



Kajian Yuridis Normatif terhadap Pengaturan Tindak Pidana Siber dalam Undang-Undang Informasi dan Transaksi Elektronik di Indonesia

Windi Audina

Ilmu Hukum, Universitas Terbuka, Indonesia

Email Korespondensi: 049803107@ecampus.ut.ac.id

Article received: 01 Januari 2026, Review process: 12 Januari 2026

Article Accepted: 22 Februari 2026, Article published: 21 April 2026

ABSTRACT

The rapid development of information technology has given rise to increasingly complex forms of cybercrime in Indonesia. The Electronic Information and Transactions Law (ITE Law), as the primary legal instrument for combating cybercrime, continues to experience dynamics through regulatory changes, most recently through Law Number 1 of 2024. This study aims to analyze the normative legal provisions of cybercrime in the ITE Law and to examine the consistency and harmonization of norms in ensuring legal certainty. The research method used is a normative legal approach with literature review techniques, through regulatory, conceptual, and historical approaches to the ITE Law, the National Criminal Code, and the Personal Data Protection Law. The results of the study indicate that constructively, the regulation of cybercrime in the ITE Law has been improved through the addition of new norms, strengthening of electronic evidence, and expanding the authority of law enforcement. However, normative weaknesses remain in the form of multi-interpretable norms, overlapping regulations with the Criminal Code and the Personal Data Protection Law, and the existence of transitional provisions that have the potential to create legal ambiguities. Limited institutional capacity and challenges in digital evidence also affect the effectiveness of law enforcement. Therefore, comprehensive regulatory harmonization and strengthening the capacity of law enforcement officials are needed to ensure legal certainty, justice, and expediency in combating cybercrime in Indonesia.

Keywords: *Legal harmonization; normative juridical studies; legal certainty; cybercrime; ITE Law.*

ABSTRAK

Perkembangan teknologi informasi yang pesat telah melahirkan berbagai bentuk tindak pidana siber yang semakin kompleks di Indonesia. Keberadaan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai instrumen hukum utama dalam penanggulangan cybercrime terus mengalami dinamika melalui perubahan regulasi, terakhir melalui Undang-Undang Nomor 1 Tahun 2024. Penelitian ini bertujuan untuk menganalisis secara yuridis normatif pengaturan tindak pidana siber dalam UU ITE serta mengkaji konsistensi dan harmonisasi norma dalam menjamin kepastian hukum. Metode penelitian yang digunakan adalah pendekatan yuridis normatif dengan teknik studi kepustakaan, melalui pendekatan perundang-undangan, konseptual, dan historis terhadap UU ITE, KUHP Nasional, dan UU Perlindungan Data Pribadi. Hasil penelitian menunjukkan bahwa secara konstruktif, pengaturan tindak pidana siber dalam UU ITE telah mengalami penyempurnaan melalui penambahan norma baru, penguatan alat bukti elektronik, serta perluasan kewenangan penegak hukum. Namun masih terdapat kelemahan

normatif berupa multitafsir norma, tumpang tindih pengaturan dengan KUHP dan UU PDP, serta adanya ketentuan transisi (sunset clause) yang berpotensi menimbulkan ketidakpastian hukum. Keterbatasan kapasitas kelembagaan dan tantangan pembuktian digital turut mempengaruhi efektivitas penegakan hukum. Dengan demikian, diperlukan harmonisasi regulasi secara komprehensif dan penguatan kapasitas aparat penegak hukum guna mewujudkan kepastian hukum, keadilan, dan kemanfaatan dalam penanggulangan tindak pidana siber di Indonesia.

Kata Kunci: Harmonisasi hukum; kajian yuridis normatif; kepastian hukum; tindak pidana siber; UU ITE.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang berlangsung secara masif dalam dua dekade terakhir telah membawa transformasi mendalam pada hampir seluruh sendi kehidupan masyarakat Indonesia. Transformasi tersebut tidak hanya menghadirkan kemudahan dalam mengakses informasi, melakukan transaksi ekonomi, dan menjalin komunikasi lintas batas, tetapi juga memunculkan dimensi baru dalam dunia kejahatan yang dikenal dengan istilah *cybercrime* atau tindak pidana siber. Fenomena ini berkembang seiring dengan meningkatnya penetrasi internet di Indonesia, di mana pengguna aktif internet nasional terus mengalami pertumbuhan signifikan dari tahun ke tahun. Kondisi demikian menciptakan medan yang subur bagi para pelaku kejahatan untuk memanfaatkan celah-celah teknologi sebagai instrumen perbuatan melawan hukum, mulai dari penipuan daring, penyebaran informasi palsu (*hoaks*), ujaran kebencian, pencemaran nama baik melalui media sosial, hingga peretasan sistem elektronik dan pencurian data pribadi. Modus operandi kejahatan siber pun terus berevolusi mengikuti perkembangan teknologi, sehingga upaya pencegahan dan penindakan hukum kerap tertinggal di belakang laju inovasi kejahatan itu sendiri (Pansariadi & Soekorini, 2023).

Respons negara terhadap fenomena tersebut diwujudkan melalui pembentukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diubah pertama kali melalui Undang-Undang Nomor 19 Tahun 2016, dan yang paling mutakhir diubah kembali melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Perubahan kedua ini hadir dengan tujuan untuk menjaga ruang digital Indonesia agar lebih bersih, sehat, beretika, produktif, dan berkeadilan, serta memberikan kejelasan terhadap pasal-pasal yang selama ini menimbulkan multitafsir dan kontroversi di tengah Masyarakat. Secara substansial, UU No. 1 Tahun 2024 menambahkan tujuh pasal baru, meliputi Pasal 13A, 16A, 16B, 18A, 27A, 27B, dan 40A, serta mempertegas kewenangan penyidik dalam melakukan intervensi terhadap akun media sosial dan aset digital yang berkaitan dengan proses penyidikan. Namun demikian, berbagai kalangan akademisi, praktisi hukum, dan organisasi masyarakat sipil menilai bahwa revisi tersebut masih menyisakan sejumlah persoalan normatif yang belum tuntas diselesaikan.

Data empiris menunjukkan bahwa tren kejahatan siber di Indonesia terus mengalami peningkatan yang cukup mengkhawatirkan. Berdasarkan laporan

Direktorat Tindak Pidana Siber Bareskrim Polri, tercatat sebanyak 4.250 kasus pada tahun 2020, meningkat menjadi 5.126 kasus pada tahun 2021, kemudian 5.681 kasus pada tahun 2022, hingga mencapai sekitar 6.100 kasus pada tahun 2023. Bentuk kejahatan yang dilaporkan mencakup penipuan daring, ujaran kebencian, penyebaran *hoaks*, penghinaan di media sosial, serta penyalahgunaan data pribadi (Santoso et al., 2024). Lonjakan angka tersebut mengindikasikan bahwa kerangka hukum yang ada belum mampu memberikan efek jera yang memadai bagi pelaku, sekaligus mencerminkan adanya kelemahan struktural dalam penegakan hukum tindak pidana siber di Indonesia.

Dalam perspektif kajian yuridis normatif, pengaturan tindak pidana siber dalam UU ITE menghadapi berbagai problematika yang bersifat mendasar. Pertama, sejumlah pasal dalam undang-undang ini dinilai masih bersifat *rubberstamp* atau multitafsir, sehingga membuka peluang bagi penegak hukum untuk menggunakannya secara subyektif terhadap pihak tertentu (Djarawula et al., 2023). Kedua, terdapat tumpang tindih norma antara ketentuan dalam UU ITE dengan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang baru sebagaimana diatur dalam Undang-Undang Nomor 1 Tahun 2023, sehingga menimbulkan ketidakpastian dalam interpretasi hukum dan berpotensi menghambat proses penegakan hukum yang konsisten dan proporsional. Ketiga, lemahnya instrumen pembuktian dalam kasus-kasus kejahatan siber yang bersifat teknis dan lintas yurisdiksi turut menjadi hambatan serius dalam penegakan hukum. Kondisi ini mempertegas urgensi dilakukannya kajian yuridis normatif yang mendalam terhadap pengaturan tindak pidana siber dalam UU ITE (Djibu, 2025).

Sejumlah penelitian terdahulu telah memberikan kontribusi penting dalam memetakan permasalahan ini. Mengkaji *cybercrime* di Indonesia dalam perspektif UU Nomor 11 Tahun 2008 secara deskriptif-analitis, dengan temuan bahwa regulasi yang ada belum sepenuhnya mampu menjangkau bentuk-bentuk kejahatan siber yang terus berkembang. Sementara itu, meneliti tindak pidana *cybercrime* dan penegakan hukumnya dengan menyoroti masalah koordinasi antarinstansi penegak hukum yang dinilai masih lemah. Mengkaji kebijakan hukum pidana terhadap perbuatan melawan hukum dalam UU ITE pasca berlakunya Pedoman Implementasi, dengan kesimpulan bahwa pedoman tersebut berperan dalam mengatasi ketidakpastian penafsiran hukum, meskipun masih memerlukan penguatan lebih lanjut. Secara khusus menganalisis implikasi hukum Pasal 27A UU No. 1 Tahun 2024 terhadap kebebasan berekspresi dan penegakan hukum di ranah siber, dengan menggunakan pendekatan hukum normatif yang mengacu pada peraturan perundang-undangan yang berlaku (Munir, 2024).

Meskipun demikian, terdapat *gap* penelitian yang signifikan dalam kajian-kajian tersebut. Sebagian besar penelitian terdahulu memfokuskan pembahasannya pada satu jenis tindak pidana siber tertentu, misalnya pencemaran nama baik, penipuan daring, atau peretasan sistem elektronik, tanpa mengkajinya secara holistik dalam kerangka pengaturan yang komprehensif. Selain itu, kajian yang secara spesifik menganalisis implikasi yuridis normatif dari keseluruhan perubahan substansial dalam UU No. 1 Tahun 2024 terhadap konstruksi tindak pidana siber termasuk relevansinya dengan KUHP baru dan Undang-Undang Perlindungan Data

Pribadi (UU PDP) Nomor 27 Tahun 2022 masih sangat terbatas. Di samping itu, belum terdapat penelitian yang secara eksplisit menganalisis keterkaitan antara kelemahan normatif dalam UU ITE dengan konsistensi putusan pengadilan dalam menangani perkara tindak pidana siber. Kesenjangan inilah yang menjadi pijakan *novelty* dari penelitian ini (Aini & Lubis, 2024).

Kebaruan penelitian ini terletak pada analisis yuridis normatif yang bersifat integratif terhadap pengaturan tindak pidana siber dalam UU ITE pasca perubahan kedua melalui UU No. 1 Tahun 2024, dengan mengkaji secara simultan harmonisasinya terhadap KUHP Nasional 2023 dan UU PDP 2022. Pendekatan ini memungkinkan identifikasi secara sistematis terhadap kelemahan normatif, potensi disharmoni regulasi, serta rekonstruksi konseptual atas prinsip kepastian hukum dan keadilan dalam penegakan hukum tindak pidana siber di Indonesia sesuatu yang belum pernah dilakukan secara komprehensif dalam penelitian-penelitian sebelumnya.

Berdasarkan uraian latar belakang tersebut, penelitian ini merumuskan dua permasalahan pokok sebagai berikut: pertama, bagaimana pengaturan tindak pidana siber dalam Undang-Undang Informasi dan Transaksi Elektronik dilihat dari perspektif kajian yuridis normatif?; dan kedua, sejauh mana konsistensi dan harmonisasi norma dalam UU ITE pasca perubahan kedua dapat menjamin kepastian hukum dalam penegakan tindak pidana siber di Indonesia? Secara umum, penelitian ini bertujuan untuk menganalisis secara mendalam konstruksi yuridis pengaturan tindak pidana siber dalam UU ITE dan implikasinya terhadap kepastian hukum dalam sistem hukum pidana Indonesia. Secara khusus, penelitian ini dimaksudkan untuk mengidentifikasi kelemahan normatif yang masih terdapat dalam UU ITE pasca perubahan kedua serta merumuskan rekomendasi akademis bagi penyempurnaan regulasi siber yang lebih adaptif dan berkeadilan. Manfaat teoretis penelitian ini adalah memberikan sumbangan ilmiah bagi pengembangan ilmu hukum pidana, khususnya di bidang *cyber law*, sedangkan manfaat praktisnya adalah menjadi referensi bagi pembentuk kebijakan, penegak hukum, dan masyarakat dalam memahami dan menerapkan ketentuan hukum tindak pidana siber secara tepat dan proporsional.

METODE

Penelitian ini menggunakan pendekatan yuridis normatif (*normative legal research*) dengan metode *library research* atau studi kepustakaan sebagai landasan metodologisnya. Pendekatan yuridis normatif dipilih karena penelitian ini berfokus pada analisis terhadap norma-norma hukum positif yang tertuang dalam peraturan perundang-undangan, doktrin hukum, serta literatur ilmiah yang relevan, tanpa melibatkan pengumpulan data empiris di lapangan secara langsung (Marzuki, 2021; Widiarty, 2024). Dua regulasi utama yang menjadi objek kajian dalam penelitian ini adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah kedua kalinya melalui Undang-Undang Nomor 1 Tahun 2024, serta Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) Nasional. Kedua regulasi ini dikaji secara komparatif dan sinkronisatif guna mengidentifikasi potensi disharmoni norma,

celah pengaturan (*legal gap*), serta konsistensi konstruksi delik tindak pidana siber dalam sistem hukum pidana Indonesia. Sumber bahan hukum yang digunakan meliputi bahan hukum primer berupa kedua regulasi tersebut beserta peraturan pelaksanaannya, bahan hukum sekunder berupa jurnal ilmiah, hasil penelitian terdahulu, dan doktrin hukum dari para ahli, serta bahan hukum tersier berupa kamus hukum dan ensiklopedia. Seluruh bahan hukum dikumpulkan, diklasifikasikan, dan dianalisis secara sistematis menggunakan teknik deskriptif-analitis (Santoso et al., 2024).

Analisis dalam penelitian ini dilakukan melalui tiga pendekatan yang saling melengkapi, yakni pendekatan perundang-undangan (*statute approach*) untuk menelaah substansi normatif kedua regulasi yang dikaji, pendekatan konseptual (*conceptual approach*) untuk menggali konstruksi teoritis terkait prinsip kepastian hukum dan keadilan dalam konteks *cybercrime*, serta pendekatan historis (*historical approach*) untuk memahami dinamika perkembangan pengaturan tindak pidana siber di Indonesia sejak awal pembentukan UU ITE hingga perubahan keduanya (Djulaeka & Rahayu, 2020). Data kepustakaan yang terkumpul kemudian dianalisis secara kualitatif dengan menggunakan logika deduktif, yakni berangkat dari prinsip-prinsip hukum umum menuju kesimpulan khusus terkait konstruksi pengaturan tindak pidana siber. Pendekatan ini sejalan dengan karakter penelitian hukum normatif yang menempatkan norma sebagai entitas utama yang diteliti, bukan perilaku sosial secara empiric (Primadhany et al., 2025). Hasil analisis selanjutnya diinterpretasikan secara kritis untuk menghasilkan rekomendasi akademis bagi penyempurnaan regulasi siber yang lebih adaptif, harmonis, dan berkeadilan dalam sistem hukum nasional Indonesia (Pansariadi & Soekorini, 2023).

HASIL DAN PEMBAHASAN

Konstruksi Yuridis Pengaturan Tindak Pidana Siber dalam Undang-Undang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan respons legislatif terhadap dinamika kejahatan digital yang terus berkembang di Indonesia. Secara konstruktif, undang-undang ini memuat sejumlah perbuatan yang dikualifikasikan sebagai tindak pidana siber, di antaranya penyebaran konten asusila melalui Pasal 27 ayat (1), penyebaran informasi bohong yang merugikan konsumen dalam transaksi elektronik sebagaimana Pasal 28 ayat (1), serta penyebaran ujaran kebencian berbasis SARA dalam Pasal 28 ayat (2). Perubahan kedua ini turut menambahkan Pasal 27A yang mengatur serangan terhadap kehormatan atau nama baik secara elektronik, dan Pasal 27B yang mengatur pemerasan berbasis informasi elektronik. Konstruksi delik dalam pasal-pasal tersebut menggunakan pendekatan *actus reus* yang mensyaratkan perbuatan yang dilakukan dengan sengaja dan tanpa hak, sejalan dengan prinsip dasar hukum pidana yang mensyaratkan adanya unsur *mens rea* dan *actus reus* sebagai fondasi pertanggungjawaban pidana (Yudistira & Ramadani, 2023).

Dalam praktik penegakan hukum, konstruksi delik dalam UU ITE kerap bersinggungan dengan ketentuan dalam Kitab Undang-Undang Hukum Pidana

Nasional (UU No. 1 Tahun 2023). Hal ini terlihat dari kenyataan bahwa Pasal II UU No. 1 Tahun 2024 secara eksplisit menegaskan bahwa sejumlah pasal pidana di dalamnya hanya berlaku sampai dengan diberlakukannya UU No. 1 Tahun 2023 tentang KUHP. Artinya, terdapat *sunset clause* yang menciptakan kondisi transisi normatif yang berpotensi menimbulkan kerancuan dalam penerapan hukum. Aspek penting lainnya adalah kedudukan alat bukti elektronik sebagaimana diatur dalam Pasal 5 UU No. 1 Tahun 2024, yang menegaskan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti hukum yang sah sebagai perluasan dari alat bukti konvensional. Hal ini menjadi dasar yuridis bagi aparat penegak hukum dalam memproses perkara tindak pidana siber di pengadilan, meskipun dalam tataran praktis pembuktian digital masih menghadapi berbagai hambatan teknis (Zhafira et al., 2023).

Ketentuan pidana dalam UU ITE mengalami penyesuaian yang cukup signifikan melalui perubahan kedua ini. Pasal 45 UU No. 1 Tahun 2024 memuat ancaman pidana yang bervariasi sesuai jenis pelanggarannya, mulai dari pidana penjara paling lama 2 tahun dan denda Rp400.000.000,00 untuk pelanggaran Pasal 27A, hingga pidana penjara paling lama 10 tahun dan denda Rp10.000.000.000,00 untuk pelanggaran muatan perjudian. Gradasi sanksi ini mencerminkan kehendak pembentuk undang-undang untuk menerapkan prinsip *proportionality* dalam penjatuhan pidana. Terhadap Putusan Pengadilan Negeri Ternate Nomor 155/Pid.Sus/2024/PN.Tte menunjukkan bahwa konstruksi delik dalam Pasal 27A telah diterapkan secara konkret oleh hakim dengan penjatuhan pidana penjara 6 bulan disertai denda, yang mencerminkan pemenuhan unsur-unsur delik secara kumulatif dalam praktik peradilan (Aulia et al., 2026).

Dimensi kelembagaan dalam penegakan hukum tindak pidana siber juga dipertegas melalui Pasal 43 UU No. 1 Tahun 2024, yang memperluas kewenangan penyidik termasuk kewenangan memerintahkan pemutusan akses terhadap akun media sosial, rekening bank, uang elektronik, dan aset digital. Penguatan kewenangan ini relevan mengingat bahwa selama ini hambatan terbesar dalam penegakan hukum siber bersumber dari keterbatasan kapasitas teknis penyidik dan lemahnya koordinasi antarinstansi. Secara politik hukum, perluasan kewenangan penyidik ini merupakan wujud nyata dari transformasi *cyber law* Indonesia yang terus beradaptasi dengan perkembangan kejahatan digital, sekalipun masih memerlukan pengaturan teknis lebih lanjut melalui regulasi pelaksana guna memastikan penerapannya tidak berbenturan dengan prinsip-prinsip hak asasi manusia (Zamayya et al., 2025).

Aspek perlindungan anak dalam ruang digital yang diatur melalui Pasal 16A UU No. 1 Tahun 2024 merupakan salah satu materi baru yang tidak dijumpai dalam versi undang-undang sebelumnya. Pasal tersebut mewajibkan setiap Penyelenggara Sistem Elektronik untuk memberikan perlindungan bagi anak yang menggunakan atau mengakses sistem elektronik, termasuk kewajiban menyediakan mekanisme verifikasi usia, mekanisme pelaporan penyalahgunaan, serta penerapan teknologi perlindungan sejak tahap pengembangan hingga penyelenggaraan sistem. Ketentuan ini mencerminkan kesadaran pembentuk undang-undang bahwa anak-anak merupakan kelompok rentan yang memerlukan perlindungan khusus dalam

ekosistem digital. Namun demikian, efektivitas implementasi ketentuan ini sangat bergantung pada kapasitas teknis dan komitmen para penyelenggara sistem elektronik, yang dalam praktiknya masih sangat bervariasi (Sahlepi, 2023). Tanpa mekanisme pengawasan yang ketat dan sanksi yang proporsional, ketentuan perlindungan anak ini berisiko hanya menjadi norma deklaratif yang tidak memiliki daya paksa yang memadai dalam tataran implementasi.

Dimensi internasional dari pengaturan tindak pidana siber dalam UU ITE juga patut mendapat perhatian serius. Pasal 43 ayat (8) UU No. 1 Tahun 2024 secara eksplisit membuka ruang bagi kerja sama penyidik Indonesia dengan penyidik negara lain dalam rangka berbagi informasi dan alat bukti guna mengungkap tindak pidana siber lintas yurisdiksi. Ketentuan ini sangat relevan mengingat karakteristik *cybercrime* yang bersifat *borderless* dan kerap melibatkan pelaku atau infrastruktur yang berdomisili di luar wilayah Indonesia. Dalam kajiannya tentang implikasi *The United Nations Convention Against Cybercrime* menegaskan bahwa harmonisasi definisi tindak pidana siber, prosedur penegakan hukum lintas negara, serta mekanisme kerja sama internasional merupakan kebutuhan mendesak yang harus diakomodasi dalam kerangka hukum nasional. Akan tetapi, ketentuan kerja sama internasional dalam UU ITE masih bersifat umum dan belum dilengkapi dengan mekanisme teknis yang operasional, sehingga memerlukan penguatan melalui perjanjian bilateral maupun instrumen hukum internasional yang lebih spesifik.

Aspek pencegahan tindak pidana siber melalui pendekatan non-penal juga menjadi bagian yang tidak terpisahkan dari konstruksi yuridis UU ITE secara keseluruhan. Pasal 40A UU No. 1 Tahun 2024 menegaskan tanggung jawab pemerintah dalam mendorong terciptanya ekosistem digital yang adil, akuntabel, aman, dan inovatif, termasuk kewenangan pemerintah untuk memerintahkan penyesuaian pada sistem elektronik dan melakukan tindakan tertentu guna melindungi kepentingan masyarakat. Ketentuan ini menempatkan pemerintah tidak sekadar sebagai aktor penegak hukum yang bersifat reaktif, melainkan juga sebagai fasilitator aktif dalam pembentukan tata kelola digital yang bertanggung jawab. Peran garda terdepan dalam pencegahan kejahatan siber, termasuk oleh aparat kepolisian tingkat desa, masih belum optimal akibat keterbatasan keterampilan teknis dan minimnya dukungan sumber daya yang memadai. Oleh sebab itu, penguatan kapasitas pencegahan melalui edukasi digital dan pemberdayaan masyarakat harus menjadi bagian integral dari strategi penanggulangan tindak pidana siber yang komprehensif.

Konsistensi dan Harmonisasi Norma UU ITE Pasca Perubahan Kedua dalam Menjamin Kepastian Hukum

Persoalan harmonisasi norma antara UU ITE dan regulasi terkait menjadi isu krusial yang belum sepenuhnya terselesaikan melalui perubahan kedua ini. Salah satu indikator ketidakharmonisan paling nyata adalah keberadaan *sunset clause* dalam Pasal II UU No. 1 Tahun 2024, yang menetapkan bahwa sejumlah pasal pidana dalam UU ITE hanya berlaku sampai mulai berlakunya KUHP Nasional. Kondisi transisi normatif ini berpotensi menciptakan *legal gap* yang membingungkan aparat penegak hukum dan masyarakat, terutama terkait pasal-pasal yang memiliki

padanan dalam KUHP baru namun dengan rumusan delik yang berbeda. Selain itu, tumpang tindih norma antara UU ITE dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi juga belum mendapat penyelesaian yang tuntas, khususnya dalam konteks tindak pidana pencurian data dan penyalahgunaan sistem elektronik untuk mengakses data pribadi tanpa hak (Fitri, 2022).

Permasalahan multitafsir yang menjadi dasar utama dilakukannya perubahan kedua UU ITE ternyata masih menyisakan problematika normatif yang belum terpecahkan sepenuhnya. Pasal 27A yang menggantikan Pasal 27 ayat (3) lama tentang pencemaran nama baik dinilai masih bersifat ambigu karena penggunaan frasa "menyerang kehormatan atau nama baik" yang membuka ruang penafsiran berbeda-beda di kalangan penegak hukum. Dalam penelitian yang menganalisis Putusan MA Nomor 1909K/Pid.Sus/2021, ditemukan bahwa putusan hakim dalam perkara pencemaran nama baik menyimpangi beberapa poin pedoman implementasi UU ITE, mengindikasikan bahwa ketidakkonsistenan putusan pengadilan merupakan cerminan langsung dari ketidakjelasan norma dalam regulasi itu sendiri (Zhafira et al., 2023).. Hal ini secara langsung mengancam terwujudnya kepastian hukum sebagai salah satu tujuan utama pembentukan UU ITE (Nursyamsu et al., 2025).

Dalam perspektif *legal system*, ketidakharmonisan UU ITE dengan regulasi lain semakin tampak ketika dikonfrontasikan dengan ketentuan dalam UU No. 1 Tahun 2023 tentang KUHP Nasional. KUHP baru memuat sejumlah delik yang secara substansial serupa dengan ketentuan dalam UU ITE, namun dengan formulasi dan ancaman pidana yang berbeda, sehingga menciptakan potensi *disharmoni* regulasi yang membingungkan baik penegak hukum maupun masyarakat. Tentang tindak pidana penipuan *online* juga mengungkap bahwa dalam praktiknya, aparat penegak hukum kerap mengalami kebingungan dalam memilih landasan hukum yang tepat antara KUHP dan UU ITE untuk menjerat pelaku kejahatan siber. Kondisi ini mempertegas urgensi harmonisasi menyeluruh antara kedua instrumen hukum tersebut guna menghindari inkonsistensi penuntutan dan disparitas putusan yang dapat merusak kepercayaan publik terhadap sistem peradilan pidana (Zhafira et al., 2023).

Upaya mewujudkan kepastian hukum dalam penegakan tindak pidana siber juga dipengaruhi oleh kapasitas kelembagaan penegak hukum itu sendiri. Menemukan bahwa meskipun UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mengatur sanksi pidana, efektivitasnya masih sangat rendah akibat ketidakjelasan unsur-unsur delik, disharmoni antarperaturan, serta minimnya kapasitas aparat penegak hukum dalam bidang forensik digital. Temuan ini selaras dengan hasil penelitian yang mengidentifikasi bahwa jaksa sebagai *dominus litis* dalam penuntutan perkara ITE masih menghadapi hambatan serius berupa keterbatasan SDM yang menguasai *cyber law* serta tantangan teknis dalam pengumpulan dan pembuktian bukti elektronik. Dengan demikian, pencapaian kepastian hukum tidak semata bergantung pada kualitas norma undang-undang, melainkan juga pada penguatan kapasitas kelembagaan dan harmonisasi regulasi secara menyeluruh (Silalahi et al., 2025).

Ketidakpastian hukum dalam penegakan tindak pidana siber juga tampak dari lemahnya sinergi antara UU ITE dengan regulasi perlindungan data pribadi sebagai instrumen hukum yang saling berkaitan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah mengatur sanksi pidana bagi pelaku pelanggaran data, namun belum terdapat koordinasi normatif yang jelas antara UU PDP dan UU ITE dalam konteks penanganan tindak pidana siber yang berkaitan dengan pencurian atau penyalahgunaan data pribadi secara elektronik. Kebutuhan untuk mengatasi masalah kebocoran data menjadi fokus utama yang harus segera diselesaikan, mengingat kasus-kasus kebocoran data di Indonesia terus meningkat dan menimbulkan kerugian yang sangat signifikan bagi masyarakat. Ketiadaan mekanisme koordinasi yang tegas antara dua instrumen hukum ini berpotensi menimbulkan *forum shopping* oleh aparat penegak hukum dalam menentukan dasar hukum penuntutan, yang pada akhirnya justru memperlemah kepastian hukum bagi korban maupun pelaku tindak pidana siber.

Aspek pembuktian dalam perkara tindak pidana siber merupakan salah satu dimensi yang paling kritis dalam konteks kepastian hukum. Meskipun Pasal 5 UU No. 1 Tahun 2024 telah menegaskan kedudukan informasi elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah, persoalan teknis terkait keabsahan, keutuhan, dan *chain of custody* bukti digital dalam proses peradilan masih menjadi titik lemah yang belum sepenuhnya teratasi. menegaskan bahwa jaksa sebagai penuntut umum dalam perkara ITE masih menghadapi tantangan serius dalam pengumpulan dan pembuktian bukti elektronik, yang pada gilirannya berpengaruh pada kualitas dakwaan dan keberhasilan penuntutan di persidangan. Kondisi ini diperparah oleh minimnya standar prosedur operasional yang baku dalam penanganan barang bukti digital, sehingga tidak jarang ditemukan putusan pengadilan yang tidak konsisten dalam menilai keabsahan alat bukti elektronik yang diajukan oleh penuntut umum.

Politik hukum pembentukan dan perubahan UU ITE sejak awal pembentukannya pada tahun 2008 hingga perubahan keduanya pada tahun 2024 mencerminkan dinamika tarik-menarik antara kepentingan perlindungan individu, kebebasan berekspresi, dan kepentingan keamanan negara dalam ruang digital. Perubahan-perubahan dalam *cyber law* Indonesia sangat dipengaruhi oleh dinamika politik hukum yang menjadi kebijakan dasar dalam menentukan arah, bentuk, dan isi hukum yang dibentuk sesuai kebutuhan negara pada masa berlakunya undang-undang tersebut. Realitas ini menjelaskan mengapa sejumlah pasal dalam UU ITE yang dinilai bermasalah oleh masyarakat sipil dan akademisi justru dipertahankan meskipun telah direvisi, karena pertimbangan politik tidak selalu selaras dengan tuntutan kepastian hukum dan perlindungan hak asasi manusia. Untuk menjamin efektivitas UU ITE sebagai instrumen hukum siber, diperlukan reformasi hukum yang berkelanjutan yang tidak hanya berfokus pada aspek normatif tekstual, tetapi juga mencakup dimensi sosiologis dan filosofis guna memastikan bahwa regulasi yang terbentuk benar-benar mencerminkan keadilan, kemanfaatan, dan kepastian hukum yang hakiki bagi seluruh lapisan masyarakat Indonesia.

Keterbatasan Penelitian

Penelitian ini dilaksanakan dengan menggunakan pendekatan yuridis normatif yang sepenuhnya bertumpu pada analisis bahan hukum sekunder berupa peraturan perundang-undangan, jurnal ilmiah, dan dokumen hukum yang tersedia secara kepustakaan. Konsekuensi metodologis dari pilihan pendekatan ini adalah tidak diperolehnya data empiris primer yang bersumber dari lapangan, seperti wawancara mendalam dengan aparat penegak hukum, jaksa, hakim, maupun korban tindak pidana siber. Ketiadaan data lapangan tersebut menjadikan analisis dalam penelitian ini terbatas pada dimensi normatif dan tekstual, sehingga belum mampu menggambarkan secara utuh realitas implementasi UU ITE dalam praktik penegakan hukum sehari-hari di tingkat pengadilan maupun penyidikan. Selain itu, cakupan regulasi yang dikaji dibatasi pada dua instrumen utama, yakni UU No. 1 Tahun 2024 dan UU No. 1 Tahun 2023 tentang KUHP Nasional, sehingga dimensi komparatif dengan regulasi *cybercrime* di negara-negara lain belum dapat dianalisis secara mendalam dalam penelitian ini (Altansa & Rahmat, 2024).

Keterbatasan kedua berkaitan dengan ketersediaan sumber referensi yang secara spesifik mengkaji implementasi pasal-pasal baru dalam UU No. 1 Tahun 2024 melalui putusan pengadilan yang telah berkekuatan hukum tetap. Mengingat undang-undang tersebut baru disahkan pada 2 Januari 2024, jumlah putusan pengadilan yang menggunakan pasal-pasal hasil perubahan kedua sebagai dasar penghukuman masih sangat terbatas pada saat penelitian ini dilakukan, sehingga analisis yurisprudensial belum dapat dilakukan secara komprehensif (Aprilianti, 2024).

SIMPULAN

Berdasarkan hasil analisis yuridis normatif yang telah dilakukan, penelitian ini menghasilkan dua kesimpulan pokok. Pertama, pengaturan tindak pidana siber dalam UU ITE pasca perubahan kedua melalui UU No. 1 Tahun 2024 secara konstruktif telah mengalami penyempurnaan substantif yang mencakup penambahan tujuh pasal baru, reformulasi delik pencemaran nama baik melalui Pasal 27A, penegasan kedudukan alat bukti elektronik, perluasan kewenangan penyidik, serta penguatan perlindungan bagi anak dalam ruang digital. Konstruksi delik dalam regulasi ini pada dasarnya telah merespons kebutuhan hukum di era digital, namun sejumlah pasal masih bersifat multitafsir dan berpotensi disalahgunakan sebagai instrumen kriminalisasi terhadap kebebasan berekspresi. Kedua, konsistensi dan harmonisasi norma dalam UU ITE pasca perubahan kedua belum sepenuhnya mampu menjamin kepastian hukum dalam penegakan tindak pidana siber. Hal ini ditandai oleh adanya *sunset clause* yang menciptakan kondisi transisi normatif, tumpang tindih antara UU ITE dengan KUHP Nasional dan UU PDP, inkonsistensi putusan pengadilan dalam menangani perkara siber, serta keterbatasan kapasitas kelembagaan aparat penegak hukum. Keseluruhan permasalahan tersebut menunjukkan bahwa reformasi regulasi hukum siber di Indonesia masih memerlukan langkah lanjutan yang lebih komprehensif, integratif, dan berbasis pada prinsip kepastian hukum, keadilan, serta kemanfaatan.

Berdasarkan kesimpulan penelitian di atas, terdapat beberapa saran yang dapat dirumuskan. Pertama, pembentuk undang-undang perlu segera melakukan harmonisasi menyeluruh antara UU ITE, KUHP Nasional (UU No. 1 Tahun 2023), dan UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022) guna mengeliminasi tumpang tindih norma dan potensi *legal gap* yang dapat menghambat penegakan hukum secara konsisten. Proses harmonisasi ini idealnya dilakukan melalui pembentukan kodifikasi hukum siber yang bersifat *lex specialis* dan komprehensif, yang mampu mengakomodasi seluruh aspek tindak pidana siber dalam satu kerangka regulasi yang kohesif. Kedua, aparat penegak hukum khususnya penyidik, jaksa, dan hakim perlu mendapatkan pelatihan teknis secara berkelanjutan di bidang forensik digital dan *cyber law*, mengingat karakteristik tindak pidana siber yang sangat teknis dan terus berkembang. Ketiga, pembentukan pedoman teknis (*technical guidelines*) yang lebih operasional terkait penerapan pasal-pasal yang berpotensi multitafsir dalam UU ITE, seperti Pasal 27A dan Pasal 28 ayat (2), perlu diprioritaskan guna mencegah inkonsistensi putusan pengadilan. Keempat, penguatan literasi digital masyarakat perlu digalakkan sebagai strategi preventif jangka panjang dalam penanggulangan tindak pidana siber, sejalan dengan semangat pembentukan ekosistem digital Indonesia yang bersih, sehat, beretika, dan berkeadilan sebagaimana diamanatkan oleh UU No. 1 Tahun 2024.

DAFTAR RUJUKAN

- Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge : Jurnal Hukum*, 5(02), 55-63.
- Altansa, F., & Rahmat, D. (2024). Analisis Yuridis Kewenangan Jaksa Dalam Penegakan Hukum Tindak Pidana Informasi Dan Transaksi Elektronik. *LEX LAGUENS: Jurnal Kajian Hukum dan Keadilan*, 2(1), 1-13. <https://doi.org/10.08221/lexlaguens.v2i1.27>
- Aprilianti, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Begawan Abioso*, 15(1), 41-50. <https://doi.org/10.37893/abioso.v15i1.1002>
- Aulia, H., Muhlizar, & Harmuzan. (2026). Tinjauan Yuridis Tindak Pidana Cyber Crime Menurut Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik: (Studi Kasus Putusan Pengadilan Negeri Ternate Nomor: 155/Pid.Sus/2024.PN.Tte). *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, 4(1), 7198-7212. <https://doi.org/10.61104/alz.v4i1.4607>
- Djarawula, M., Alfiani, N., & Mayasari, H. (2023). Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan

- Transaksi Elektronik. *Jurnal Cakrawala Ilmiah*, 2(10), 3799–3806.
<https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i10.5842>
- Djibu, M. A. (2025). Transformasi Digital dan Keamanan Siber: Upaya Penanggulangan Kejahatan di Era Teknologi di Indonesia. *Judge: Jurnal Hukum*, 6(01), 341–347. <https://doi.org/10.54209/judge.v6i01.1182>
- Djulaeka, & Rahayu, D. (2020). *Metode Penelitian Hukum*. Scopindo Media Pustaka.
- Fitri, S. N. (2022). Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial*, 7(1), 104–124. <https://doi.org/10.22373/justisia.v7i1.12719>
- Fitri, S. N. (2024). *Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia*. 104–124.
- Marzuki, P. M. (2021). *Pengantar ilmu hukum*. Prenada Media.
- Maudy. (2025). *Transformasi Digital dan Keamanan Siber: Upaya Penanggulangan Kejahatan di Era Teknologi di Indonesia*. 06(01), 341–347.
- Munir. (2024). Kajian Pasal 27 A UU No. 1 Tahun 2024 Tentang Perubahan Kedua Undang-Undang Nomor 8 Tahun 2008 Tentang ITE: *Fundamental: Jurnal Ilmiah Hukum*, 13(2), 1–12. <https://doi.org/10.34304/jf.v13i2.284>
- Nursyamsu, M. R. A., Kurniati, Y., & Krisnamurti, H. (2025). Peran Bhabinkamtibmas Dalam Pencegahan Tindak Pidana Siber Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Informasi Transaksi Elektronik. *Innovative: Journal Of Social Science Research*, 5(4), 6127–6136. <https://doi.org/10.31004/innovative.v5i4.20769>
- Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. *Binamulia Hukum*, 12(2), 287–298. <https://doi.org/10.37893/jbh.v12i2.605>
- Primadhany, E. F., Hadi, A. M., Rasyid, A., S, H. T. H., Bhakti, I. S. G., Rosita, D., Ramadhani, D. W., Rauf, A., Rustan, Widodo, M. F. S., Dewi, S. R., Anita, A. A., Hidayat, D. N., Musthofa, M. A. A., Rohmah, A. N., & Surayda, H. I. (2025). *Pengantar Hukum Siber Indonesia*. Sada Kurnia Pustaka.
- Sahlepi, M. A. (2023). Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online Di Tinjau Dari Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. *Innovative: Journal Of Social Science Research*, 3(6), 1402–1412.
- Santoso, I., Syahrin, A., Mulyadi, M., & Agusmidah, A. (2024). Kebijakan Hukum Pidana Terhadap Perbuatan Melawan Hukum Dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal–Pasal Tertentu UU ITE. *Locus Journal of Academic Literature Review*, 3(4), 329–335. <https://doi.org/10.56128/ljoalr.v3i4.312>
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

- Widiarty, W. S. (2024). *Buku Ajar Metode Penelitian Hukum* (M. Tajuddin, Ed.). Publika Global Media.
- Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo. *UNES Law Review*, 5(4), 3917–3929. <https://doi.org/10.31933/unesrev.v5i4.698>
- Zamayya, A. R. R., Wagiyanto, D. I., Joesoef, P. G., Salim, R. E., & Thendean, T. (2025). Kajian Teoritis Implikasi The United Nations Convention Against Cybercrime Terhadap Pengaturan Tindak Pidana Siber Indonesia. *IKRA-ITH HUMANIORA : Jurnal Sosial Dan Humaniora*, 9(2), 343–354.
- Zhafira, I., Ismansyah, I., & Yoserwan, Y. (2023). Tinjauan Yuridis Tindak Pidana Pencemaran Nama Baik Dalam Kitab Undang-undang Hukum Pidana Dikaitkan dengan Pasal 27 Ayat (3) Undang-undang Informasi dan Transaksi Elektronik: Studi Putusan Nomor 1909 K/Pid.Sus/2021. *Unes Journal of Swara Justisia*, 7(3), 901–912. <https://doi.org/10.31933/ujsj.v7i3.408>