CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 10 No 11 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

05PERBANDINGAN HUKUM TINDAK PIDANA SIBER ANTARA INDONESIA DENGAN SINGAPURA

Syadid Jiddan Alharun
Universitas Bengkulu
jiddansyadid@gmail.com

Abstract

In the digital era, cybercrime has dynamically evolved, posing serious threats to individuals, corporations, and governments. Indonesia and Singapore adopt different legal approaches to addressing cybercrime. Indonesia relies on the Electronic Information and Transactions Law (UU ITE), which is more repressive and faces various implementation challenges, including fragmented authority and low digital literacy among the public. In contrast, Singapore enforces the Cybersecurity Act, which emphasizes a risk-based approach, centralized coordination, and more effective mitigation policies. This study aims to analyze the differences in cyber regulations between the two countries and evaluate their effectiveness in law enforcement. Using normative legal research methods and a comparative legal approach, this study finds that risk-based regulations with strong coordination are more effective in combating cyber threats than reactive approaches. Therefore, regulatory reforms in Indonesia are necessary to enhance the effectiveness of cyber law enforcement, including strengthening inter-agency coordination, improving law enforcement capacity, and implementing broader digital literacy strategies.

Keywords: *Cybercrime, cyber regulation, cybercriminal law, UU ITE, Cybersecurity Act, comparative law.*

Abstrak

Dalam era digital, kejahatan siber berkembang secara dinamis dan menjadi ancaman serius bagi individu, perusahaan, serta pemerintah. Indonesia dan Singapura memiliki pendekatan hukum yang berbeda dalam menanggulangi tindak pidana siber. Indonesia mengandalkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang lebih bersifat represif dan menghadapi berbagai tantangan dalam implementasinya, termasuk fragmentasi kewenangan dan rendahnya literasi digital masyarakat. Sebaliknya, Singapura menerapkan *Cybersecurity Act*, yang mengedepankan pendekatan berbasis risiko, koordinasi yang lebih terpusat, serta kebijakan mitigasi yang lebih efektif. Penelitian ini bertujuan untuk menganalisis perbedaan regulasi siber di kedua negara dan menilai efektivitasnya dalam penegakan hukum. Dengan menggunakan metode penelitian hukum normatif dan pendekatan perbandingan hukum, penelitian ini menemukan bahwa regulasi siber yang

Article History
Received: February 2025
Reviewed: February 2025
Published: February 2025
Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/CAUSA.v1i2.365
Copyright : Author
Publish by : CAUSA

berbasis mitigasi risiko dan koordinasi yang kuat lebih efektif dalam menangani ancaman kejahatan siber dibandingkan pendekatan yang masih bersifat reaktif. Oleh karena itu, diperlukan reformasi regulasi di Indonesia untuk meningkatkan efektivitas penegakan hukum siber, termasuk penguatan koordinasi antar lembaga, peningkatan kapasitas aparat penegak hukum, serta strategi literasi digital yang lebih luas.
Kata kunci: Kejahatan siber, regulasi siber, hukum pidana siber, UU ITE, *Cybersecurity Act*, perbandingan hukum.

PENDAHULUAN

A. Latar Belakang

Dalam era digital yang semakin berkembang pesat, penggunaan teknologi informasi telah menjadi bagian tak terpisahkan dari kehidupan masyarakat modern. Kemudahan akses internet dan perkembangan ekosistem digital membuka peluang besar bagi berbagai sektor, namun, di saat yang sama juga menghadirkan ancaman baru berupa kejahatan siber yang terus mengalami evolusi dalam pola dan modus operandinya. Berbagai bentuk kejahatan, seperti pencurian data pribadi, penipuan daring, serangan *ransomware*, serta peretasan terhadap infrastruktur kritis, semakin sering terjadi, bahkan menyasar tidak hanya individu dan perusahaan, tetapi juga lembaga pemerintahan.

Seiring dengan meningkatnya ketergantungan terhadap teknologi digital, dampak dari kejahatan siber pun semakin luas, mencakup aspek ekonomi, sosial, hingga keamanan nasional.[1] Banyak individu dan perusahaan mengalami kerugian finansial yang signifikan akibat pencurian identitas dan penipuan daring,[2] sementara kebocoran data yang bersifat rahasia dapat merusak reputasi institusi, menurunkan kepercayaan masyarakat terhadap layanan digital, serta mengganggu stabilitas bisnis dan pemerintahan.[3] Di beberapa kasus, serangan siber bahkan berimplikasi pada gangguan infrastruktur penting, seperti sistem perbankan, jaringan komunikasi, hingga layanan kesehatan, menunjukkan bahwa ancaman ini tidak dapat dianggap remeh.

Dalam menghadapi tantangan tersebut, regulasi menjadi instrumen utama yang digunakan untuk menanggulangi kejahatan siber dan melindungi kepentingan publik. Di Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi dasar hukum dalam menangani berbagai kasus kejahatan siber, meskipun masih menghadapi berbagai kritik terkait implementasi dan efektivitasnya dalam menghadapi perkembangan modus kejahatan yang semakin canggih. Sementara itu, Singapura telah mengadopsi pendekatan hukum yang lebih komprehensif melalui *Cybersecurity Act*, yang tidak hanya mengatur aspek hukum pidana

[1] Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum. *JURNAL BEVINDING*, *2*(01), 44–55.
[2] Iskandar, O. (2024). Analisis Kejahatan Online Phishing Pada Masyarakat. Leuser: Jurnal Hukum Nusantara, 1(2), 32-36.
[3] Azmi, M. N. A., Saifudin, H., Purba, C. T., Suryaningtyas, A., & Situmorang, U. S. (2024). Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan: Indonesia. *Jurnal Multidisiplin Ilmu Akademik*, *1*(6), 448-458.

Jurnal Hukum dan Kewarganegaraan
Vol 10 No 11 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

dalam kejahatan siber, tetapi juga mencakup penguatan infrastruktur keamanan digital serta kerja sama internasional dalam menangani ancaman lintas batas.[4]

Meskipun kedua negara telah memiliki perangkat hukum dalam menanggulangi kejahatan siber, efektivitas dan implementasi regulasi tersebut masih menjadi isu yang terus berkembang, terutama dalam menyelaraskan perlindungan keamanan digital dengan hak-hak individu. Perdebatan tentang keseimbangan antara perlindungan privasi dan pengawasan negara masih menjadi isu yang belum sepenuhnya terselesaikan, terlebih dengan adanya kejahatan siber yang bersifat transnasional, yang menuntut kerja sama hukum antarnegara.

Kompleksitas persoalan ini menarik untuk dikaji lebih lanjut, terutama dalam melihat bagaimana perbedaan sistem hukum di Indonesia dan Singapura dalam merespons ancaman siber, menilai sejauh mana efektivitas kebijakan yang telah diterapkan, serta mengidentifikasi potensi langkah-langkah yang dapat diadopsi guna meningkatkan perlindungan terhadap keamanan digital, sehingga penulis tertarik mengangkat judul ini.

B. Rumusan Masalah

1. Bagaimana pengaruh perbedaan regulasi tindak pidana siber di Indonesia dan Singapura terhadap efektivitas penegakan hukum dalam kasus kejahatan siber?
2. Mengapa regulasi tindak pidana siber di Indonesia masih menghadapi tantangan dalam implementasi dan efektivitasnya dibandingkan dengan Singapura?

C. Tujuan

1. Untuk menganalisis dan mendeskripsikan pengaruh perbedaan regulasi tindak pidana siber di Indonesia dan Singapura terhadap efektivitas penegakan hukum dalam kasus kejahatan siber.
2. Untuk menganalisis dan mendeskripsikan faktor-faktor yang menyebabkan regulasi tindak pidana siber di Indonesia masih menghadapi tantangan dalam implementasi dan efektivitasnya dibandingkan dengan Singapura.

METODE PENULISAN

1. Jenis Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif, yang meneliti hukum sebagai suatu sistem norma dengan mengkaji peraturan perundang-undangan, doktrin, serta prinsip-prinsip hukum yang berlaku.[5] Jenis penelitian ini dipilih karena penelitian berfokus pada analisis perbandingan regulasi tindak pidana siber di Indonesia dan Singapura serta efektivitas implementasinya dalam penegakan hukum. Pendekatan yang digunakan dalam penelitian ini adalah:

a. Pendekatan Peraturan Perundang-undangan (*Statute Approach*), yaitu dengan mengkaji ketentuan hukum positif yang berlaku di Indonesia (UU ITE) dan Singapura (*Cybersecurity Act*).

[4] Gorian, E. (2020). Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection. Dalam Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Economy and Production (hal. 1–9). Springer.
[5] Marzuki, P. M. (2017). *Penelitian Hukum* (Edisi Revisi). Prenada Media.

b. Pendekatan Perbandingan Hukum (*Comparative Approach*), yaitu dengan membandingkan kebijakan dan regulasi siber di Indonesia dan Singapura untuk menilai efektivitasnya.
c. Pendekatan Konseptual (*Conceptual Approach*), yaitu dengan mengkaji teori-teori hukum yang relevan, seperti teori efektivitas hukum Soerjono Soekanto dan teori hukum responsif Nonet & Selznick.

2. Sumber Data

Penelitian ini menggunakan data hukum yang terdiri dari bahan hukum primer dan bahan hukum sekunder:

a. Bahan Hukum Primer:
    1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya.
    2. *Cybersecurity Act* 2018 (Singapura).
    3. Peraturan pelaksana terkait di Indonesia dan Singapura yang mengatur tentang kejahatan siber.
b. Bahan Hukum Sekunder:
    1. Buku, jurnal, dan artikel ilmiah yang membahas hukum siber, efektivitas regulasi, serta implementasi kebijakan keamanan siber.
    2. Doktrin hukum dari para ahli mengenai efektivitas hukum dan model penegakan hukum siber.
    3. Laporan dari lembaga yang berwenang, seperti *Cyber Security Agency of Singapore* dan laporan dari Kementerian Komunikasi dan Informatika Indonesia.

3. Metode Pengumpulan Data

Metode pengumpulan data dalam penelitian ini dilakukan melalui studi kepustakaan (*library research*) dengan menelusuri sumber hukum primer dan sekunder. Pengumpulan data dilakukan dengan:

a. Menganalisis teks peraturan perundang-undangan terkait kejahatan siber.
b. Menelaah dokumen akademik, jurnal ilmiah, dan buku yang relevan.
c. Mengkaji laporan dari lembaga terkait untuk melihat bagaimana regulasi siber diterapkan dalam praktik.

4. Metode Analisis Data

Data yang diperoleh dianalisis dengan metode analisis kualitatif, yaitu dengan menginterpretasikan norma hukum, membandingkan regulasi di Indonesia dan Singapura, serta menilai efektivitasnya berdasarkan teori hukum yang relevan. Analisis ini dilakukan dengan:

a. Deskriptif-analitis, yaitu menggambarkan dan menjelaskan perbedaan regulasi tindak pidana siber di Indonesia dan Singapura.
b. Kritis-evaluatif, yaitu menilai efektivitas regulasi berdasarkan indikator efektivitas hukum menurut teori Soerjono Soekanto (faktor hukum, penegak hukum, sarana dan prasarana, masyarakat, serta budaya hukum).
c. Komparatif, yaitu membandingkan kelebihan dan kelemahan regulasi siber di kedua negara untuk memberikan rekomendasi perbaikan bagi sistem hukum di Indonesia.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 10 No 11 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

5. Kerangka Pemikiran

Kerangka pemikiran dalam penelitian ini didasarkan pada hubungan antara regulasi hukum siber, efektivitas penegakan hukum, dan model kebijakan keamanan siber. Pemikiran ini berangkat dari asumsi bahwa perbedaan pendekatan regulasi akan berpengaruh pada efektivitas penegakan hukum terhadap kejahatan siber.

a. Teori Efektivitas Hukum (Soerjono Soekanto) digunakan untuk menilai sejauh mana regulasi yang ada mampu ditegakkan secara optimal. Lima faktor yang berpengaruh terhadap efektivitas hukum yaitu:[6]
   1. Faktor hukum itu sendiri.
   2. Faktor penegak hukum.
   3. Faktor sarana dan prasarana.
   4. Faktor masyarakat.
   5. Faktor budaya hukum.
b. Teori Hukum Responsif (Nonet & Selznick) digunakan untuk membandingkan model regulasi siber di Indonesia dan Singapura. Regulasi berbasis pencegahan dan mitigasi risiko (seperti di Singapura) lebih sesuai dengan model hukum responsif dibandingkan regulasi yang lebih represif (seperti UU ITE di Indonesia).
c. Pendekatan Regulasi Berbasis Risiko (*Risk-Based Regulation*) digunakan untuk menjelaskan keunggulan model regulasi siber di Singapura yang lebih adaptif terhadap perkembangan teknologi dan ancaman kejahatan siber.

Dengan kerangka pemikiran ini, penelitian ini berusaha menunjukkan bahwa pendekatan regulasi yang lebih terstruktur, berbasis mitigasi risiko, dan memiliki koordinasi yang kuat lebih efektif dalam menangani kejahatan siber dibandingkan dengan pendekatan yang masih bersifat reaktif dan fragmentaris.

PEMBAHASAN

1. Pengaruh Perbedaan Regulasi Tindak Pidana Siber di Indonesia dan Singapura terhadap Efektivitas Penegakan Hukum.

Hukum memiliki peran fundamental dalam menata masyarakat dan mengatur hubungan sosial, termasuk dalam ruang digital yang semakin kompleks. Dalam konteks tindak pidana siber, regulasi hukum harus mampu menyesuaikan diri dengan perkembangan teknologi informasi yang dinamis. Menurut teori efektivitas hukum yang dikemukakan oleh Soerjono Soekanto, efektivitas suatu regulasi bergantung pada lima faktor utama: Faktor hukum itu sendiri, penegak hukum, sarana dan prasarana, masyarakat, serta budaya hukum.[7] Menganalisis perbedaan regulasi tindak pidana siber antara Indonesia dan Singapura memerlukan pendekatan multidimensional untuk menilai sejauh mana hukum mampu berfungsi sebagaimana mestinya dalam menanggulangi kejahatan siber.

Dalam hukum pidana, dikenal dua model utama dalam perumusan norma, yaitu model represif dan preventif. Di Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) lebih cenderung mengedepankan pendekatan represif, di mana sanksi pidana menjadi instrumen utama dalam menangani pelanggaran di ruang digital. UU ITE mengalami berbagai

[6] Soekanto, S. (2007). Faktor-Faktor yang Mempengaruhi Penegakan Hukum. Jakarta: PT Raja Grafindo Persada.
[7] Soekanto, S. (2007). *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: PT Raja Grafindo Persada.

revisi sejak pertama kali disahkan pada tahun 2008, mencerminkan dinamika perkembangan hukum siber di Indonesia. Namun, beberapa kajian menunjukkan bahwa implementasi regulasi ini masih memiliki sejumlah tantangan, terutama dalam hal kepastian hukum dan perlindungan hak-hak digital masyarakat.[8] Menurut Rahardjo (2000), hukum siber di Indonesia masih bersifat reaktif, di mana respons terhadap kejahatan siber lebih banyak terjadi setelah peristiwa terjadi, bukan melalui mekanisme pencegahan yang ketat.[9]

Berbeda dengan Indonesia, Singapura menerapkan *Cybersecurity Act* 2018, yang memiliki pendekatan lebih komprehensif dan preventif. *Cybersecurity Act* memberikan kewenangan luas kepada *Cyber Security Agency (CSA)* untuk menangani ancaman siber secara sistematis dan terstruktur.[10] Dalam perspektif teori hukum responsif (Nonet & Selznick, 1978), regulasi semacam ini lebih adaptif terhadap perubahan lingkungan sosial dan teknologi. Kebijakan hukum Singapura menekankan pentingnya mitigasi risiko serta peningkatan kesiapan infrastruktur keamanan siber.[11] Hal ini sejalan dengan konsep *deterrence theory* dalam kriminologi yang menekankan bahwa ancaman hukuman bukan satu-satunya faktor penekan kejahatan, tetapi juga kesiapan sistem dalam mendeteksi dan mencegah pelanggaran sebelum terjadi.

Salah satu aspek yang membedakan kedua negara dalam implementasi hukum siber adalah koordinasi antar lembaga. Di Indonesia, penegakan hukum terhadap tindak pidana siber sering kali melibatkan banyak lembaga dengan kewenangan yang tumpang tindih, termasuk Kementerian Komunikasi dan Informatika (Kominfo), Kepolisian, dan Badan Siber dan Sandi Negara (BSSN). Hal ini dapat menyebabkan fragmentasi kebijakan dan inkonsistensi dalam implementasi aturan. Menurut studi, hambatan koordinasi antar lembaga merupakan salah satu faktor yang menghambat efektivitas penegakan hukum siber di Indonesia.[12] Sebaliknya, Singapura memiliki struktur yang lebih terpusat di bawah koordinasi CSA, yang bertanggung jawab atas keamanan siber secara nasional dan memiliki wewenang dalam menentukan langkah-langkah strategis untuk mencegah serta menangani insiden siber.[13]

Pendekatan hukum juga dipengaruhi oleh filosofi legislasi yang mendasari pembentukan regulasi tersebut. Dalam konteks hukum pidana siber, Indonesia masih berorientasi pada perlindungan hukum pidana klasik, di mana fokus utama adalah penegakan hukum setelah terjadinya tindak pidana. Sementara itu, Singapura lebih condong pada pendekatan regulasi berbasis risiko (*risk-based regulation*), di mana strategi keamanan siber dirancang untuk mengidentifikasi, menganalisis, dan mengurangi risiko sebelum pelanggaran terjadi.[14] Menurut

[8] Aprilianti, A. (2025). "Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi". *Begawan Abioso*, vol. 15, no. 1, pp. 41-50.
[9] Rahardjo, S. (2000). Ilmu hukum. Citra Aditya Bakti.
[10] Gorian, E. (2020). Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection. Dalam Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Economy and Production (hal. 1–9). Springer.
[11] Sukmana, T., Ashari, Z. S., & Darmawan, Y. (2023). Responsive Law and Progressive Law: Examining the Legal Ideas of Philip Nonet, Philip Selznick, and Sadjipto Raharjo. Peradaban Journal of Law and Society, 2(1), 92–106.
[12] Pamungkas, A. T., Muliyono, A., & Lahangatubun, N. (2024). Krisis Penegakan Hukum Cybercrime di Indonesia: Hambatan dan Solusi. Delictum: Jurnal Hukum dan Ilmu Sosial, 4(2), 123–135.
[13] Cyber Security Agency of Singapore. (2021). *The Singapore Cybersecurity Strategy 2021*. Cyber Security Agency of Singapore.
[14] Herbert Smith Freehills. (2024). Singapore expands the scope of the Cybersecurity Act. Cybersecurity Notes.

Cheng (2020), pendekatan berbasis risiko lebih efektif dalam menangani kejahatan siber karena mampu menyesuaikan dengan perkembangan ancaman yang terus berubah.[15]

Selain perbedaan dalam pendekatan regulasi dan implementasi, efektivitas hukum siber juga dipengaruhi oleh aspek kepatuhan dan budaya hukum masyarakat. Lawrence Friedman (1975) menjelaskan bahwa keberhasilan suatu regulasi tidak hanya ditentukan oleh aturan yang ada, tetapi juga oleh penerimaan dan pemahaman masyarakat terhadap hukum tersebut. Di Indonesia, masih terdapat kesenjangan antara peraturan yang berlaku dan kesadaran hukum digital masyarakat.[16] Tingkat literasi digital yang rendah menjadi salah satu faktor utama yang menyebabkan maraknya kejahatan siber, baik yang dilakukan dengan sengaja maupun akibat kurangnya pemahaman terhadap batasan hukum dalam ruang digital. Sebaliknya, Singapura memiliki tingkat literasi digital yang lebih tinggi, serta program edukasi keamanan siber yang didukung oleh pemerintah dan sektor swasta, yang secara tidak langsung meningkatkan efektivitas regulasi.[17]

Dengan mempertimbangkan berbagai teori hukum yang telah dibahas, dapat disimpulkan bahwa efektivitas penegakan hukum siber sangat dipengaruhi oleh karakteristik regulasi yang diterapkan, kesiapan infrastruktur hukum, koordinasi antar lembaga, serta budaya hukum masyarakat. Studi perbandingan antara Indonesia dan Singapura menunjukkan bahwa regulasi yang lebih terstruktur, berbasis risiko, dan memiliki pendekatan preventif lebih efektif dalam menghadapi kejahatan siber dibandingkan regulasi yang masih bersifat reaktif dan fragmentaris.

2. Kendala Implementasi Regulasi Tindak Pidana Siber di Indonesia terhadap Efektivitas Penegakan Hukum Dibandingkan dengan Singapura.

Dalam lanskap hukum siber, efektivitas regulasi tidak hanya diukur dari keberadaan aturan tertulis, tetapi juga dari bagaimana regulasi tersebut diterapkan dalam praktiknya. Indonesia telah memiliki perangkat hukum yang mengatur tindak pidana siber, namun dalam penerapannya masih ditemukan berbagai tantangan yang menghambat efektivitasnya. Situasi ini mengundang pertanyaan mengenai faktor-faktor yang menyebabkan regulasi di Indonesia belum mampu memberikan hasil optimal, terutama jika dibandingkan dengan Singapura yang berhasil menegakkan sistem hukum siber yang lebih solid.

Struktur regulasi siber di Indonesia didasarkan pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta perangkat hukum turunannya. Meski telah mengalami beberapa kali revisi, aturan tersebut masih menghadapi kritik terkait penerapannya yang dinilai kurang adaptif terhadap dinamika kejahatan siber yang terus berkembang.[18] Di sisi lain, Singapura telah membangun sistem regulasi yang lebih holistik dengan mengedepankan prinsip mitigasi risiko yang jelas dan kewenangan yang terpusat.[19] Perbedaan ini mendorong analisis

[15] Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, 1(2), 172-191.
[16] Friedman, L. M. (1975). The Legal System: A Social Science Perspective. Russell Sage Foundation.
[17] Center for Digital Society. (2021). Belajar dari Tata Kelola Keamanan Siber Singapura. Center for Digital Society, Universitas Gadjah Mada.
[18] Salsabilla, A., & Angelina, J. (2024). Peran Hukum Pidana dalam Menangani Kejahatan Siber pada Era Digital di Indonesia. JERUMI: Journal of Education, Religion, Humanities, and Multidisciplinary, 2(2), 1545–1555.
[19] Pusat Studi Keamanan dan Perdamaian Universitas Gadjah Mada. (2021). Belajar dari Tata Kelola Keamanan Siber Singapura. Center for Digital Society

lebih lanjut mengenai penyebab masih adanya kendala dalam implementasi regulasi tindak pidana siber di Indonesia.

Dalam teori hukum, keberhasilan suatu regulasi dipengaruhi oleh kesinambungan antara norma hukum, penegak hukum, dan kesiapan sistem pendukungnya. Dalam kasus Indonesia, aspek normatif yang diatur dalam UU ITE belum sepenuhnya mampu menyesuaikan diri dengan kejahatan siber yang semakin kompleks. Kejahatan siber bersifat dinamis, berkembang seiring dengan kemajuan teknologi, sementara regulasi hukum sering kali mengalami keterlambatan dalam merespons perubahan ini. Akibatnya, beberapa jenis kejahatan yang muncul belakangan, seperti serangan *ransomware* yang menyerang infrastruktur kritis atau manipulasi data berbasis kecerdasan buatan, tidak sepenuhnya diakomodasi oleh regulasi yang ada. Keadaan ini menyebabkan celah dalam penegakan hukum yang dimanfaatkan oleh para pelaku kejahatan siber.

Di samping aspek normatif, tantangan implementasi juga berkaitan dengan kapasitas lembaga penegak hukum dalam menangani kejahatan siber. Penegakan hukum dalam ruang digital menuntut pemahaman yang mendalam mengenai mekanisme kerja teknologi informasi dan teknik investigasi forensik digital yang canggih.[20] Namun, di Indonesia, kesiapan aparatur penegak hukum dalam menghadapi tantangan ini masih terbatas. Kurangnya pelatihan khusus di bidang keamanan siber menyebabkan proses investigasi terhadap kejahatan siber sering kali mengalami kendala teknis dan administratif. Keterbatasan ini berimplikasi pada rendahnya tingkat keberhasilan dalam mengungkap pelaku kejahatan siber serta lemahnya daya cegah terhadap kasus serupa di masa mendatang.

Faktor lain yang turut mempengaruhi efektivitas implementasi regulasi di Indonesia adalah fragmentasi kewenangan antara berbagai institusi yang bertanggung jawab atas keamanan siber.[21] Di Singapura, *Cyber Security Agency (CSA)* bertindak sebagai lembaga sentral yang mengoordinasikan kebijakan keamanan siber dan penegakan hukumnya. Sistem ini memungkinkan adanya satu garis komando yang jelas dalam menangani insiden siber serta meminimalkan tumpang tindih kewenangan.[22] Sebaliknya, di Indonesia, pengelolaan keamanan siber melibatkan berbagai lembaga, termasuk Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), serta Kepolisian Republik Indonesia. Tidak adanya koordinasi yang terintegrasi menyebabkan kebijakan yang diterapkan sering kali berjalan sendiri-sendiri tanpa sinergi yang optimal.[23] Akibatnya, respons terhadap ancaman siber menjadi kurang efisien dan sering kali bersifat reaktif dibandingkan preventif.

Selain kendala struktural dan teknis, faktor budaya hukum juga berperan dalam menentukan efektivitas regulasi tindak pidana siber. Kesadaran masyarakat terhadap hukum siber masih perlu ditingkatkan, mengingat masih banyak kasus di mana pelanggaran terjadi akibat kurangnya pemahaman mengenai batasan hukum dalam ruang digital.[24] Fenomena

[20] Prakoso, A. (2022). Tantangan Pembuktian dalam Kasus Kejahatan Siber. Jurnal Hukum dan Peradilan, 11(2), 123–145.
[21] Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(2), 222-238.
[22] Purnomo, A. (2023). Analisis Implementasi Kebijakan Keamanan Siber di Singapura. Journal of Social and Economics Research, 2(3), 45–60.
[23] Cornelia, S. Strategi Penanganan Keamanan Siber (Cyber Security) di Indonesia. Jurnal Review Politik dan Pemerintahan, 1(1), 2022, 9.
[24] Manurung, E. T., & Siregar, M. (2023). Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional. Jurnal Inovatif, 5(1), 44–56.

penyebaran informasi hoaks, penggunaan data pribadi tanpa izin, serta peretasan akun digital menunjukkan bahwa masih terdapat kesenjangan antara regulasi yang ada dan kesadaran publik dalam mematuhi aturan tersebut. Di Singapura, pendekatan berbasis literasi digital telah menjadi bagian dari kebijakan keamanan siber nasional, di mana pemerintah secara aktif melibatkan masyarakat dan sektor swasta dalam upaya peningkatan kesadaran serta mitigasi risiko.[25] Model ini memungkinkan adanya partisipasi aktif dari berbagai pihak dalam mendukung keberhasilan regulasi siber.

Jika ditelusuri lebih dalam, keberhasilan regulasi di Singapura juga ditopang oleh hubungan erat antara pemerintah dan sektor industri teknologi. Kolaborasi ini menciptakan sistem di mana perusahaan-perusahaan digital memiliki kewajiban hukum yang jelas dalam menjaga keamanan data dan infrastruktur digital mereka.[26] Di Indonesia, masih terdapat kesenjangan dalam penerapan kebijakan yang mengatur keterlibatan sektor swasta dalam sistem keamanan siber nasional. Beberapa perusahaan masih menghadapi dilema dalam menyeimbangkan kepentingan bisnis dan kepatuhan terhadap regulasi yang ada. Ketidakjelasan mekanisme kepatuhan ini menyebabkan lemahnya kontrol terhadap kebocoran data serta masih rentannya infrastruktur digital dari serangan siber.

Dari berbagai faktor yang telah dibahas, dapat disimpulkan bahwa tantangan utama dalam implementasi regulasi tindak pidana siber di Indonesia tidak hanya terletak pada aspek hukum, tetapi juga melibatkan dimensi teknis, struktural, dan sosial. Kompleksitas permasalahan ini menuntut adanya reformasi yang menyeluruh dalam pengelolaan keamanan siber di Indonesia. Penyelarasan regulasi dengan perkembangan teknologi, peningkatan kapasitas aparat penegak hukum, integrasi kebijakan antar lembaga, serta peningkatan literasi digital masyarakat menjadi langkah-langkah yang perlu diperkuat agar regulasi yang ada dapat berjalan secara efektif dan sesuai dengan kebutuhan zaman.

PENUTUP

1. Kesimpulan

a. Perbandingan regulasi antara Indonesia dan Singapura menunjukkan bahwa efektivitas hukum siber tidak hanya bergantung pada keberadaan perangkat peraturan, tetapi juga pada implementasi yang sistematis dan koordinasi antar lembaga. Indonesia masih menghadapi tantangan dalam memastikan bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dapat secara efektif mengakomodasi dinamika kejahatan siber. Sementara itu, Singapura dengan *Cybersecurity Act* telah menerapkan pendekatan berbasis risiko yang lebih adaptif dan preventif, memungkinkan penanganan ancaman siber secara lebih sistematis. Efektivitas penegakan hukum juga dipengaruhi oleh tingkat literasi digital masyarakat dan kesiapan infrastruktur keamanan siber yang menjadi penunjang utama keberhasilan kebijakan di masing-masing negara.
b. Implementasi regulasi tindak pidana siber di Indonesia masih dihadapkan pada sejumlah hambatan, termasuk lemahnya koordinasi antar lembaga, keterbatasan kapasitas aparatur penegak hukum dalam memahami dan menangani kejahatan siber, serta rendahnya

[25] Mok, K. H., Xu, H., & Zhang, X. (2022). Digital Transformation in Singapore: The Role of Government Policy and Public–Private Partnership. Journal of Asian Public Policy, 15(3), 1–19.
[26] Pusat Studi Keamanan dan Perdamaian Universitas Gadjah Mada. (2021). Belajar dari Tata Kelola Keamanan Siber Singapura. Center for Digital Society.

literasi digital masyarakat. Fragmentasi kewenangan antara berbagai institusi seperti Kominfo, BSSN, dan Kepolisian RI menyebabkan tumpang tindih kebijakan dan ketidakefisienan dalam respons terhadap insiden siber. Selain itu, pendekatan hukum yang lebih reaktif dibanding preventif mengakibatkan kejahatan siber sulit dicegah sejak dini, berbeda dengan Singapura yang telah membangun sistem keamanan siber yang lebih terintegrasi dan berbasis mitigasi risiko.

2. Saran

a. Pemerintah Indonesia perlu mengadopsi pendekatan berbasis risiko dalam kebijakan keamanan siber, sebagaimana diterapkan di Singapura. Hal ini mencakup pembentukan pusat koordinasi tunggal yang bertanggung jawab atas regulasi dan penegakan hukum siber secara nasional untuk mengurangi fragmentasi kewenangan. Selain itu, revisi terhadap UU ITE perlu dilakukan agar lebih responsif terhadap perkembangan teknologi dan modus operandi kejahatan siber yang terus berevolusi. Penguatan regulasi juga harus diimbangi dengan peningkatan kapasitas aparat penegak hukum dalam melakukan investigasi digital forensik serta penegakan hukum yang adil dan konsisten.

b. Upaya peningkatan efektivitas regulasi harus disertai dengan strategi peningkatan literasi digital di masyarakat. Program edukasi mengenai keamanan siber harus diperluas, baik melalui inisiatif pemerintah maupun kerja sama dengan sektor swasta dan akademisi. Selain itu, penerapan kebijakan yang mendorong kepatuhan sektor industri dalam menjaga keamanan data dan infrastruktur digital menjadi langkah penting untuk menciptakan ekosistem siber yang lebih aman. Keberhasilan Singapura dalam membangun kerja sama erat antara pemerintah, industri, dan masyarakat dapat menjadi model bagi Indonesia dalam meningkatkan ketahanan siber nasional secara lebih menyeluruh.

DAFTAR PUSTAKA

BUKU:

Aprilianti, A. (2025). "Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi". *Begawan Abioso*, 41-50.

Freehills, H. S. (2024). "Singapore expands the scope of the Cybersecurity Act". *Cybersecurity Notes*.

Friedman, L. M. (1975). *The Legal System: A Social Science Perspective.* Russell Sage Foundation.

Gorian, E. (2020). "Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection. Dalam Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Economy and Product". *Springer*, 1-9.

Mada, P. S. (2021). "Belajar dari Tata Kelola Keamanan Siber Singapura". *Center for Digital Society*.

Manurung, E. T. (2023). "Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional". *Jurnal Inovatif*, 44–56.

Marzuki, P. M. (2017). *Penelitian Hukum (Edisi Revisi).* Pranada Media.

Rahardjo, S. (2000). *Ilmu Hukum.* Citra Aditya Bakti.

Singapore., C. S. (2021). "The Singapore Cybersecurity Strategy 2021". *Cyber Security Agency of Singapore*.

Society, C. f. (2021). "Belajar dari Tata Kelola Keamanan Siber Singapura". *Center for Digital Society, Universitas Gadjah Mada.*

Soekanto, S. (2007). *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: PT Raja Grafindo Persada.

Sukmana, T. A. (2023). "Responsive Law and Progressive Law: Examining the Legal Ideas of Philip Nonet, Philip Selznick, and Sadjipto Raharjo". *Peradaban Journal of Law and Society*, 92–106.

Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). "Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum". *JURNAL BEVINDING*, 44–55.

BUKU:

Aji, M. P. (2023). "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]". *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 222-238.

Azmi, M. N., Saifudin, H., Purba, C. T., Suryaningtyas, A., & & Situmorang, U. S. (2024). "Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan: Indonesia". *Jurnal Multidisiplin Ilmu Akademik*, 448-458.

Cornelia, S. (2022). "Strategi Penanganan Keamanan Siber (Cyber Security) di Indonesia". *Jurnal Review Politik dan Pemerintahan*, 9.

Iskandar, O. (2024). "Analisis Kejahatan Online Phishing Pada Masyarakat". *Leuser: Jurnal Hukum Nusantara*, 32-36.

Mok, K. H. (2022). "Transformation in Singapore: The Role of Government Policy and Public–Private Partnership". *Journal of Asian Public Policy*, 1-19.

Pamungkas, A. T., Muliyono, A., & & Lahangatubun, N. (2024). "Krisis Penegakan Hukum Cybercrime di Indonesia: Hambatan dan Solusi". *Delictum: Jurnal Hukum dan Ilmu Sosial*, 123–135.

Prakoso, A. (2022). "Tantangan Pembuktian dalam Kasus Kejahatan Siber". *Jurnal Hukum dan Peradilan*, 123–145.

Purnomo, A. (2023). "Analisis Implementasi Kebijakan Keamanan Siber di Singapura". *Journal of Social and Economics Research*, 45–60.

Salsabilla, A., & & Angelina, J. (2024.). "Peran Hukum Pidana dalam Menangani Kejahatan Siber pada Era Digital di Indonesia". *JERUMI: Journal of Education, Religion, Humanities, and Multidisciplinary*, 1545–1555.

Soesanto, E., Romadhon, A., Mardika, B. D., & & Setiawan, M. F. (2023). "Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File". *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen*.

Sukmana, T., Ashari, Z. S., & & Darmawan, Y. (2023). "Responsive Law and Progressive Law: Examining the Legal Ideas of Philip Nonet, Philip Selznick, and Sadjipto Raharjo". *Peradaban Journal of Law and Society*, 92–106.