

Pengaruh Penerapan Undang-Undang ITE Terhadap Tingkat Kejahatan Siber Di Indonesia

Aldi ferdiansyah^a, Berdi Adityas Wiryawan Wahyono^b, Almansyah Harahap^c, Evan Gustian^d,
Dzakwan Zaidan^e

^aUniversitas Bengkulu, fakultas hukum, aldiferdiansyah9111@gmail.com

^bUniversitas Bengkulu, fakultas hukum, aditberdi17@gmail.com

^cUniversitas Bengkulu, fakultas hukum, almanharahap123@gmail.com

^dUniversitas Bengkulu, fakultas hukum, evanlinggau2019@gmail.com

^eUniversitas Bengkulu, fakultas hukum, dzakwanzaidan13@gmail.com

Abstract

This study aims to examine the impact of the implementation of the Electronic Information and Transactions Law (UU ITE) on the level of cybercrime in Indonesia. The background of this research highlights that the rapid digital transformation has significantly altered societal interactions while simultaneously creating opportunities for the growth of cybercrimes, such as ransomware attacks, phishing, and personal data theft. This research employs an empirical-normative approach through a literature review and a comparative analysis of cybercrime data before and after the implementation of UU ITE. The study involves an in-depth examination of legal sources, government reports, and case studies to identify challenges in regulatory enforcement and the shortcomings of digital security systems. Findings indicate that while UU ITE provides a clear legal framework, gaps in its implementation have been exploited by cybercriminals to evade legal repercussions. The assessment of regulatory effectiveness emphasizes that strengthening law enforcement capacity and enhancing information technology infrastructure are crucial aspects in reducing cybercrime rates. This study offers policy recommendations for refining digital regulations and improving inter-agency coordination in addressing cyber threats.

Keywords: Cybercrime, Regulation, Security, Enforcement, Digital

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license



PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa dampak signifikan dalam berbagai aspek kehidupan, termasuk dalam dunia ekonomi, sosial, hingga keamanan. Perkembangan teknologi yang pesat telah mendorong transformasi digital yang semakin kompleks, memungkinkan aksesibilitas informasi yang lebih luas dan efisien bagi masyarakat global. Di Indonesia, adopsi teknologi digital meningkat pesat, terlihat dari jumlah pengguna internet yang mencapai 212,9 juta pada awal 2023, yang berarti hampir 77% dari total populasi telah terhubung dengan dunia digital¹. Fenomena ini memperlihatkan bagaimana teknologi telah mengubah pola perilaku masyarakat dalam berinteraksi, bekerja, hingga melakukan transaksi. Namun, di balik kemudahan tersebut, teknologi juga membuka peluang bagi meningkatnya *cybercrime* atau kejahatan siber yang terus berkembang mengikuti inovasi teknologi. Kejahatan siber tidak hanya terbatas pada pencurian identitas atau pembobolan rekening bank, tetapi juga mencakup bentuk kejahatan baru seperti serangan *ransomware*, penyebaran *malware*, hingga eksploitasi data pribadi untuk kepentingan ekonomi ilegal². Kelemahan dalam sistem keamanan siber yang belum optimal semakin mempermudah pelaku kejahatan dalam mengeksploitasi celah keamanan yang ada.

Kemunculan berbagai teknologi baru seperti kecerdasan buatan (*artificial intelligence*), *Internet of Things* (IoT), dan *blockchain* telah mengubah lanskap kejahatan siber menjadi lebih kompleks. Pemanfaatan kecerdasan buatan oleh pelaku kejahatan siber telah memungkinkan terciptanya skema kejahatan yang lebih canggih, seperti serangan berbasis *deepfake*, pencurian data biometrik, dan manipulasi informasi digital dalam skala yang lebih luas. Di sisi lain, penggunaan *blockchain* dalam transaksi mata uang kripto juga menjadi tantangan tersendiri dalam upaya penegakan hukum, sebab sistem desentralisasi yang dimiliki oleh teknologi ini memungkinkan transaksi yang lebih anonim dan sulit dilacak oleh aparat penegak hukum. Hal ini memunculkan tantangan bagi regulasi di berbagai negara, termasuk Indonesia, yang masih tertinggal dalam hal adaptasi terhadap kejahatan siber berbasis teknologi baru. Dalam konteks regulasi di Indonesia, Undang-Undang Informasi dan Transaksi

¹ We Are Social. (2023). Jumlah Pengguna Internet di Indonesia. <https://inet.detik.com/telecommunication/d-6582738/jumlah-pengguna-internet-ri-tembus-2129-juta-di-awal-2023>

² AllahRakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, 16(2), 23–54. <https://doi.org/10.22201/ij.24485306e.2024.2.18892>

Elektronik (UU ITE) berperan penting dalam menangani berbagai bentuk kejahatan siber, tetapi masih terdapat celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan untuk menghindari jerat hukum. Studi menunjukkan bahwa banyak kasus *cybercrime* yang tidak tertangani dengan optimal karena adanya keterbatasan dalam implementasi UU ITE serta kurangnya pemahaman aparat penegak hukum dalam menghadapi serangan siber yang lebih canggih³.

Perkembangan kejahatan siber di Indonesia semakin pesat dengan maraknya kasus pencurian data dan peretasan sistem yang menyerang berbagai institusi, termasuk lembaga keuangan, perusahaan swasta, hingga instansi pemerintahan. Salah satu kasus yang menjadi perhatian adalah kebocoran data yang dialami oleh BPJS Kesehatan pada tahun 2021, di mana lebih dari 279 juta data penduduk Indonesia diduga bocor dan diperjualbelikan di forum gelap (*dark web*)⁴. Kejadian serupa juga terjadi pada sejumlah perusahaan e-commerce, seperti Tokopedia pada tahun 2020, di mana sekitar 91 juta data pengguna mengalami kebocoran akibat serangan peretas. Kasus-kasus ini menunjukkan bahwa sistem keamanan digital di Indonesia masih lemah dan memerlukan penguatan baik dalam aspek regulasi maupun penerapan teknologi keamanan siber yang lebih canggih. Dengan semakin berkembangnya teknologi, pendekatan dalam menangani kejahatan siber harus bersifat lebih proaktif dan adaptif terhadap perubahan. Regulasi yang ada saat ini, seperti UU ITE, perlu diperbarui agar lebih relevan dengan tantangan keamanan digital yang terus berkembang. Kerja sama antara pemerintah, sektor swasta, dan masyarakat sipil sangat dibutuhkan dalam membangun sistem keamanan siber yang lebih tangguh dan responsif terhadap ancaman yang semakin kompleks.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) terus menjadi perdebatan publik karena penerapannya yang dianggap bertentangan dengan prinsip kebebasan berpendapat dalam sistem demokrasi Indonesia. Salah satu tantangan utama dalam implementasi UU ITE adalah adanya *pasal karet*, yakni ketentuan yang memiliki tafsir luas sehingga dapat digunakan secara subjektif untuk menjerat individu atau kelompok tertentu. Pasal 27 ayat (3), Pasal 28 ayat (2), dan Pasal 45A sering dikritik karena dianggap memberikan peluang bagi aparat penegak hukum untuk menindak individu atas dasar pencemaran nama baik atau ujaran kebencian, meskipun konteksnya adalah kritik yang sah terhadap pemerintah atau pejabat publik⁵. Situasi ini berimplikasi pada meningkatnya fenomena *self-censorship*, di mana masyarakat menjadi enggan menyampaikan opini kritis di media sosial karena takut dijerat hukum. Interpretasi yang berlebihan terhadap UU ITE sering kali dimanfaatkan oleh pihak-pihak berkepentingan, termasuk aktor politik, untuk membungkam kritik dan mengontrol wacana publik di ranah digital. Sebagai contoh, kasus kriminalisasi aktivis dan jurnalis menunjukkan bahwa UU ITE dapat dijadikan alat untuk membungkam oposisi politik dan meredam diskusi terbuka terkait kebijakan pemerintah⁶. Selain aspek hukum, tantangan lainnya datang dari lemahnya literasi digital di kalangan masyarakat, yang menyebabkan banyak orang tidak memahami batasan antara kebebasan berekspresi dan pelanggaran hukum dalam konteks digital. Penegakan hukum yang belum merata dan transparansi dalam penerapan UU ITE juga menjadi permasalahan, karena banyak kasus yang diproses secara selektif sesuai dengan kepentingan tertentu, bukan berdasarkan kepentingan keadilan. Dengan meningkatnya kasus kriminalisasi berbasis UU ITE, banyak pihak menyerukan perlunya revisi terhadap pasal-pasal yang berpotensi mengekang kebebasan berekspresi, termasuk dengan menetapkan batasan yang lebih jelas terhadap definisi ujaran kebencian dan pencemaran nama baik. Keberadaan UU ITE seharusnya bertujuan untuk menciptakan lingkungan digital yang aman dan kondusif, namun jika tidak diterapkan secara adil dan transparan, maka justru akan menjadi ancaman bagi demokrasi serta mempersempit ruang kebebasan berekspresi di Indonesia.

Urgensi penelitian ini terletak pada perlunya evaluasi mendalam mengenai sejauh mana penerapan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) berpengaruh terhadap tingkat kejahatan siber di Indonesia. Dengan perkembangan teknologi digital yang semakin pesat, kasus kejahatan siber seperti *hacking*, *phishing*, *identity theft*, serta penyebaran konten ilegal terus mengalami peningkatan, sehingga efektivitas UU ITE sebagai instrumen hukum perlu dikaji secara komprehensif. Regulasi yang bertujuan untuk menekan kejahatan digital ini

³ Rolando, D. M., Aulia, H. H., Rahmaningsih, A. A., & Andani, M. T. (2023). Transformasi Digital dan Ancaman Cybercrime. *Siyasah: Jurnal Hukum Tata Negara*, 3(1), 69–86. <https://doi.org/10.32332/siyasah.v4i1>

⁴ Cyber Security. (2023). Kasus Cyber Crime di Indonesia. <https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/>

⁵ Rahmadani, A., Paramita, M. L., Haura, S., & Firman, F. (2024). *Regulasi Digital dan Implikasinya Terhadap Kebebasan Berpendapat Pada Undang-Undang ITE Pada Platform Media Sosial di Indonesia*. *Journal of Social Contemplativa*, 2(1), 01-18. <https://idreach.com/Journal/index.php/JSC>

⁶ Nur, Z., & Mahzaniar, M. (2022). *Implementasi Undang-Undang Transaksi Elektronik (UU ITE) Ditinjau Berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) Terhadap Kebebasan Berekspreasi Masyarakat di Media Sosial*. *Jurnal Smart Hukum (JSH)*, 1(1), 223-228. <https://doi.org/10.55299/jsh.v1i1.153>

tidak hanya harus mampu melindungi pengguna internet dari ancaman siber, tetapi juga harus diterapkan secara adil dan transparan agar tidak menjadi alat represif yang membatasi kebebasan berekspresi di dunia maya. Kajian literatur menjadi pendekatan yang tepat untuk menganalisis berbagai perspektif dalam implementasi UU ITE, dengan mengeksplorasi dampaknya terhadap dinamika kejahatan siber serta bagaimana regulasi ini dapat diselaraskan dengan kebijakan perlindungan data dan hak digital masyarakat. Studi ini juga akan mengidentifikasi tantangan utama dalam penerapannya, termasuk aspek penegakan hukum, interpretasi pasal yang masih multitafsir, serta efektivitasnya dalam memberikan rasa aman bagi pengguna internet di Indonesia. Penelitian ini diharapkan dapat memberikan kontribusi akademik dan rekomendasi kebijakan yang lebih relevan dalam penguatan regulasi digital guna menanggulangi ancaman siber secara optimal.

METODE PENELITIAN

Metodologi penelitian ini menggunakan pendekatan *empiris-normatif*, yaitu dengan menggabungkan analisis normatif terhadap regulasi hukum yang berlaku dengan kajian empiris berdasarkan data dan temuan di lapangan. Penelitian ini bersifat *literature review* yang menelaah berbagai sumber hukum, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan regulasi turunannya, serta mengkaji jurnal ilmiah, artikel akademik, laporan pemerintah, dan studi kasus yang relevan dalam membahas kejahatan siber serta regulasi digital. Penelitian ini juga memanfaatkan data dari lembaga penegak hukum, Kementerian Komunikasi dan Informatika (Kominfo), serta organisasi yang berfokus pada keamanan siber untuk mendapatkan gambaran empiris mengenai dinamika kejahatan siber di Indonesia. Teknik analisis data dalam penelitian ini dilakukan dengan studi komparatif terhadap tingkat kejahatan siber sebelum dan sesudah implementasi UU ITE guna mengukur efektivitas regulasi tersebut. Penelitian ini menggunakan analisis konten terhadap berbagai penelitian terdahulu yang membahas efektivitas UU ITE dalam mengurangi atau mengendalikan kejahatan digital. Identifikasi pola dan tren dari berbagai temuan ilmiah juga dilakukan untuk melihat bagaimana penerapan UU ITE memengaruhi dinamika dunia siber, baik dari segi keamanan maupun implikasinya terhadap hak digital masyarakat. Dengan pendekatan ini, penelitian dapat memberikan gambaran holistik tentang efektivitas serta tantangan dalam implementasi UU ITE di Indonesia.

HASIL DAN PEMBAHASAN

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk dalam pola kejahatan. Kejahatan siber atau *cyber crime* di Indonesia mengalami peningkatan yang signifikan, seiring dengan semakin meluasnya penggunaan internet dan perangkat digital. Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2021-2022 mencapai 210,03 juta orang, meningkat 6,78% dari tahun sebelumnya⁷. Lonjakan jumlah pengguna internet ini turut meningkatkan potensi kejahatan digital, mulai dari pencurian identitas, penipuan daring, hingga serangan siber terhadap infrastruktur penting. Kejahatan siber yang awalnya hanya sebatas *hacking* dan *carding* kini berkembang menjadi ancaman yang lebih kompleks, termasuk serangan *malware*, *ransomware*, dan *phishing* yang menargetkan perusahaan serta individu. Fenomena ini semakin diperparah dengan rendahnya kesadaran masyarakat terhadap keamanan digital, yang menyebabkan banyak pengguna internet menjadi korban kejahatan siber tanpa disadari.

Kejahatan siber di Indonesia mulai muncul sejak tahun 1983, dengan sektor perbankan menjadi target utama serangan digital. Seiring waktu, jenis kejahatan siber semakin bervariasi, meliputi pembajakan perangkat lunak, penyebaran konten ilegal, penipuan daring, serta pencurian data pribadi. Berdasarkan data dari Kementerian Komunikasi dan Informatika (Kominfo), kasus kejahatan siber yang paling sering terjadi di Indonesia meliputi *carding*, *phishing*, *cyber espionage*, dan *ransomware*⁸. Dalam beberapa tahun terakhir, kasus pencurian data pengguna semakin marak, seperti kebocoran data 279 juta penduduk Indonesia dari BPJS Kesehatan pada tahun 2021 dan kebocoran data aplikasi e-HAC Kementerian Kesehatan pada tahun yang sama. Kasus-kasus ini menunjukkan bahwa selain pelaku individu, kelompok kriminal siber terorganisir juga semakin aktif di Indonesia, memanfaatkan celah keamanan sistem digital untuk keuntungan finansial maupun kepentingan lain.

Salah satu faktor utama meningkatnya kejahatan siber di Indonesia adalah kurangnya kesadaran masyarakat tentang keamanan digital dan lemahnya regulasi dalam menindak kejahatan siber. Dalam banyak kasus, pengguna

⁷ Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). *Survei Profil Internet Indonesia 2022*. <https://survei.apjii.or.id/>

⁸ Kominfo. (2021). *Kominfo Tangani Dugaan Kebocoran Data Aplikasi E-HAC*. <https://aptika.kominfo.go.id/2021/09/kominfo-tangani-dugaan-kebocoran-data-aplikasi-e-hac/>

internet di Indonesia masih kurang memahami pentingnya perlindungan data pribadi, sehingga sering kali menjadi korban serangan *phishing* atau pencurian identitas. Sistem keamanan digital yang lemah juga menjadi penyebab utama kebocoran data dan serangan siber. Laporan dari Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan menyebutkan bahwa Indonesia menghadapi lebih dari 1,225 miliar serangan siber setiap harinya, dengan ancaman *ransomware* menjadi yang paling dominan⁹. Serangan ini tidak hanya menargetkan individu tetapi juga institusi pemerintah dan perusahaan besar, yang sering kali belum memiliki sistem keamanan yang cukup kuat untuk menangkalkan serangan tersebut. Kondisi ini semakin memburuk dengan meningkatnya penggunaan perangkat digital tanpa adanya edukasi yang memadai tentang ancaman keamanan siber.

Sebagai upaya untuk menekan angka kejahatan siber, pemerintah Indonesia telah mengambil beberapa langkah strategis, seperti pembentukan Badan Siber dan Sandi Negara (BSSN) serta kerja sama dengan berbagai lembaga internasional dalam menangani ancaman digital¹⁰. Peningkatan literasi digital juga menjadi faktor penting dalam pencegahan kejahatan siber. Kampanye edukasi mengenai pentingnya keamanan data pribadi, penggunaan kata sandi yang kuat, serta kewaspadaan terhadap modus penipuan daring menjadi langkah preventif yang dapat membantu mengurangi risiko kejahatan siber. Dalam jangka panjang, penguatan kebijakan keamanan siber yang berbasis pada teknologi canggih, seperti *artificial intelligence* dan *big data*, juga menjadi solusi untuk menghadapi ancaman digital yang semakin kompleks. Kejahatan siber di Indonesia merupakan fenomena yang terus berkembang, sehingga diperlukan strategi yang adaptif dan berkelanjutan dalam menghadapi tantangan ini¹¹.

Undang-Undang Informasi dan Transaksi Elektronik memiliki kedudukan khusus dalam melindungi aktivitas digital masyarakat. Peraturan tersebut memuat ketentuan pidana yang bertujuan menghalangi perbuatan melanggar hukum pada berbagai platform daring. Penegakan UU ITE berupaya memberikan kepastian hukum bagi korban serangan *malware*, pencemaran nama baik, dan bentuk pelanggaran siber lainnya. Pihak berwenang memanfaatkan ketentuan dalam undang-undang itu untuk menjerat pelaku kejahatan yang memanfaatkan celah dunia maya. Aparat penegak hukum tetap menghadapi kesulitan dalam hal pembuktian digital, sehingga peningkatan kapasitas teknologi forensik menjadi hal penting. Tingkat kepatuhan masyarakat bergantung pada pemahaman terhadap batasan hukum dalam interaksi daring dan penerapan sanksi yang adil. Proses penindakan kejahatan digital tercermin pada sejumlah kasus yang menunjukkan perlunya kolaborasi intens antara kepolisian, kejaksaan, dan pengadilan¹².

Ketika menerapkan UU ITE, aparat penegak hukum memerlukan keahlian teknis, mengingat *cybercrime* bersifat dinamis dan menggunakan pola serangan yang kian canggih. Peningkatan pemahaman forensik siber mendukung pengungkapan bukti digital secara tepat dan mengurangi potensi kekeliruan dalam menilai sebuah tindak kejahatan. Penerapan pasal-pasal UU ITE terkait ujaran kebencian, pencemaran nama baik, hingga penipuan daring membuktikan bahwa regulasi ini mampu menjangkau pelaku tindak pidana di ranah virtual. Program sosialisasi edukatif perlu digalakkan untuk meningkatkan kesadaran masyarakat akan risiko serangan digital dan ancaman pidana yang menanti. Lembaga penegak hukum juga perlu membangun sinergi dengan entitas lain semisal Kominfo maupun lembaga internasional. Kontrol dan pengawasan dalam jaringan sangat dipengaruhi oleh dukungan infrastruktur, termasuk penangkal *malware* serta pemindaian otomatis konten ilegal. Efektivitas penindakan baru terwujud jika penanganan teknis sejalan dengan asas keadilan hukum yang tercantum dalam UU ITE¹³.

⁹ Rachmadie, D. T. (2020). *Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016*. *RECIDIVE*, 9(2), 128–156. <https://jurnal.uns.ac.id/recidive/article/view/47400>

¹⁰ Center for Digital Society Fisipol UGM. (2021). *The Existence of Indonesia Cyber Police: What does it mean for Us Netizens?*. <https://digitalsociety.id/2021/02/05/the-existence-of-indonesia-cyber-police-what-does-it-mean-for-us-netizens/>

¹¹ Rowe, N. C. (2019). *Honeypot Deception Tactics*. Dalam *Autonomous Cyber Deception* (hlm. 35–45). https://faculty.nps.edu/ncrowe/honeypot_deception_tactics.htm

¹² Elan, E., Situmeang, A., & Girsang, J. (2022). *Efektivitas Undang-Undang ITE dalam menangani ujaran kebencian melalui media sosial di Kota Batam*. *Jurnal Pendidikan Kewarganegaraan Undiksha*, 10(3), 83–100. <https://doi.org/10.23887/jpku.v10i3.51205>

¹³ Yana, E., Amboro, F. Y. P., Nurisman, E., & Hadiyati, N. (2021). *The role of the Polri in the law enforcement of the distribution of hate speech in the city of Batam, Indonesia*. *Ganesha Law Review*, 3(1), 43–55. <https://doi.org/10.23887/glr.v3i1.321>

Pembuktian tindak kejahatan digital di pengadilan memerlukan saksi ahli teknologi, dokumen digital yang sah, serta interpretasi pasal UU ITE yang tidak merugikan hak-hak konstitusional. Kolaborasi lintas sektor, antara lain universitas dan lembaga penelitian, diharapkan membantu polisi dan jaksa dalam menyiapkan bukti digital yang lengkap. Efektivitas UU ITE kian meningkat saat masyarakat dilibatkan melalui pemahaman tentang etika bermedia, pelebagaan literasi digital, dan pemanfaatan mekanisme pengaduan yang transparan. Regulasi yang mengikat pengguna internet menekan lonjakan *cybercrime* melalui peran sanksi yang tegas dan bersifat pencegahan. Penegakan hukum tidak cuma bersandar pada pembalasan, melainkan juga menekankan peringatan dan rehabilitasi pelaku yang terlibat kasus kejahatan daring. Sejumlah pengamat menekankan perlunya interpretasi UU ITE yang seimbang agar tindak pidana siber tertangani secara tepat tanpa menghambat kebebasan berekspresi. Artinya, keberhasilan UU ITE bergantung pada keselarasan antara kemampuan teknologi kepolisian, kematangan yuridis, dan kesadaran publik¹⁴.

Undang-Undang Informasi dan Transaksi Elektronik (*UU ITE*) memiliki peran yang signifikan dalam mengatur dan menertibkan interaksi digital di Indonesia. Namun, penerapannya juga menimbulkan kekhawatiran serius terkait potensi penyalahgunaan terhadap kebebasan berekspresi. Beberapa pasal dalam *UU ITE*, terutama Pasal 27 ayat (3) yang mengatur tentang pencemaran nama baik dan Pasal 28 ayat (2) yang melarang penyebaran kebencian berbasis SARA, memiliki ruang interpretasi yang luas dan dapat disalahgunakan untuk menekan opini publik¹⁵. Kasus-kasus yang melibatkan jurnalis, aktivis, dan masyarakat umum yang mengkritik pemerintah menunjukkan bahwa regulasi ini dapat digunakan sebagai alat untuk membungkam perbedaan pendapat. Di banyak situasi, individu yang menyampaikan kritik terhadap kebijakan negara sering kali dikriminalisasi dengan tuduhan pencemaran nama baik, meskipun kritik tersebut didasarkan pada data dan fakta yang valid. Hal ini bertentangan dengan semangat demokrasi yang menempatkan kebebasan berekspresi sebagai pilar utama dalam pemerintahan yang sehat. Ada celah besar dalam regulasi yang memungkinkan penyalahgunaan kekuasaan terhadap hak-hak konstitusional warga negara.

UU ITE juga sering kali digunakan secara tidak proporsional dalam menindak ujaran yang dianggap sebagai penghinaan atau penyebaran kebencian, tanpa memperhatikan konteks dan niat dari pernyataan tersebut. Dalam banyak kasus, individu yang menghadapi tuntutan berdasarkan *UU ITE* sebenarnya hanya mengekspresikan pendapat mereka di media sosial tanpa maksud untuk mencemarkan nama baik atau menyebarkan kebencian¹⁶. Namun, pasal-pasal yang bersifat *multitafsir* ini memungkinkan pihak yang merasa dirugikan, termasuk pejabat negara dan elite politik, untuk melaporkan seseorang hanya karena perbedaan pendapat¹⁷. Di sinilah letak permasalahan mendasar dari penerapan *UU ITE*: kurangnya kejelasan definisi hukum dan standar yang jelas dalam membedakan kritik yang sah dengan penghinaan. Akibatnya, hukum tidak hanya menjadi alat perlindungan bagi masyarakat dari kejahatan digital, tetapi juga dapat berfungsi sebagai instrumen represi yang melanggar hak-hak asasi manusia yang telah dijamin dalam konstitusi. Dalam konteks ini, revisi terhadap pasal-pasal yang problematik menjadi sangat mendesak agar tidak terus menjadi senjata bagi mereka yang ingin membungkam kebebasan berpendapat.

Kekhawatiran lainnya yang muncul dari implementasi *UU ITE* adalah bagaimana hukum ini diterapkan secara tidak adil dan selektif. Studi menunjukkan bahwa dalam banyak kasus, individu yang berafiliasi dengan kekuasaan sering kali lebih terlindungi dari jeratan *UU ITE*, sementara pihak oposisi atau mereka yang dianggap sebagai "pengkritik" lebih sering menjadi target kriminalisasi. Fenomena ini menunjukkan bahwa *UU ITE* tidak hanya memiliki kelemahan dalam substansi hukumnya, tetapi juga dalam aspek implementasi dan penegakan hukum. Beberapa kasus yang melibatkan tokoh-tokoh tertentu membuktikan bahwa delik-delik dalam *UU ITE* sering kali diproses lebih cepat ketika menyangkut kritik terhadap pemerintah dibandingkan ketika kasus yang sama

¹⁴ Disemadi, H. S. (2021). *Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia*. Jurnal Wawasan Yuridika, 5(2), 177–199. <https://doi.org/10.25072/jwy.v5i2.460>

¹⁵ Koalisi Masyarakat Sipil. (2021). *Catatan dan Desakan Masyarakat Sipil atas Revisi UU ITE*. https://icjr.or.id/wp-content/uploads/2021/04/kertas_posisi_revisi_UU_ITE.pdf

¹⁶ Aditya, Z. F., & Al-Fatih, S. (2021). *Indonesian constitutional rights: expressing and purposing opinions on the internet*. The International Journal of Human Rights, 25(9), 1395–1419. <https://doi.org/10.1080/13642987.2020.1826450>

¹⁷ Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). *Pedoman Implementasi UU ITE*. <https://aptika.kominfo.go.id/2021/06/pedoman-implementasi-uu-ite-berbentuk-buku-saku/>

menimpa tokoh pro-pemerintah¹⁸. Hal ini menciptakan ketidakadilan hukum yang semakin memperburuk citra demokrasi di Indonesia. Sistem hukum yang seharusnya berfungsi sebagai alat keadilan justru menjadi alat politik yang mengekang kebebasan berekspresi bagi mereka yang tidak sejalan dengan narasi penguasa. Konsekuensi dari penerapan hukum yang diskriminatif ini adalah meningkatnya ketakutan di kalangan masyarakat untuk mengekspresikan pendapat mereka secara terbuka, yang pada akhirnya menghambat peran media sosial sebagai ruang diskusi publik yang sehat.

SIMPULAN

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah membentuk kerangka hukum untuk menangani beragam kejahatan di dunia digital, mulai dari pencemaran nama baik hingga pencurian data dan aktivitas siber lain yang bersifat transnasional. Peningkatan jumlah pengguna internet dan evolusi teknologi di Indonesia berdampak pada melonjaknya kasus kejahatan siber, termasuk serangan *ransomware*, penipuan daring, serta eksploitasi data pribadi. Analisis temuan menunjukkan bahwa UU ITE berkontribusi dalam memberikan perlindungan hukum dan kepastian prosedur penindakan, meskipun masih terdapat kerentanan dalam pembuktian digital dan kelemahan koordinasi antar lembaga. Beberapa kasus kebocoran data yang dialami institusi publik dan swasta juga memunculkan pandangan bahwa penerapan UU ITE dan perangkat hukum terkait belum optimal menekan angka kejahatan siber.

Tantangan dalam penerapan UU ITE tercermin dari beberapa hambatan, seperti tumpang tindih regulasi, kurangnya literasi digital di kalangan masyarakat, dan potensi penyalahgunaan pasal-pasal yang bersifat multitafsir. Meski kehadiran UU ITE sudah membantu menindak pelaku kejahatan, kasus pencurian data berskala besar dan serangan terhadap infrastruktur kritis mengisyaratkan bahwa kerangka hukum memerlukan penyesuaian lebih lanjut. Pelibatan aparat penegak hukum dengan kapasitas teknis forensik digital, serta kolaborasi dengan pihak internasional, menjadi kunci untuk menghadapi kejahatan siber yang bersifat lintas negara. Ketika regulasi, kapasitas kelembagaan, dan penegakan hukum dapat dikembangkan selaras, maka dampak negatif kejahatan siber bagi individu, sektor usaha, dan pemerintahan dapat ditekan secara lebih efektif.

DAFTAR PUSTAKA

- Aditya, Z. F., & Al-Fatih, S. (2021). *Indonesian constitutional rights: expressing and purposing opinions on the internet*. The International Journal of Human Rights, 25(9), 1395–1419. <https://doi.org/10.1080/13642987.2020.1826450>
- AllahRakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, 16(2), 23–54. <https://doi.org/10.22201/ijl.24485306e.2024.2.18892>
- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). *Survei Profil Internet Indonesia 2022*. <https://survei.apjii.or.id/>
- Center for Digital Society Fisipol UGM. (2021). *The Existence of Indonesia Cyber Police: What does it mean for Us Netizens?*. <https://digitalsociety.id/2021/02/05/the-existence-of-indonesia-cyber-police-what-does-it-mean-for-us-netizens/>
- Cyber Security. (2023). Kasus Cyber Crime di Indonesia. <https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/>
- Disemadi, H. S. (2021). *Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia*. Jurnal Wawasan Yuridika, 5(2), 177–199. <https://doi.org/10.25072/jwy.v5i2.460>
- Elan, E., Situmeang, A., & Girsang, J. (2022). *Efektivitas Undang-Undang ITE dalam menangani ujaran kebencian melalui media sosial di Kota Batam*. Jurnal Pendidikan Kewarganegaraan Undiksha, 10(3), 83–100. <https://doi.org/10.23887/jpku.v10i3.51205>
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). *Pedoman Implementasi UU ITE*. <https://aptika.kominfo.go.id/2021/06/pedoman-implementasi-uu-ite-berbentuk-buku-saku/>
- Koalisi Masyarakat Sipil. (2021). *Catatan dan Desakan Masyarakat Sipil atas Revisi UU ITE*. https://icjr.or.id/wp-content/uploads/2021/04/kertas_posisi_revisi_UU_ITE.pdf
- Kominfo. (2021). *Kominfo Tangani Dugaan Kebocoran Data Aplikasi E-HAC*. <https://aptika.kominfo.go.id/2021/09/kominfo-tangani-dugaan-kebocoran-data-aplikasi-e-hac/>
- Nur, Z., & Mahzaniar, M. (2022). *Implementasi Undang-Undang Transaksi Elektronik (UU ITE) Ditinjau Berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) Terhadap Kebebasan Bereksresi Masyarakat di Media Sosial*. Jurnal Smart Hukum (JSH), 1(1), 223–228. <https://doi.org/10.55299/jsh.v1i1.153>
- Rachmadie, D. T. (2020). *Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016. RECIDIVE*, 9(2), 128–156. <https://jurnal.uns.ac.id/recidive/article/view/47400>

¹⁸ Siregar, G., & Lubis, M. R. (2021). *Juridical analysis of religious blasphemy crimes through smartphone application based on the information and electronic transaction law*. Journal of Contemporary Issues in Business and Government, 27(2), 1006–1012. <https://doi.org/10.47750/cibg.2021.27.02.131>

- Rahmadani, A., Paramita, M. L., Haura, S., & Firman, F. (2024). *Regulasi Digital dan Implikasinya Terhadap Kebebasan Berpendapat Pada Undang-Undang ITE Pada Platform Media Sosial di Indonesia*. *Journal of Social Contemplativa*, 2(1), 01-18. <https://idereach.com/Journal/index.php/JSC>
- Rolando, D. M., Aulia, H. H., Rahmaningsih, A. A., & Andani, M. T. (2023). Transformasi Digital dan Ancaman Cybercrime. *Siyasah: Jurnal Hukum Tata Negara*, 3(1), 69–86. <https://doi.org/10.32332/siyasah.v4i1>
- Rowe, N. C. (2019). *Honeypot Deception Tactics*. Dalam *Autonomous Cyber Deception* (hlm. 35–45). https://faculty.nps.edu/ncrowe/honeypot_deception_tactics.htm
- Siregar, G., & Lubis, M. R. (2021). *Juridical analysis of religious blasphemy crimes through smartphone application based on the information and electronic transaction law*. *Journal of Contemporary Issues in Business and Government*, 27(2), 1006–1012. <https://doi.org/10.47750/cibg.2021.27.02.131>
- We Are Social. (2023). Jumlah Pengguna Internet di Indonesia. <https://inet.detik.com/telecommunication/d-6582738/jumlah-pengguna-internet-ri-tembus-2129-juta-di-awal-2023>
- Yana, E., Amboro, F. Y. P., Nurisman, E., & Hadiyati, N. (2021). *The role of the Polri in the law enforcement of the distribution of hate speech in the city of Batam, Indonesia*. *Ganesha Law Review*, 3(1), 43–55. <https://doi.org/10.23887/glr.v3i1.321>