Hudi Yusuf, "Anatomi Kriminal Siber: Motif, Modus, Dan Penanggulangannya Dari Perspektif Kriminologi," *Jurnal Intelek Insan Cendikia* 2, no. 8 (2025): 14613–23.

Dalam konteks ini, keberadaan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi instrumen hukum yang strategis dalam menanggulangi kejahatan siber.²³ Pembaruan regulasi melalui Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik mencerminkan upaya negara untuk membangun hukum yang adaptif terhadap dinamika ancaman siber, termasuk cyberterrorism. Sejumlah jurnal hukum menegaskan bahwa pembaruan UU ITE merupakan bentuk konkret dari hukum progresif, di mana hukum tidak bersifat statis, tetapi mampu menyesuaikan diri dengan perkembangan teknologi dan kebutuhan masyarakat.²⁴

Lebih lanjut, efektivitas UU ITE dalam pencegahan cyberterrorism sangat ditentukan oleh dukungan alat dan sarana teknologi yang memadai. Pemanfaatan teknologi pemantauan siber berbasis kecerdasan buatan (Artificial Intelligence) dan analitik big data oleh Badan Siber dan Sandi Negara (BSSN) dinilai sebagai langkah preventif yang signifikan. Jurnal-jurnal keamanan siber menjelaskan bahwa sistem ini memungkinkan deteksi dini terhadap pola komunikasi mencurigakan, penyebaran propaganda radikal, serta potensi serangan terorisme digital sebelum menimbulkan dampak yang lebih luas terhadap keamanan nasional.²⁵

Di sisi lain, aspek kelembagaan juga menjadi faktor penentu keberhasilan implementasi UU ITE. Penelitian empiris menunjukkan bahwa koordinasi antar lembaga penegak hukum, seperti Kepolisian, Kejaksaan, Kominfo, dan BSSN, masih menghadapi berbagai hambatan struktural dan teknis.²⁶ Ketidaksamaan pemahaman mengenai kewenangan, prosedur penanganan perkara siber, serta standar operasional pembuktian digital sering kali menyebabkan proses penegakan hukum berjalan lambat dan kurang optimal. Kondisi ini menegaskan pentingnya penguatan sinergi antar lembaga dalam kerangka penegakan hukum siber yang terintegrasi.²⁷

Permasalahan pembuktian digital juga menjadi tantangan krusial dalam penanganan kejahatan siber. Berbagai jurnal hukum acara pidana menyoroti bahwa alat bukti elektronik memiliki karakteristik yang rentan terhadap manipulasi, penghapusan, dan perubahan data.

²³ Gunawan Widjaja, "Penyesuaian Hukum Nasional Indonesia Terhadap Konvensi Pbb Anti-Kejahatan Siber 2024: Kajian Pustaka Tentang Harmonisasi Uu Ite Dan Kuhp Untuk Penguatan Penanganan Kejahatan Siber Lintas Negara," *NETIZEN: JOURNAL OF SOCIETY AND BUSSINESS* 1, no. 11 (2025): 611–21.

²⁴ Eren Arif Budiman dan M H SH, "Literasi Hukum Digital Di Tingkat Masyarakat," *Transformasi Hukum* 47 (2025).

²⁵ Puteri Ananda Khairunnisa, Norul Annisa, dan Jadianan Parhusip, "Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia," *Teknik: Jurnal Ilmu Teknik Dan Informatika* 4, no. 2 (2024): 9–16.

²⁶ Muhammad Singgih Imam Wibowo dan Akhmad Munawar, "Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia," *Jurnal Hukum Lex Generalis* 5, no. 7 (2024).

²⁷ Wibowo dan Munawar.

Oleh karena itu, aparat penegak hukum dituntut memiliki kompetensi teknis dalam memastikan keaslian (authenticity), integritas (integrity), dan ketersediaan (availability) alat bukti digital. Tanpa dukungan keahlian forensik digital yang memadai, banyak perkara kejahatan siber berpotensi gugur pada tahap penyidikan atau persidangan.²⁸

Selain pendekatan represif, upaya preventif melalui peningkatan literasi digital masyarakat juga memiliki peran yang sangat penting. Berbagai penelitian menunjukkan bahwa rendahnya kesadaran masyarakat terhadap keamanan data dan validitas informasi menjadi faktor utama meningkatnya kejahatan siber. Program penyuluhan hukum dan edukasi keamanan siber yang dilakukan oleh aparat kepolisian, pemerintah daerah, serta institusi pendidikan dinilai perlu dilakukan secara berkelanjutan dan masif agar masyarakat mampu mengenali potensi ancaman serta melindungi data pribadinya secara mandiri.²⁹

keberhasilan UU ITE dalam menanggulangi kejahatan ekonomi digital dan cyberterrorism tidak hanya bergantung pada kekuatan norma hukum semata, tetapi juga pada kesiapan teknologi, kapasitas kelembagaan, kualitas penegakan hukum, serta tingkat kesadaran masyarakat. Sejumlah jurnal hukum kontemporer menegaskan bahwa hukum siber harus terus dikembangkan secara adaptif dan responsif agar mampu menjadi instrumen perlindungan kepentingan nasional, menjamin kepastian hukum, serta memberikan rasa keadilan bagi masyarakat di tengah pesatnya perkembangan teknologi informasi.³⁰

2. Penerapan Hukum terhadap Putusan - Putusan Pengadilan

a. Putusan Nomor 95/Pid.Sus/2024/ PN JKT. Sel

Putusan Pengadilan Negeri Jakarta Selatan Nomor 95/Pid.Sus/2024/PN JKT. Sel. berkaitan dengan tindak pidana penyebaran informasi bohong dan menyesatkan dalam transaksi elektronik yang dilakukan oleh terdakwa melalui media daring. Perbuatan tersebut dilakukan dengan cara menawarkan transaksi kepada konsumen menggunakan informasi yang tidak sesuai dengan keadaan sebenarnya, sehingga menimbulkan kerugian materiil bagi para korban. Atas perbuatannya, terdakwa didakwa melanggar Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik, serta dikaitkan dengan dugaan tindak pidana pencucian uang atas hasil kejahatan tersebut. Dalam pertimbangannya, majelis hakim menilai

²⁸ Soetardi Tri Cahyono, Wina Erni, dan Taufik Hidayat, "Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia," *Dame Journal of Law* 1, no. 1 (2025): 1–23.

²⁹ Muhammad Aabid Tyas Dzaky dan Ibrahim Fikma Edrisy, "Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital," *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 2 (2025): 3614–25.

³⁰ Adinda Lola Sariyani Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia," *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 2 (2024): 69–77.

bahwa unsur kesengajaan, penyebaran berita bohong dan menyesatkan, serta adanya kerugian konsumen dalam transaksi elektronik telah terpenuhi berdasarkan alat bukti yang sah, termasuk keterangan saksi dan bukti elektronik. Putusan ini mencerminkan penerapan hukum pidana terhadap kejahatan berbasis teknologi informasi serta menegaskan komitmen peradilan dalam memberikan perlindungan hukum kepada konsumen dan menjaga kepercayaan terhadap sistem transaksi elektronik di Indonesia.

1) Substansi Hukum

- a) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
- b) Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU).
- c) Kitab Undang-Undang Hukum Pidana (KUHP): Sebagai aturan umum, digunakan sebagai alternatif jika UU khusus tidak diterapkan, seperti Pasal 378 KUHP tentang penipuan.

2) Struktur Hukum

Dalam kasus ini, struktur hukum melibatkan: a. Pengadilan Negeri Jakarta Selatan; b. Kejaksaan Negeri Jakarta Selatan; c. Kepolisian (Polda Metro Jaya).

3) Budaya Hukum

- a) Kesadaran Masyarakat terhadap Penipuan Online: Kasus ini menunjukkan budaya masyarakat yang semakin sadar akan risiko penipuan melalui media sosial, terutama di kalangan diaspora Indonesia di luar negeri (seperti Jerman). Korban membentuk grup WhatsApp untuk saling mendukung, menunjukkan nilai solidaritas dan keadilan sosial.
- b) Nilai Keadilan dan Perlindungan Konsumen: Budaya hukum menekankan perlindungan konsumen dari informasi menyesatkan, dengan fokus pada kerugian materiil (miliaran rupiah). Ini mencerminkan nilai etis bahwa penyebaran berita bohong adalah pelanggaran norma sosial, meskipun terdakwa mengaku tidak sengaja.
- c) Sikap terhadap Hukum Pidana: Masyarakat cenderung melihat hukum sebagai alat pencegah kejahatan siber, dengan tekanan pada pidana penjara dan denda sebagai deterrent. Namun, ada budaya itikad baik dalam pembelaan terdakwa,

yang mengklaim perbuatan sebagai bisnis tanpa niat jahat, menunjukkan variasi interpretasi norma hukum.

- d) Pengaruh Budaya Digital: Budaya masyarakat Indonesia yang aktif di media sosial (*Instagram, Facebook*) membuat kasus ini relevan, dengan nilai transparansi dan akuntabilitas dalam transaksi elektronik. Ini mendorong pengembangan hukum yang lebih adaptif terhadap teknologi.

b. Putusan Nomor 184/Pid.Sus/2023/PN Lgs

Perkara muncul dari pengelolaan/unggahan sebuah akun Facebook palsu bernama “Usman Udin” yang diduga menyebarkan informasi fitnah/berita bohong sehingga menimbulkan kegaduhan di masyarakat Langsa. Majelis Hakim PN Langsa pada 28 Maret 2024 menjatuhkan hukuman terhadap Fakhran (register 184) pidana penjara 1 tahun 4 bulan. terdakwa dijerat terkait pelanggaran UU ITE (terutama Pasal 27 ayat (3) jo. Pasal 45 ayat (3) UU No. 11/2008 sebagaimana diubah UU No.19/2016) yaitu menyebarkan informasi yang memuat pencemaran nama baik/fitnah lewat media elektronik. Dari pasal di atas, pengertian penyebaran berita bohong secara legal meliputi:

- a. Informasi tidak benar atau menyesatkan (hoaks),
- b. Disebarkan melalui media elektronik (mis. Internet, media sosial),
- c. Secara sengaja dan tanpa hak oleh pelaku,
- d. Menimbulkan akibat merugikan terutama pada pihak lain (mis. Konsumen atau publik).

Berdasarkan teori sistem hukum Lawrence M. Friedman, penegakan hukum terhadap tindak pidana siber dapat dianalisis melalui tiga unsur, yaitu substansi hukum, struktur hukum, dan budaya hukum. Dari aspek substansi hukum, dasar hukum yang digunakan dalam perkara ini meliputi Pasal 14 Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana jo. Pasal 55 ayat (1) ke-1 Kitab Undang-Undang Hukum Pidana (KUHP), serta ketentuan mengenai perbuatan dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang mengandung penghinaan atau pencemaran nama baik sebagaimana diatur dalam Pasal 27 ayat (3) jo. Pasal 45 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), jo. Pasal 55 ayat (1) ke-1 KUHP dan Pasal 65 ayat (1) KUHP.

Aspek struktur hukum, proses penegakan hukum melibatkan berbagai lembaga, yaitu Kepolisian sebagai penyidik, Kejaksaan Negeri Langsa sebagai penuntut umum, dan

Pengadilan Negeri Langsa sebagai lembaga yang memeriksa dan memutus perkara. Sementara itu, dari aspek budaya hukum, salah satu tantangan utama dalam penanggulangan kejahatan siber adalah masih rendahnya tingkat literasi digital dan kesadaran hukum masyarakat terhadap ketentuan UU ITE. Selain itu, perkembangan globalisasi digital menyebabkan norma-norma hukum yang sebelumnya berlaku dalam ruang konvensional belum sepenuhnya terinternalisasi dalam aktivitas masyarakat di ruang digital. Akibatnya, masih banyak pengguna media sosial yang belum menyadari bahwa unggahan, komentar, atau penyebaran konten yang bersifat penghinaan, pencemaran nama baik, maupun fitnah dapat menimbulkan konsekuensi hukum dan memenuhi unsur tindak pidana sebagaimana diatur dalam Pasal 27 ayat (3) UU ITE.

D. Kesimpulan

1. Simpulan

Perkembangan teknologi informasi telah membawa dampak positif dalam berbagai aspek kehidupan, tetapi juga memicu peningkatan kejahatan ekonomi berbasis digital. Kejahatan ini meliputi berbagai bentuk pelanggaran, seperti penipuan online, pencurian data pribadi, dan pencucian uang melalui jaringan internet, yang semakin meningkat sejalan dengan semakin besarnya peran internet dalam kehidupan sehari-hari. Peraturan perundang-undangan terkait kejahatan siber telah berkembang pesat di berbagai negara belahan dunia. Di Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) menjadi dasar utama, yang diperkuat oleh peraturan turunan seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Tantangan Implementasi di Lapangan Meskipun undang-undang ini cukup komprehensif, Putusan Pengadilan Negeri Jakarta Selatan Nomor 95/Pid.Sus/2024/PN JKT.SEL berkaitan dengan tindak pidana penyebaran informasi bohong dan menyesatkan dalam transaksi elektronik. Lalu Putusan Nomor 184/Pid.Sus/2023/PN Lgs Perkara muncul dari pengelolaan/unggahan sebuah akun Facebook palsu menyebarkan informasi fitnah/berita bohong. Budaya masyarakat Indonesia yang aktif di media sosial (Instagram, Facebook) membuat kasus ini relevan, dengan nilai transparansi dan akuntabilitas dalam transaksi elektronik. Ini mendorong pengembangan hukum yang lebih adaptif terhadap teknologi.

2. Saran

Mendorong peningkatan literasi dan etika digital masyarakat agar lebih waspada terhadap penipuan dan penyalahgunaan teknologi, sekaligus menekankan peran negara dalam memperkuat regulasi yang adil dan tidak multitafsir, meningkatkan kapasitas aparat penegak hukum di bidang forensik digital.

Perlu adanya pembangunan sistem perlindungan data dan mekanisme pelaporan yang efektif guna menjamin keamanan ruang digital dan perlindungan hak asasi manusia.

Daftar Pustaka

- Ajamalus, H, dan Agung Cucu Purnawirawan. “Perkembangan Hukum Cyber di Indonesia: Tantangan dan Peluang.” *Bulletin of Community Engagement* 4, no. 3 (2024): 109–16.
- Aprilianti, Astri. “Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi” 15 (2024).
- Arafah, Rasya, dan Irwan Triadi. “Analisis Peran Hukum Internasional Dalam Mencegah Perdagangan Manusia Di Indonesia.” *Media Hukum Indonesia (MHI)* 3, no. 3 (2025).
- Arafat, Muhammad, dan Alexander Tito Enggar Wirasto. “Kebijakan kriminal dalam penanganan siber di era digital: Studi kasus di Indonesia.” *Equality: Journal of Law and Justice* 1, no. 2 (2024): 220–41.
- Arkhan, Muhammad, Maulana Bastian, Rudy Sutanto, dan Raden Ruli Basuni. “Evaluasi Efektivitas Undang-Undang No . 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik dalam Pencegahan Cyberterrorism Evaluation of the Effectiveness of Law No . 1 of 2024 on Information and Electronic Transactions in Preventing Cyberterrorism” 5681, no. 2 (2024): 430–43.
- Budiman, Eren Arif, dan M H SH. “Literasi Hukum Digital Di Tingkat Masyarakat.” *Transformasi Hukum* 47 (2025).
- Cahyono, Soetardi Tri, Wina Erni, dan Taufik Hidayat. “Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia.” *Dame Journal of Law* 1, no. 1 (2025): 1–23.
- Chandra, Jansen, Vincent Tanaka, dan Ricky Banke. “Peran Interpol dalam Menangani dan Menanggulangi Kejahatan Siber di Indonesia.” *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora* 4, no. 3 (2025): 4710–19.
- Dinda, Adinda Lola Sariani. “Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia.” *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 2 (2024): 69–77.
- Dzaky, Muhammad Aabid Tyas, dan Ibrahim Fikma Edrisy. “Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital.” *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 2 (2025): 3614–25.
- Fatimah, Sitti, dan Ludfi Ludfi. “Navigasi Hukum Di Era Fintech Syariah: Tinjauan Literatur Dan Regulasi.” *IDEALITA: Jurnal Pendidikan Dan Sosial Keagamaan* 4, no. 1 (2024): 41–52.
- Hasan, Zainudin, dan Ahmad Mahardika. “Peranan Cyber Law Dalam Penanganan Tindak Pidana” 2, no. 5 (2024): 337–45.
- Kawisen, Heryanto, Rafael Agrerio Firera, Alpon Siyus, dan Pelagia Melati. “Analisis efektivitas dan tantangan hukum internasional dalam penanggulangan kejahatan siber lintas negara secara global.” *JATI (Jurnal Mahasiswa Teknik Informatika)* 9, no. 5

- (2025): 8613–18.
- Khairunnisa, Puteri Ananda, Norul Annisa, dan Jadianan Parhusip. “Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia.” *Teknik: Jurnal Ilmu Teknik Dan Informatika* 4, no. 2 (2024): 9–16.
- Laksito, Joni, Maulana Fahmi Idris, dan Agus Waryanto. “Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif.” *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 4 (2024): 774–90.
- Markus, Novita Alfiani, dan Hanita 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” 2, no. 10 (2023): 3799–3806.
- Maulidya, Erine Nur, Angga Natalia, Iin Yulianti, dan Muhammad Havez. “Strategi Penanggulangan Informasi Hoax dan Terorisme di Media Sosial Oleh Unit Polisi Virtual Provinsi Lampung.” *Jurnal Dakwah dan Komunikasi* 8, no. 1 (2023): 139–56.
- Muhammad, Ilham, dan Akbar Muhammad. “Pelaku Penyebaran Data Pribadi Yang Tersimpan Pada Barcode Ditinjau Dari Undang-Undang Informasi Transaksi,” 2024, 43–52. <https://doi.org/10.47709/ijbl.v3i1.4281>.
- Munajat, Andi Ahmad, dan Hudi Yusuf. “Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus : Studi Tentang Kejahatan Keuangan Berbasis Digital The Role of Information Technology in the Prevention and Disclosure of Special Economic Crimes : A Study of Digital-Based Financial Crimes,” no. November (2024): 4853–65.
- Pramudya, Deva Wira, dan Hudi Yusuf. “Anatomi kriminal siber: motif, modus, dan penanggulangannya dari perspektif kriminologi.” *Jurnal Intelek Insan Cendikia* 2, no. 8 (2025): 14613–23.
- Rahakbauw, Isro’Kurniawan, dan Ika Arini Batubara. “Analisis Potensi Ancaman Siber pada Bidang Ekonomi di Indonesia.” *Jurnal Kajian Strategik Ketahanan Nasional* 7, no. 1 (2024): 5.
- Rahayuningsih, Uut, dan Bayu Prasetyo. “Sosialisasi Pembuktian Cyber Crime dalam KUHAP dan UU ITE” 4, no. 3 (2025): 649–58.
- Sari, Jayanti Armida, dan Bambang Agus Diana. “Dampak Transformasi Digitalisasi terhadap Perubahan Perilaku Masyarakat Pedesaan.” *Jurnal Pemerintahan dan Politik* 9, no. 2 (2024): 88–96.
- Suci, Indah Meisyana, Achmad Hanif Avicenna, Sekar Marchayu Setiawan, dan Rheyna Wisnu. “Perlindungan Hak Kekayaan Intelektual Di Era Digital Melalui Undang-Undang Informasi Dan Transaksi Elektronik (Uu Ite),” n.d.
- Susilowati, Dwi Erna, Muhammad Muhtarom, dan Amir Junaidi. “Analisis yuridis keabsahan tanda tangan digital dalam transaksi e-commerce di Indonesia.” *Jurnal Penelitian Serambi Hukum* 18, no. 01 (2025): 17–26.
- Syahrir, Mukum. “Efektivitas Hukuman bagi Pelaku Kejahatan Siber di Indonesia: Analisis Kriminologi dengan Metode Content Analysis.” *Perkara: Jurnal Ilmu Hukum dan Politik* 3, no. 1 (2025): 694–711.
- Wibowo, Muhammad Singgih Imam, dan Akhmad Munawar. “Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia.” *Jurnal Hukum Lex Generalis* 5, no. 7 (2024).
- Widjaja, Gunawan. “Penyesuaian Hukum Nasional Indonesia Terhadap Konvensi Pbb Anti-Kejahatan Siber 2024: Kajian Pustaka Tentang Harmonisasi Uu Ite Dan Kuhp Untuk Penguatan Penanganan Kejahatan Siber Lintas Negara.” *NETIZEN: JOURNAL OF SOCIETY AND BUSSINESS* 1, no. 11 (2025): 611–21.

Yamani, Akhmad Zaki. “Analisis Tantangan Dalam Penyusunan Rancangan Undang-Undang Di Era Transformasi Digital: Antara Regulasi, Inovasi, Dan Perlindungan Hak.” *Journal Of Law And Nation* 4, no. 2 (2025): 312–24.