AL-BAHST
Jurnal Ilmu Sosial, Politik, dan Hukum
Vol. 2, No. 1, April 2024 ISSN: 3031-7029

# Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia

**Fadhila Rahman Najwa**
Program Studi Ilmu Hukum, Universitas Sebelas Maret
fadhilarahmannajwa@gmail.com

**Kata Kunci:**

Keamanan Siber
Hukum Cyber
Penegakan Hukum

**Abstract**

*In the increasingly developing digital era, cyber security has become an important issue that requires serious attention, especially in the context of law and law enforcement. Cyberattacks are becoming increasingly sophisticated and troubling, posing significant challenges to law enforcement and personal data protection. This research reveals that although Indonesia has adopted several regulations related to cyber security, such as the Information and Electronic Transactions Law (UU ITE), there are still shortcomings in terms of implementation and consistency. A series of cyber security incidents that occurred in Indonesia highlight the need for increased law enforcement capacity. This article examines the challenges faced by Indonesia in dealing with cyber security issues, with a special focus on legal aspects and law enforcement. Using a qualitative approach, this research analyzes secondary data from legal sources, government policies, and selected case studies to identify gaps in current regulations and provide recommendations for improving cyber security in Indonesia. The main objective of this research is to evaluate the effectiveness of the existing legal framework in dealing with cybercrime and promote cross-sector cooperation in preventing and responding to cyberattacks. The research results show that although Indonesia has made progress in cyber security regulations, there is still an urgent need for increased cooperation between institutions, development of law enforcement capacity, and implementation of legal strategies that are more adaptive and responsive to the dynamics of cyber threats.*

**Abstrak**

Dalam era digital yang semakin berkembang, keamanan siber menjadi isu penting yang memerlukan perhatian serius, terutama dalam konteks hukum dan penegakan hukum. Serangan siber menjadi semakin canggih dan meresahkan, menimbulkan tantangan signifikan bagi penegakan hukum dan perlindungan data pribadi. Penelitian ini mengungkapkan bahwa meskipun Indonesia telah mengadopsi beberapa regulasi terkait keamanan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), masih terdapat kekurangan dalam hal implementasi dan konsistensi. Serangkaian insiden keamanan siber yang terjadi di Indonesia, menyoroti kebutuhan akan peningkatan kapasitas penegakan hukum. Artikel ini mengkaji tantangan yang dihadapi oleh Indonesia dalam menangani masalah keamanan siber, dengan fokus khusus pada aspek hukum dan penegakan hukum. Melalui metode pendekatan kualitatif, penelitian ini menganalisis data sekunder dari sumber hukum, kebijakan pemerintah, dan studi kasus terpilih untuk

mengidentifikasi celah dalam regulasi saat ini dan memberikan rekomendasi untuk peningkatan keamanan siber di Indonesia. Tujuan utama dari penelitian ini adalah untuk mengevaluasi efektivitas kerangka hukum yang ada dalam menangani kejahatan siber dan mempromosikan kerjasama lintas sektor dalam pencegahan dan penanggulangan serangan cyber. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah membuat kemajuan dalam regulasi keamanan siber, masih terdapat kebutuhan mendesak untuk peningkatan kerjasama antar lembaga, pengembangan kapasitas penegakan hukum, dan penerapan strategi hukum yang lebih adaptif dan responsif terhadap dinamika ancaman cyber.

***Corresponding Author:***

Fadhila Rahman Najwa
Program Studi Ilmu Hukum
Universitas Sebelas Maret
fadhilarahmannajwa@gmail.com

## 1. PENDAHULUAN

Revolusi dalam teknologi informasi dan komunikasi telah menyebabkan perubahan mendasar dalam cara kita berinteraksi di dunia digital. Perkembangan ini, meskipun membawa banyak manfaat, juga mengundang risiko yang semakin besar. Di Indonesia, peningkatan akses dan penggunaan internet telah memperluas jangkauan dan dampak serangan siber. Tidak hanya individu yang menjadi sasaran; lembaga-lembaga pemerintah dan entitas sektor swasta yang memegang data kritis dan infrastruktur esensial juga rentan terhadap serangan ini.

Berdasarkan laporan Interpol Cyber Assessment Report 2021, terdapat sekitar 2,7 juta serangan *ransomware* yang terdeteksi di Asia Tenggara pada periode Januari-September 2020, dengan Indonesia berada di peringkat teratas dengan 1,3 juta kasus. Kemudian berdasarkan data dari Bareskrim Polri, terjadi peningkatan drastis dalam jumlah kasus kejahatan siber yang ditangani. Pada tahun 2022, terdapat 8.831 kasus kejahatan siber yang ditindak, meningkat hingga 14 kali lipat dibandingkan dengan tahun 2021, di mana jumlah kasus yang ditindak hanya 612. Selain itu, riset dari Fortinet mengungkapkan bahwa serangan siber *ransomware* di Indonesia meningkat dua kali lipat selama tahun 2023, dengan target utama adalah perusahaan swasta. Kasus spesifik termasuk peretasan terhadap aplikasi Jakarta Kini (Jaki) yang terjadi setelah disinggung dalam debat capres.

Data-data di atas menunjukkan kejahatan siber yang terjadi di Indonesia. Kejahatannya yang terus meningkat dan besarnya kerugian yang dihadapi membuat kejahatan siber ini menjadi semakin mengkhawatirkan. Di samping itu, meskipun upaya pencegahan kejahatan siber ini telah dilakukan namun belum menunjukkan hasil sebagaimana yang diharapkan.

Untuk menghadapi tantangan keamanan siber, Pemerintah Indonesia telah mengambil langkah proaktif dengan memperkuat infrastruktur keamanan digital nasional. Upaya ini meliputi pengembangan kebijakan, peningkatan teknologi keamanan, dan program kesadaran masyarakat tentang risiko keamanan siber. Salah satu langkah utama yang telah diambil adalah pengesahan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

UU ITE merupakan pilar utama dalam kerangka hukum keamanan siber Indonesia (Saly et al., 2023). UU ITE memainkan peran krusial dalam menangani isu-isu terkait dengan transaksi elektronik dan distribusi informasi di ranah digital. UU ini tidak hanya fokus pada aspek legal transaksi online, namun juga secara ekstensif mengatur tentang bagaimana informasi disebarkan di internet, memberikan kerangka untuk melindungi data pribadi warga, dan menetapkan standar untuk menangani kejahatan siber yang berkembang pesat. Secara umum, landasan hukum penanganan kejahatan siber di Indonesia berpusat pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang direvisi dengan Undang-Undang Nomor 19 Tahun 2016. UU ITE mengatur transaksi dan aktivitas yang dilakukan melalui sistem elektronik, termasuk mengatur isu penyebaran konten ilegal, penipuan online, pencurian data, dan peretasan. UU ini menargetkan berbagai bentuk pelanggaran siber, mulai dari penyebaran konten ilegal hingga penipuan dan peretasan.

Upaya pemerintah sebagai wujud tanggung jawab dalam memenuhi hak asasi manusia bagi pengguna internet di Indonesia ditunjukkan melalui revisi atas UU ITE. Revisi ini dilakukan karena banyaknya perdebatan yang datang dari masyarakat dan pemahaman multitafsir terkait UU ITE (Wijaya et al., 2021). Hal ini dipicu oleh adanya pemahaman yang multitafsir mengenai beberapa ketentuan dalam UU ITE, yang sering kali menimbulkan kekhawatiran terkait dengan kebebasan berekspresi dan hak asasi manusia. Revisi ini melibatkan penyempurnaan beberapa norma pasal terkait dengan alat bukti elektronik, sertifikasi elektronik, transaksi elektronik, dan identitas digital (Hamanduna & Widjanarko, 2023). Perubahan pada Pasal 5, Pasal 13, dan Pasal 17, bertujuan untuk memperjelas dan menyempurnakan

peraturan dalam konteks digital yang berkembang. UU ITE yang baru menambahkan pasal khusus tentang perlindungan anak dalam mengakses layanan elektronik (Pasal 16A dan 16B) yang mengatur soal batasan usia minimum anak dan mekanisme verifikasi pengguna anak.

Perubahan substansi pada Pasal 27 yang sering disebut sebagai 'pasal karet', yakni pasal yang tafsirannya sangat subjektif dari penegak hukum ataupun pihak lainnya, mengurangi potensi penyalahgunaan hukum ini (Nanda & Hariyanta, 2022). Perubahan ini termasuk penghapusan muatan penghinaan, pencemaran nama baik, pemerasan, dan pengancaman, yang sebelumnya dapat menimbulkan multitafsir. Perubahan pada Pasal 40A mengatur peran pemerintah dalam menciptakan ekosistem digital yang aman, adil, akuntabel, dan inovatif. Hal ini penting untuk mendorong pertumbuhan ekonomi digital yang sehat di Indonesia. Perubahan pada Pasal 43 memperkuat kewenangan penyidik dalam hal intervensi ke akun media sosial dan aset digital terkait penyidikan, menunjukkan penguatan dalam penegakan hukum (Irawan, 2023).

Menurut Menkominfo, perubahan UU ITE ini mencerminkan tanggung jawab pemerintah dalam memenuhi hak asasi manusia bagi pengguna internet di Indonesia, sesuai dengan konstitusi negara. Perubahan ini juga dianggap memberikan kepastian hukum yang lebih baik dalam ruang digital, yang penting mengingat dinamika dan perkembangan teknologi yang cepat.

Namun, meskipun UU ITE sudah melewati upaya penyempurnaan dan menyediakan dasar hukum yang lebih baik untuk menangani kejahatan siber, masih terdapat kekurangan dalam hal detail dan spesifikasi. Definisi dan ruang lingkup UU ITE yang luas, mencakup semua tindak pidana yang menggunakan semua sarana sistem elektronik menyebabkan kesulitan dalam interpretasi dan penerapan undang-undang dalam kasus nyata (Rohmy et al., 2021). Karena sifatnya yang mencakup berbagai aspek, sering kali terdapat kesulitan dalam menentukan batas-batas penerapan hukum ini, terutama dalam kasus-kasus yang berada di wilayah abu-abu antara kejahatan siber dan aktivitas online yang sah. Hal ini juga mengakibatkan adanya celah antara tujuan undang-undang dan penerapannya di lapangan. Misalnya, Beberapa pasal dalam UU ITE, terutama yang berkaitan dengan pencemaran nama baik dan ujaran kebencian, seringkali dianggap multitafsir. Hal ini membuat penegakan hukum menjadi subjektif dan terkadang digunakan untuk menargetkan opini yang berbeda di media sosial atau platform digital lainnya. Dampaknya, ini bisa menimbulkan kekhawatiran tentang pembatasan kebebasan berekspresi.

Kemudian Berdasarkan data dari Kepolisian Nasional Indonesia, terdapat peningkatan signifikan dalam penindakan kasus yang terkait dengan konten ilegal seperti penipuan dan pencemaran nama baik. Ini menunjukkan bahwa fokus penegakan hukum cenderung pada pelanggaran konten daripada kejahatan siber yang lebih kompleks seperti peretasan atau pencurian identitas. Menurut pakar hukum di Indonesia, penanganan kejahatan siber memang memiliki tingkat kompleksitas yang tinggi dan memerlukan harmonisasi yang baik antar lembaga terkait (Kemit et al., 2023). Kejahatan siber ini disebut memiliki kompleksitas yang tinggi karena seringkali mencakup aspek-aspek yang sangat teknis dan spesifik, yang mengharuskan penegak hukum memiliki keahlian khusus dalam bidang teknologi informasi dan komunikasi.

Di samping UU ITE, terdapat juga regulasi lain yang berhubungan dengan keamanan siber di Indonesia, seperti

1. Undang-Undang Perlindungan Data Pribadi (PDP Law) No. 27 Tahun 2022
2. Peraturan Pemerintah No. 71 Tahun 2019 tentang Pelaksanaan Sistem dan Transaksi Elektronik (GR 71)
3. Inisiatif Badan Siber dan Sandi Negara (BSSN), sebagai lembaga pemerintah yang bertugas di bidang keamanan siber
4. Regulasi Baru untuk Sektor Keuangan, yang dikembangkan oleh Otoritas Jasa Keuangan (OJK).

Regulasi-regulasi ini mencakup berbagai aspek, mulai dari perlindungan data pribadi hingga tindakan pencegahan terhadap serangan siber. Namun, banyak dari regulasi ini masih terfragmentasi dan belum menyediakan kerangka kerja yang komprehensif. Hambatan yang pertama, terdapat kendala dalam hal sumber daya, baik dari segi keuangan maupun tenaga ahli. Kemudian, adanya kesenjangan pengetahuan dan keahlian antara pembuat kebijakan dan praktisi keamanan siber. Kesenjangan ini menyebabkan kesulitan dalam menerjemahkan kebijakan menjadi praktik yang efektif.

Oleh karena itu, penting untuk melakukan pengembangan kapasitas penegakan hukum dalam menghadapi kejahatan siber. Mengingat kompleksitas dan sifat teknis dari kejahatan siber, penegakan hukum di Indonesia memerlukan sumber daya yang memadai dan pelatihan khusus. Juga peningkatan kerjasama antar lembaga, pengembangan kapasitas penegakan hukum, dan penerapan strategi hukum yang lebih adaptif dan responsif terhadap dinamika ancaman cyber.

## 2. METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif yang menggunakan metode deskriptif. Metode ini dipilih untuk memberikan gambaran rinci dan sistematis tentang implementasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam konteks keamanan siber di Indonesia, serta bagaimana UU ITE

ini diharmonisikan dengan standar keamanan siber internasional. Dalam pengumpulan data, penulis melakukan pengamatan terhadap penerapan UU ITE oleh penegak hukum dan sistem peradilan, serta pencatatan terkait dengan efektivitas dan tantangan dalam penegakan UU ITE.

Metode ini penulis gunakan untuk memberikan analisis komprehensif tentang status quo dari kerangka hukum keamanan siber di Indonesia. Melalui analisis ini, penelitian ini bertujuan untuk mengidentifikasi area potensial yang dapat diperbaiki dalam kerangka hukum tersebut, sehingga memberikan rekomendasi yang bermanfaat untuk meningkatkan efektivitas dan efisiensi dalam penegakan UU ITE di masa depan.

## 3. PEMBAHASAN

### 1. Permasalahan Yang dihadapi UU ITE

Dalam lanskap keamanan siber Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan revisinya pada tahun 2016, menduduki posisi sentral. UU ITE lahir dari kebutuhan untuk mengatur ruang siber yang berkembang cepat. Sejak pengesahannya, UU ini telah menjadi landasan dalam menangani berbagai kasus siber.

Ruang lingkup UU ITE mencakup berbagai aspek mulai dari keamanan informasi, perlindungan data pribadi, transaksi elektronik, dan pencegahan kejahatan siber. UU ITE juga mengatur tentang penyebaran informasi yang dapat dianggap merugikan, menipu, atau melanggar kesusilaan. Hukum ini memberikan definisi jelas tentang apa yang dianggap sebagai tindakan kriminal dalam ruang siber, seperti penipuan online, pencurian identitas, dan penyebaran konten illegal (Ramadhani, 2023). Namun, dalam penerapannya hukum ini menghadapi kritik terkait dengan potensi penyalahgunaan dan efektifitasnya. Kritik yang ada tersebut sebagai berikut

*Pertama*, isu yang berkaitan dengan kebebasan berpendapat dan berekspresi (Jahriyah et al., 2021). Banyak pengamat hukum dan aktivis hak asasi manusia menganggap bahwa beberapa ketentuan dalam UU ITE bisa diterjemahkan secara luas dan multitafsir, yang berpotensi digunakan untuk membatasi kebebasan berpendapat. Pasal-pasal tertentu dalam UU ITE, seperti yang berkaitan dengan pencemaran nama baik dan penyebaran informasi yang menyesatkan, sering kali menjadi titik fokus dalam debat ini.

Ditemukan kasus-kasus seperti Kasus Prita Mulyasari pada tahun 2009, dimana Prita Mulyasari dituntut berdasarkan UU ITE setelah menulis keluhan tentang layanan rumah sakit di media sosial (Sufiyah, n.d.). Kasus ini menjadi sorotan karena dianggap sebagai contoh penyalahgunaan UU ITE untuk membungkam kritik. Selain itu, Kasus Dandhy Laksono dan Ananda Badudu pada tahun 2019, Keduanya ditangkap karena diduga menyebarkan informasi yang memprovokasi melalui media sosial terkait demonstrasi mahasiswa (Firmansyah et al., 2022). Kasus ini menimbulkan kekhawatiran tentang kebebasan berekspresi, khususnya dalam konteks jurnalisme dan protes sosial. Kasus Baiq Nuril pada 2018, seorang mantan staf sekolah di Lombok, divonis bersalah karena merekam dan menyebarkan percakapan yang berisi pelecehan seksual oleh atasannya (Cipta & Masyhar, 2021). Meski dia adalah korban, penerapan UU ITE dalam kasus ini dipertanyakan banyak pihak terkait dengan perlindungan terhadap korban pelecehan.

Dari kasus tersebut dapat teridentifikasi adanya kesenjangan antara tujuan legislatif UU ITE dan realitas penegakannya di lapangan. Menurut penelitian dari Institute for Criminal Justice Reform (ICJR), UU ITE telah menimbulkan konsekuensi yang tidak diinginkan, termasuk dampak sosial dengan meluasnya efek jera, penggunaan untuk balas dendam, barter kasus, shock terapi, hingga membungkam kritik dan persekusi. Direktur Eksekutif SAFEnet, Damar Juniarto, menyatakan bahwa UU ITE belum memberi rasa keadilan dan perlu direvisi. Dalam webinar yang diadakan oleh Amnesty International Indonesia Chapter UNAIR, periset Adhigama A. Budiman dari ICJR mengemukakan bahwa UU ITE setidaknya membatasi tiga jenis HAM:

1. Kebebasan berekspresi dan berpendapat
2. Hak atas akses informasi
3. Hak atas privasi.

Budiman menunjukkan bahwa dalam kurun waktu 2016-2020, ICJR mendata terdapat 768 perkara terkait UU ITE dari tiga pasal tersebut, dengan 744 perkara diputus bersalah oleh hakim (sumber: Unair News).

*Kedua*, kekurangan dalam perlindungan data pribadi. Di dalam UU ITE ketentuan spesifik tentang perlindungan data pribadi pengguna internet di Indonesia masih kurang (Fuad, 2023). Terkait dampaknya terhadap kebebasan berpendapat dan berekspresi, di mana kekhawatiran muncul bahwa undang-undang ini dapat mengekang ekspresi publik melalui penerapan ketentuan yang multitafsir. Kedua, UU ITE dikritik karena kekurangannya dalam perlindungan data pribadi. Dibandingkan dengan standar internasional seperti GDPR Uni Eropa, UU ITE kurang detail dalam mengatur hak subjek data dan kewajiban pemberitahuan kebocoran data. Contoh kasus konkrit yang menunjukkan kelemahan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam hal perlindungan data pribadi adalah insiden kebocoran data pengguna Tokopedia pada Mei 2020 . Tokopedia, salah satu platform e-commerce terbesar di Indonesia,

mengalami kebocoran data yang mempengaruhi sekitar 91 juta pengguna dan data yang bocor termasuk nama, email, dan hashed password pengguna (Delpiero et al., 2021). Menyoroti bahwa UU ITE tidak memiliki ketentuan yang cukup spesifik atau kuat untuk menangani pelanggaran data pribadi pada skala besar dan mungkin kurang dalam hal persyaratan keamanan data yang komprehensif, mekanisme pelaporan kebocoran data yang efektif, dan ketentuan yang jelas tentang tanggung jawab perusahaan dalam melindungi data pengguna.

Dari penanganan yang dilakukan pemerintah pada kasus ini, dapat dianalisa bahwa ada ketidakjelasan hukum disana, dimana kewajiban perusahaan dalam melindungi data pengguna dan tindakan yang harusnya diambil saat terjadi kebocoran data, tidak sepenuhnya jelas atau tegas. UU ITE tidak memiliki ketentuan wajib untuk melaporkan insiden kebocoran data kepada otoritas atau pihak yang terdampak dalam waktu yang tertentu. Hal ini yang kemudian menyebabkan keterlambatan dalam penanganan kebocoran data dan memperburuk dampak terhadap pengguna yang data pribadinya bocor. Seharusnya berkaca dengan regulasi GDPR, yang memberikan panduan spesifik tentang pengumpulan, pemrosesan, dan penyimpanan data pribadi.

*Ketiga*, UU ITE dianggap diimplementasikan dengan tidak konsisten, dan seringkali bergantung pada konteks politik atau sosial kasus yang ada. Pada Maret 2019, Robertus Robet ditangkap dan dijerat dengan UU ITE karena menyanyikan lagu yang dianggap menghina institusi militer dalam sebuah aksi kampanye. Lagu tersebut merupakan bagian dari pidato yang menyuarakan keprihatinan terhadap keterlibatan militer dalam jabatan sipil. Kasus ini memicu reaksi luas dari masyarakat sipil dan kelompok hak asasi manusia, yang menganggap penangkapan tersebut sebagai bentuk pembungkaman kebebasan berekspresi. Dalam kasus lain, penangkapan aktivis Walhi, yang terjadi di Kalimantan Timur pada tahun 2020 yang ditangkap dengan tuduhan menyebarkan informasi palsu terkait dengan kebakaran hutan dan lahan. Aktivis tersebut menggunakan media sosial untuk menyebarkan informasi tentang dampak kebakaran dan dugaan keterlibatan perusahaan besar.

Kasus aktivis Walhi dan kasus Robet menunjukkan bagaimana UU ITE diterapkan dalam berbagai konteks, termasuk aktivisme lingkungan. Hal ini menegaskan kekhawatiran bahwa UU ITE yang terkadang digunakan tidak semata-mata untuk keadilan hukum, tetapi juga bisa dipengaruhi oleh konteks sosial dan politik, serta kepentingan tertentu. Seharusnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) digunakan semata-mata untuk keadilan hukum, tanpa dipengaruhi oleh konteks sosial dan politik (Rohmy et al., 2021). Dalam prinsip hukum, setiap undang-undang idealnya harus diterapkan secara konsisten dan objektif, tanpa dipengaruhi oleh kepentingan sosial atau politik tertentu. Hal ini untuk memastikan bahwa semua warga negara diperlakukan sama di mata hukum, dan keadilan dapat terwujud tanpa bias. Penerapannya harus fokus pada kasus-kasus yang secara objektif melanggar hukum dengan kerugian yang jelas dan nyata, serta ditangani dengan cara yang konsisten dan transparan. Seperti penipuan online dan cyberbullying.

Inkonsistensi dalam penegakan hukum tersebut mengurangi kepercayaan publik terhadap sistem peradilan (Rizal & Wondabio, 2023). Ketika masyarakat merasakan adanya ketidakadilan atau perlakuan yang berbeda di antara kasus yang serupa, ini dapat menimbulkan persepsi bahwa hukum tidak ditegakkan secara adil dan objektif. Situasi seperti inilah yang berpotensi menimbulkan kekecewaan dan keraguan terhadap integritas sistem hukum. Dalam konteks UU ITE, jika penegakan hukum dirasakan tidak konsisten misalnya, beberapa kasus ditangani dengan serius sementara kasus lain yang serupa diabaikan, atau ketika penegakan hukum tampak lebih keras terhadap kelompok tertentu dibandingkan dengan yang lain—maka hal ini dapat menimbulkan pandangan bahwa hukum tersebut digunakan sebagai alat kekuasaan atau pengaruh politik, bukan semata-mata untuk keadilan. Ketika kepercayaan publik terhadap sistem peradilan menurun, ini dapat berdampak pada berkurangnya kepatuham masyarakat terhadap hukum dan kurangnya perlindungan terhadap hak asasi, dengan pelanggaran hak mungkin tidak ditanganiabatan sipil. Kasus ini memicu reaksi luas dari masyarakat sipil dan kelompok hak asasi manusia, yang menganggap penangkapan tersebut sebagai bentuk pembungkaman kebebasan berekspresi. Inkonsistensi dalam penegakan hukum tersebut mengurangi kepercayaan publik terhadap sistem peradilan dan akibat jangka panjangnya mengurangi kepatuham masyarakat terhadap hukum dan kurangnya perlindungan terhadap hak asasi, dengan pelanggaran hak mungkin tidak ditangani secara efektif.

**2. Tantangan Penegakan Hukum Siber**

Dalam menegakkan hukum siber, terdapat tantangan yang dihadapi penegak hukum dalam menegakkan hukum. Keterbatasan sumber daya dan kapasitas merupakan tantangan utama dalam penegakan hukum siber di Indonesia. Faktanya, menurut survei yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN), kurang dari separuh lembaga pemerintah di Indonesia yang memiliki kebijakan keamanan siber yang memadai, yang menunjukkan kesenjangan serius dalam infrastruktur keamanan digital negara. Hal ini terutama menjadi masalah ketika kita mempertimbangkan kasus-kasus seperti serangan siber terhadap database pemerintah atau kebocoran data yang besar, seperti insiden kebocoran data pengguna

platform e-commerce besar di Indonesia pada tahun 2020.

Lebih lanjut, kesulitan mengidentifikasi pelaku kejahatan siber menjadi semakin rumit dengan adanya teknologi enkripsi dan penggunaan jaringan privat virtual (VPN) oleh pelaku atau server proxy yang dapat mempersulit pelacakan dengan menyembunyikan jejak digital mereka (Citra et al., 2023). Teknologi enkripsi canggih memungkinkan pelaku untuk mengamankan komunikasi dan data mereka, sehingga sulit untuk diintersepsi atau diakses oleh penegak hukum. VPN dan server proxy menambah lapisan kompleksitas lainnya, karena mereka memungkinkan pelaku untuk menyembunyikan lokasi fisik mereka dan membuat jejak digital mereka lebih sulit untuk dilacak. Penggunaan VPN dan server proxy dapat menyulitkan penegak hukum untuk menentukan sumber sebenarnya dari serangan siber atau aktivitas ilegal lainnya. Pelaku dapat tampak seolah-olah mereka beroperasi dari negara yang berbeda, atau bahkan dari beberapa negara, membuat investigasi menjadi lebih rumit dan sering kali memerlukan kerjasama lintas yurisdiksi.

Sifat sementara dari data digital juga menjadi hambatan signifikan dalam penanganan kejahatan siber, khususnya dalam konteks mengamankan bukti. Data digital memiliki sifat yang mudah diubah atau dihapus, sehingga bukti penting bisa lenyap sebelum otoritas memiliki kesempatan untuk mengamankannya. Dalam kasus kejahatan siber, pelaku sering menggunakan alat dan metode yang canggih untuk menghapus jejak digital mereka, membuat bukti menjadi lebih sulit untuk diidentifikasi dan diamankan. Faktor ini menambah kompleksitas dalam penyelidikan karena penegak hukum harus bertindak sangat cepat untuk mengamankan bukti sebelum hilang. Misalnya, dalam kasus penyebaran konten ilegal melalui media sosial, penegak hukum sering kali kesulitan mengamankan bukti yang relevan sebelum dihapus oleh pelaku atau platform. Semua ini menunjukkan kebutuhan mendesak untuk peningkatan kapasitas di bidang teknologi dan pelatihan spesialis siber, untuk memastikan bahwa penegakan hukum dapat mengikuti langkah dengan kejahatan siber yang semakin canggih

Dalam konteks penuntutan, kejahatan siber di Indonesia seringkali terhambat oleh faktor-faktor seperti: *pertama*, hukum yang ada terkadang tidak cukup spesifik untuk mengatasi kejahatan siber tertentu. Kejahatan siber yang merupakan kejahatan yang sangat dinamis dan berkembang dengan cepat, seringkali lebih cepat daripada perkembangan peraturan hukum. Akibatnya, hukum yang ada mungkin tidak memiliki ketentuan atau definisi yang cukup jelas untuk menangani jenis kejahatan siber yang baru muncul atau kompleks. Misalnya, hukum mungkin tidak secara eksplisit mengatur tentang serangan siber tertentu atau bentuk penipuan online yang belum dikenal sebelumnya. Ketidaksesuaian ini antara sifat kejahatan siber yang terus berubah dan kerangka hukum yang lebih statis menciptakan celah hukum, di mana pelaku kejahatan siber mungkin tidak dapat dituntut secara efektif karena ketiadaan peraturan yang spesifik atau terkini.

*Kedua*, ada masalah yurisdiksi, terutama ketika pelaku beroperasi dari luar negeri. Ketidakjelasan hukum sering menghasilkan ketidakpastian dalam penuntutan. Ketika pelaku berada di luar negeri, penegak hukum di Indonesia menghadapi rintangan dalam mengejar, menangkap, dan menuntut pelaku tersebut karena terhalang oleh batas-batas yurisdiksi internasional. Situasi ini menimbulkan tantangan signifikan karena yurisdiksi hukum sebuah negara biasanya terbatas pada wilayah geografisnya sendiri. Selain itu, ketidakjelasan hukum sering menghasilkan ketidakpastian dalam penuntutan, terutama dalam kasus yang melibatkan teknologi baru. Seiring berkembangnya teknologi, jenis kejahatan siber yang baru dan lebih kompleks muncul, yang mungkin belum diatur secara eksplisit dalam hukum yang ada. Misalnya, serangan menggunakan teknologi AI canggih atau eksploitasi keamanan di Internet of Things (IoT) mungkin belum memiliki ketentuan hukum yang jelas. Tanpa definisi hukum yang spesifik, penuntutan terhadap jenis kejahatan baru ini menjadi sulit karena penegak hukum mungkin kesulitan menentukan bagaimana hukum yang ada dapat diterapkan pada kasus-kasus baru ini.

Sehingga ditemukan perlunya UU ITE disinkronkan dengan standar keamanan siber internasional. Mengingat sifat lintas batas dari banyak kejahatan siber, harmonisasi ini penting untuk memastikan keefektifan UU ITE dalam konteks global. Sehingga Indonesia dapat memperkuat kerjasama internasionalnya dan menyesuaikan kerangka hukum nasionalnya dengan praktik global terbaik. Selain itu pembaruan dan penyesuaian berkelanjutan pada UU ITE harus dilakukan agar dapat secara efektif menangani kejahatan siber yang terus berkembang. Hal ini dapat dilakukan melalui peningkatan pelatihan bagi penegak hukum, penguatan kerjasama lintas batas, dan peninjauan kembali beberapa aspek hukum untuk meningkatkan kejelasan dan efektivitasnya. Perlu juga peningkatan kapasitas penegakan hukum, termasuk pelatihan khusus dalam kejahatan siber dan investasi dalam teknologi forensik digital.

### 3. Perbandingan Regulasi UU ITE Dengan Regulasi Internasional Serta Kerjasama Antarlembaga

Dalam era globalisasi, kejahatan siber seringkali juga tidak terbatas pada batas-batas nasional, sehingga memerlukan kerjasama dan kesesuaian dengan standar internasional. Membandingkan regulasi yang ada pada UU ITE dengan regulasi Internasional dapat menjadi tolak ukur efisiensi hukum nasional (Cloramidine & Badaruddin, 2023). Regulasi internasional sering kali mencerminkan praktik terbaik yang

telah berkembang melalui konsensus antar negara dan pakar di bidangnya. Mereka menyediakan kerangka kerja untuk menangani berbagai aspek keamanan siber dan perlindungan data yang mungkin belum sepenuhnya tercakup dalam hukum nasional. Selain itu, membandingkan regulasi nasional dengan regulasi Internasional dapat membantu mengindentifikasi celah pada UU ITE untuk kemudian ditindak lanjuti sehingga meningkatkan keamanan siber nasional. Dan ketika regulasi nasional sesuai dengan regulasi Internasional, kerjasama lintas batas kaitannya dalam menangani kejahatan siber dan pertukaran data dalam penanaganan kejahatan lintas negara menjadi lebih mudah.

Ketika dibandingkan, ditemukan kesamaan dan perbedaan antara keduanya. Kesamaan dalam regulasi keamanan siber di negara-negara lain dapat dilihat pada beberapa aspek, khususnya dalam hal definisi dan sanksi untuk kejahatan siber. Seperti regulasi di banyak negara, UU ITE turut serta mengatur tentang kejahatan terkait penipuan online, penyebaran virus, dan serangan siber lainnya. Hukum ini juga mengakui perlunya melindungi data pribadi, serupa dengan regulasi di Uni Eropa seperti General Data Protection Regulation (GDPR). Aspek lain yang serupa termasuk pemberlakuan hukum terhadap penyebaran konten ilegal dan ujaran kebencian. Selain itu, ada upaya untuk mengatur transaksi elektronik, yang penting dalam ekonomi digital yang berkembang pesat.

Sedangkan perbedaan mencolok antara regulasi UU ITE Indonesia dan regulasi keamanan siber di negara lain dapat dilihat pada hal keseimbangan antara keamanan siber dan kebebasan berekspresi (Syahrin, 2020). Di beberapa negara, regulasi keamanan siber mereka lebih mengedepankan aspek perlindungan hak asasi manusia, termasuk kebebasan berekspresi. Ini berarti bahwa dalam merancang dan menerapkan hukum siber, negara-negara tersebut memberikan perhatian khusus untuk memastikan bahwa tindakan keamanan siber tidak secara tidak semestinya membatasi hak-hak dasar seperti kebebasan berekspresi, privasi, dan akses informasi. Sedangkan UU ITE sering dikritik karena potensi penyalahgunaannya dalam membatasi kebebasan berekspresi. Selain itu, dalam konteks penanganan data pribadi, UU ITE belum sekomprehensif General Data Protection Regulation (GDPR), yakni regulasi yang diterapkan oleh Uni Eropa (EU) dalam hal hak individu atas data mereka.

Perbandingan antara perbedaan dan kesamaan ini memberikan pencerahan untuk membuat kebijakan nasional sehingga dapat disesuaikan dengan standar internasional. Hal ini perlu dilakukan karena dengan menyesuaikan standar hukum siber internasional, dapat membantu dalam menghadapi kejahatan siber yang sifatnya sudah lintas batas. Selain itu, Peningkatan regulasi siber melalui peningkatan kerjasama antarlembaga juga memberikan dampak yang signifikan pada peningkatan efektivitas keamanan siber. Meskipun ditemukan bahwa efketivitas dari sinergi lembaga-lembaga—seperti Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), Kepolisian Republik Indonesia (Polri), dan lembaga lainnya termasuk sektor swasta—masih belum berjalan efektif (Yusuf et al., 2021). Ditemukan dalam banyak kasus, regulasi keamanan siber di negara-negara lain dirancang dengan sangat mempertimbangkan hak kebebasan berekspresi, memastikan bahwa upaya untuk menjaga keamanan siber tidak secara tidak adil membatasi hak individu untuk berbicara dan menyampaikan pendapat. Sedangkan di Indonesia, UU ITE sering dikritik karena dianggap tidak cukup memperhatikan keseimbangan ini. Namun, upaya peningkatan sinergitas ini tetap perlu dilakukan agar kementerian dan lembaga dapat turut serta mengantisipasi ancaman siber Kerjasama ini bisa mencakup berbagai bentuk, seperti pertukaran informasi tentang ancaman siber, pengembangan standar keamanan bersama, dan latihan bersama untuk meningkatkan kesiapsiagaan terhadap serangan siber.

*Pertama*, pertukaran informasi tentang ancaman siber antarlembaga memainkan peran penting dalam memperkuat keamanan siber secara kolektif. Ketika lembaga-lembaga berbagi data tentang serangan terbaru, taktik penipuan, atau kerentanan keamanan yang teridentifikasi, setiap entitas menjadi lebih siap dan responsif terhadap ancaman yang muncul. Proses pertukaran informasi ini memungkinkan lembaga-lembaga untuk belajar dari pengalaman satu sama lain dan secara proaktif mengadaptasi strategi keamanan mereka. Misalnya, jika satu lembaga mengidentifikasi sebuah metode serangan siber baru, informasi ini dapat dibagikan dengan cepat, memungkinkan lembaga lain untuk segera mengimplementasikan langkah-langkah pertahanan atau mitigasi yang diperlukan. *Kedua*, pengembangan standar keamanan bersama oleh berbagai lembaga merupakan langkah penting dalam menciptakan kerangka kerja yang konsisten untuk melindungi aset digital. Dengan adanya standar keamanan yang disepakati dan diterapkan secara luas, lembaga-lembaga dapat memastikan bahwa tingkat perlindungan terhadap aset digital mereka adalah seragam dan memadai. pengembangan standar keamanan bersama oleh berbagai lembaga membantu menciptakan kerangka kerja yang konsisten untuk melindungi aset digital. Ini termasuk pembuatan kebijakan yang memastikan implementasi praktik terbaik dalam keamanan siber di semua lembaga, meningkatkan keseragaman dan efektivitas dalam melawan ancaman siber. *Ketiga*, latihan bersama untuk meningkatkan kesiapsiagaan terhadap serangan siber sangat penting. Melalui simulasi serangan siber, lembaga-lembaga ini dapat mengidentifikasi kelemahan dalam sistem mereka dan memperbaikinya sebelum terjadi serangan nyata. Latihan ini juga membantu memperkuat koordinasi dan kerjasama antarlembaga dalam merespon insiden siber.

Dengan kerjasama antar lembaga memungkinkan integrasi berbagai perspektif dan keahlian, yang membantu dalam menciptakan regulasi siber yang lebih konsisten dan komprehensif (Waskita & Sidik, 2023). Ketika lembaga-lembaga dari berbagai bidang ini bekerja sama, mereka dapat saling melengkapi. Misalnya, lembaga teknologi dan keamanan siber dapat menyediakan wawasan tentang ancaman terkini dan kemajuan teknologi, sedangkan lembaga hukum dan hak asasi manusia dapat memastikan bahwa regulasi yang dikembangkan tidak hanya efektif dalam menangani kejahatan siber, tetapi juga menghormati hak-hak dasar dan kebebasan individu. Karena tiap lembaga akan membawa pemahaman uniknya masing-masing mengenai tantandangan dan solusi, sehingga cakupan regulasi menjadi semakin luas dan memfasilitasi berbagai sumber daya dari teknologi, data dan juga keahlian, sehingga kejahatan siber dapat diatasi dengan lebih baik dengan adanya fasilitas yang mendukung ini.

## 4. KESIMPULAN DAN SARAN/REKOMENDASI

### 4.1 Kesimpulan

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Indonesia memainkan peran krusial dalam kerangka hukum keamanan siber nasional. Namun, efektivitasnya dalam menangani kejahatan siber menghadapi tantangan signifikan, khususnya terkait isu pembatasan kebebasan berpendapat dan berekspresi dan ketidakjelasan dalam pasal-pasal tertentu menyebabkan kesulitan dalam penegakan hukum. Meskipun telah mengalami revisi untuk memperkuat kerangka hukum tersebut, masih ada kebutuhan untuk penyesuaian yang lebih lanjut. Ini terutama penting dalam konteks kejahatan siber yang terus berkembang dan kompleksitas teknologi digital modern. Penelitian ini menunjukkan bahwa untuk meningkatkan efektivitasnya, UU ITE memerlukan peninjauan dan pembaruan berkelanjutan, tidak hanya untuk mengatasi kelemahan internal, tetapi juga untuk menyesuaikan dengan perkembangan teknologi dan standar internasional melalui harmonisasi UU ITE dengan standar keamanan siber internasional. Meskipun ada upaya untuk harmonisasi, masih terdapat tantangan dalam memastikan kesesuaian penuh UU ITE dengan praktik keamanan siber global. Sehingga penelitian ini merekomendasikan adanya peningkatan kolaborasi internasional dan penyesuaian kebijakan.

### 4.2 Saran/Rekomendasi

Rekomendasi untuk pembaruan UU ITE, termasuk penyesuaian pasal-pasal yang multitafsir dan penguatan aspek perlindungan data pribadi. Peneliti juga menyarankan peningkatan kolaborasi antara pemerintah, sektor swasta, dan masyarakat sipil untuk meningkatkan kesadaran dan pendidikan keamanan siber. penelitian masa depan harus fokus pada evaluasi dampak amandemen UU ITE yang diusulkan, serta mengeksplorasi strategi baru dalam menangani kejahatan siber yang terus berkembang.

Kritik dan saran yang membangun dari pembaca sangat diharapkan oleh penulis guna membangun dan menyempurnakan penyusun jurnal selanjutnya. Karena penulis hanyalah manusia biasa yang tak pernah luput dari kesalahan.

## REFERENSI


Cipta, R. E., & Masyhar, A. (2021). *Controversial Criminal Punishment for Victim of the Spread of Immoral Chat*. *7*, 23–46.

Citra, Y., Desy, N. K., Pinatih, S. A., & Negara, S. P. (2023). *Strategi penanganan keamanan siber (cyber security) di Indonesia*. *6*, 1941–1949.

Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). *Populis : Jurnal Sosial Dan Humaniora*, *8*(1), 57–73. https://doi.org/10.47313/pjsh.v8i1.1957

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law Review*, *9*(1), 1–22.

Firmansyah, H., Shrishti, S., & Dumais, N. (2022). Interpretasi Pasal 28 Ayat (2) Frasa antar Golongan dalam Penerapan Undang-Undang Nomor 19 Tahun 2016. *Serina Iv*, *2*, 489–498.

Fuad, A. M. (2023). *Perlindungan Data Pribadi Cloud Computing System (Google Drive) Ditinjau Dari Perspektif Undang Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik*. *1*(1), 21–38.

Hamanduna, A. O. L., & Widjanarko, P. (2023). Discourse network on the revision of Indonesian information and electronic transaction law. *Jurnal Studi Komunikasi (Indonesian Journal of Communications Studies)*, *7*(2), 519–538. https://doi.org/10.25139/jsk.v7i2.5496

Irawan, J. E. (2023). Tinjauan Yuridis Tentang Kepastian Hukum Kewenangan Perusahaan Dalam Penggeledahan Ponsel Pribadi Karyawan. *Krtha Bhayangkara*, *17*(1), 107–118.

https://doi.org/10.31599/krtha.v17i1.2045

Ishaq, I., & Ridwan, M. (2023). A study of umar bin Khatab's Ijtihad in an effort to formulate Islamic law reform. *Cogent Social Sciences*, *9*(2), 2265522.

Jahriyah, V. F., Moch. Tommy Kusuma, Kuni Qonitazzakiyah, & Muh. Ali Fathomi. (2021). Kebebasan Berekspresi di Media Elektronik Dalam Perspektif Pasal 27 Ayat (3) Undang- Undang Nomor 19 Tahun 2016 Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Pelayanan Transaksi Elektronik (UU ITE). *Sosio Yustisia: Jurnal Hukum Dan Perubahan Sosial*, *1*(2), 65–87. https://doi.org/10.15642/sosyus.v1i2.96

Kemit, J. F., Surabaya, U. A., & H, V. A. (2023). *Yuridiksi Kejahatan Siber: Borderless*. *2*(1312100154), 55–70.

Komala, F., & Ridwan, M. (2022). KEINDAHAN HUKUM ISLAM. *Jurnal Indragiri Penelitian Multidisiplin*, *2*(3), 140–146.

Nanda, D. H., & Hariyanta, F. A. (2022). Problematika Operasionalisasi Delik Pasal 27 Ayat (3) Uu Ite Dan Formulasi Hukum Perlindungan Freedom of Speech Dalam Ham. *Jurnal Hukum Dan Pembangunan Ekonomi*, *9*(2), 214. https://doi.org/10.20961/hpe.v9i2.52779

Ramadhani, F. (2023). Dinamika UU ITE Sebagai Hukum Positif Fi Indonesia Guna Meminimalisisr Kejahatan Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *1*(1), 89–97.

Ridwan, M., Saleh, A. S., & Ghaffar, A. (2021). Islamic Law In Morocco: Study on The Government System and The Development of Islamic Law. *ARRUS Journal of Social Sciences and Humanities*, *1*(1), 13–22.

Rizal, M. R. R., & Wondabio, L. S. (2023). Analisis Inkonsistensi Antara Kinerja Dengan Kepercayaan Publik Pada Komisi Pemberantasan Korupsi. *Jurnal Aplikasi Akuntansi*, *7*(2), 236–253. https://doi.org/10.29303/jaa.v7i2.192

Rohmy, A. M., Suratman, T., & Nihayaty, A. I. (2021). UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi. *Dakwatuna: Jurnal Dakwah Dan Komunikasi Islam*, *7*(2), 309. https://doi.org/10.54471/dakwatuna.v7i2.1202

Saly, J. N., Ekalia, E., & Tarumanagara, U. (2023). Status Perlindungan Hukum Kepada Masyarakat Setempat Terkait Relokasi Pulau Rempang. *Jurnal Kewarganegaraan*, *7*(2), 1668–1676.

Sufiyah, P. (n.d.). *Penegakan Hukum Di Indonesia Untuk Si Kaya Dan Si Miskin*.

Syahrin, M. A. (2020). Konsep Keabsahan Kontrak Elektronik Berdasarkan Hukum Nasional Dan Uncitral Model Law On Electronic Commerce. *Repertorium Jurnal Ilmiah Hukum Kenotariatan*, *9*(2), 105–122. https://doi.org/10.28946/rpt.v9i2.419

Waskita, A. S., & Sidik, H. (2023). Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019. *Padjadjaran Journal of International Relations*, *5*(2), 142. https://doi.org/10.24198/padjir.v5i2.41337

Wijaya, Y. V., Erfina, A., & Warman, C. (2021). Analisis Sentimen Seputar UU ITE Menggunakan Algoritma Support Vector Machine. *Progresif: Jurnal Ilmiah Komputer*, *17*(2), 1. https://doi.org/10.35889/progresif.v17i2.644

Yusuf, Y., Prananda, A. &, & Gultom, R. A. G. (2021). Synergy of Intelligence Institutions in facing cyber threats in Indonesia. *Jurnal Peperangan Asimetris*, *7*(1), 51–70.