Jurnal Kolaboratif Sains
e-ISSN : 2623-2022
Homepage Journal: https://jurnal.unismuhpalu.ac.id/index.php/JKS

Perbandingan Hukum Siber Indonesia dengan Negara ASEAN: Suatu Kajian Normatif

Comparison of Indonesian Cyber Law with ASEAN Countries: A Normative Study

Muhammad Taufik Rusydi
Universitas Surakarta
***Corresponding Author**: **E-mail: mtaufikrusydi@gmail.com**

Artikel Penelitian

Article History:
Received: 3 Dec, 2024
Revised: 11 Dec, 2024
Accepted: 19 Dec, 2024

Kata Kunci:
Perbandingan Hukum; Hukum Siber; Hukum Siber ASEAN

Keywords:
Comparative Law; Cyber Law; ASEAN Cyber Law.

DOI: 10.56338/jks.v8i1.6536

ABSTRAK

Hukum siber telah menjadi isu penting di era digital, terutama di kawasan ASEAN, yang memiliki dinamika perkembangan teknologi informasi yang pesat. Artikel ini bertujuan untuk membandingkan kerangka hukum siber Indonesia dengan negara-negara ASEAN lainnya, seperti Singapura, Malaysia, dan Thailand. Kajian normatif ini menganalisis kelebihan, kelemahan, serta kesesuaian hukum siber Indonesia dengan standar internasional dan praktik terbaik di kawasan. Penelitian ini menggunakan pendekatan perbandingan dengan memeriksa undang-undang utama, seperti UU ITE di Indonesia, Computer Misuse Act di Singapura, dan Personal Data Protection Act di Malaysia. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki dasar hukum yang kuat melalui UU ITE, terdapat kelemahan dalam penegakan hukum, harmonisasi regulasi, dan perlindungan data pribadi. Sebagai rekomendasi, artikel ini mengusulkan pembaruan legislasi, peningkatan kapasitas penegak hukum, dan kerjasama regional yang lebih erat. Penelitian ini memberikan kontribusi bagi akademisi, pembuat kebijakan, dan masyarakat dalam memahami tantangan dan peluang hukum siber di ASEAN.

ABSTRACT

Cyber law has become an important issue in the digital era, especially in the ASEAN region, which has rapid dynamics in the development of information technology. This article aims to compare the cyber legal framework of Indonesia with other ASEAN countries, such as Singapore, Malaysia, and Thailand. This normative study analyzes the strengths, weaknesses, and conformity of Indonesian cyber law with international standards and best practices in the region. This study uses a comparative approach by examining key laws, such as the ITE Law in Indonesia, the Computer Misuse Act in Singapore, and the Personal Data Protection Act in Malaysia. The results of the study show that although Indonesia has a strong legal basis through the ITE Law, there are weaknesses in law enforcement, regulatory harmonization, and personal data protection. As recommendations, this article proposes legislative updates, increased law enforcement capacity, and closer regional cooperation. This study contributes to academics, policymakers, and the public in understanding the challenges and opportunities of cyber law in ASEAN.

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan, mulai dari ekonomi, sosial, hingga pemerintahan. Di kawasan Asia Tenggara (ASEAN), perkembangan ini sangat terasa dengan meningkatnya digitalisasi ekonomi dan pemerintahan. Sebagai contoh, laporan ASEAN *Digital Economy Framework* menunjukkan bahwa potensi ekonomi digital di ASEAN dapat mencapai USD 1 triliun pada 2030 (ASEAN, 2020). Namun, perkembangan ini juga membawa ancaman baru, yaitu kejahatan siber yang semakin kompleks.

Indonesia, sebagai salah satu negara anggota ASEAN, memiliki undang-undang khusus yang mengatur tentang teknologi informasi, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016. Undang-undang ini dirancang untuk mengatur aktivitas di dunia digital dan memberikan perlindungan hukum terhadap kejahatan siber. Namun, beberapa studi menunjukkan bahwa UU ITE masih memiliki kelemahan, terutama dalam hal harmonisasi dengan standar internasional, penegakan hukum, dan perlindungan data pribadi (Purbo, 2017; Raharjo, 2019).

Di sisi lain, negara-negara ASEAN lainnya, seperti Singapura, Malaysia, dan Thailand, telah mengembangkan kerangka hukum yang lebih spesifik dan adaptif terhadap kebutuhan era digital. Singapura, misalnya, memiliki *Computer Misuse Act* yang dianggap sebagai salah satu regulasi siber paling komprehensif di kawasan ini (Lim, 2018). Malaysia telah memberlakukan *Personal Data Protection Act* (PDPA) untuk mengatur pengelolaan data pribadi secara ketat (Idris, 2019). Thailand juga telah mengesahkan *Cybersecurity Act* pada 2019, yang menekankan pentingnya keamanan siber nasional.

Meskipun ASEAN memiliki kesepakatan untuk memperkuat kolaborasi dalam menghadapi ancaman siber, seperti yang tertuang dalam ASEAN *Framework on Personal Data Protection* dan ASEAN *Cybersecurity Cooperation Strategy*, harmonisasi kerangka hukum di antara negara-negara anggota masih menjadi tantangan besar. Perbedaan tingkat perkembangan ekonomi, prioritas nasional, dan kapasitas penegakan hukum menjadi hambatan utama (ASEAN, 2018). Di Indonesia, misalnya, regulasi siber cenderung bersifat reaktif dan sering kali tidak didukung oleh infrastruktur hukum yang memadai. Penegakan UU ITE juga menghadapi kritik karena dianggap lebih sering digunakan untuk membungkam kebebasan berekspresi daripada untuk menangani kejahatan siber secara efektif (Pratama, 2020). Situasi ini kontras dengan Singapura, di mana hukum siber diterapkan dengan pendekatan yang lebih preventif dan proaktif (Tan, 2019).

Penelitian ini bertujuan untuk membandingkan kerangka hukum siber di Indonesia dengan negara-negara ASEAN lainnya, khususnya Singapura, Malaysia, dan Thailand. Melalui pendekatan perbandingan hukum, penelitian ini akan menganalisis kelebihan, kelemahan, serta kesesuaian hukum siber Indonesia dengan standar internasional dan praktik terbaik di kawasan ASEAN. Penelitian ini memiliki beberapa kontribusi penting. Pertama, secara akademis, penelitian ini diharapkan dapat memperkaya literatur tentang hukum siber di ASEAN, khususnya yang berkaitan dengan perbandingan hukum. Kedua, penelitian ini memberikan masukan praktis bagi pembuat kebijakan di Indonesia dalam merumuskan pembaruan legislasi yang lebih adaptif dan harmonis dengan perkembangan internasional. Ketiga, bagi masyarakat umum, artikel ini dapat meningkatkan kesadaran akan pentingnya kerangka hukum yang kuat untuk melindungi hak dan kepentingan di dunia digital. Pendekatan perbandingan hukum digunakan dalam penelitian ini untuk memahami bagaimana regulasi siber di negara-negara ASEAN dapat saling melengkapi. Konsep utama yang menjadi landasan adalah legal transplants, yaitu proses adopsi elemen hukum dari satu sistem ke sistem lain untuk mencapai tujuan yang lebih baik (Watson, 1974). Dengan menggunakan kerangka ini, penelitian akan memeriksa apakah ada elemen regulasi siber di Singapura, Malaysia, dan Thailand yang dapat diadopsi oleh Indonesia untuk meningkatkan efektivitas UU ITE.

METODE

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perbandingan hukum (*comparative law approach*). Data diperoleh dari studi pustaka, meliputi analisis dokumen peraturan perundang-undangan, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, *Computer Misuse Act* di Singapura, dan *Personal Data Protection Act* di Malaysia. Sumber data sekunder meliputi jurnal ilmiah, buku hukum, dan laporan institusi. Analisis data dilakukan secara kualitatif deskriptif untuk mengidentifikasi kesamaan, perbedaan, dan implikasi hukum antarnegara. Pendekatan ini bertujuan untuk memahami kekuatan dan kelemahan kerangka hukum siber di Indonesia dalam konteks regional ASEAN (Marzuki, 2017).

HASIL DAN DISKUSI

Tinjauan Kerangka Hukum Siber di Indonesia

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) disahkan pada tahun 2008 melalui Undang-Undang Nomor 11 Tahun 2008 dan mengalami perubahan pada tahun 2016 dengan Undang-Undang Nomor 19 Tahun 2016. UU ITE menjadi kerangka hukum utama yang mengatur aktivitas di dunia maya di Indonesia, mencakup informasi elektronik, transaksi digital, hingga sanksi terhadap pelanggaran hukum di ruang siber. UU ITE bertujuan memberikan kepastian hukum dalam penggunaan teknologi informasi, melindungi hak masyarakat di dunia maya, serta mencegah dan menindak kejahatan siber (Rahayu, 2017).

UU ITE memiliki beberapa kekuatan yang signifikan: (1) Kerangka Hukum yang Komprehensif, UU ITE mencakup berbagai aspek dunia siber, mulai dari pengakuan dokumen elektronik sebagai alat bukti yang sah hingga pengaturan transaksi elektronik. Hal ini memberikan landasan hukum untuk berbagai aktivitas digital, termasuk *e-commerce*, komunikasi elektronik, dan perlindungan konsumen (Suryani, 2016). (2) Pengakuan Alat Bukti Elektronik, Pasal 5 UU ITE mengakui dokumen elektronik sebagai alat bukti hukum yang sah. Hal ini memperkuat penegakan hukum dalam kasus yang melibatkan transaksi digital atau kejahatan siber, seperti penipuan daring atau pelanggaran privasi (Handayani, 2018). (3) Penekanan pada Perlindungan Konsumen, UU ITE melindungi konsumen dari potensi penyalahgunaan teknologi, seperti pencurian identitas dan penipuan daring. Hal ini memberikan jaminan hukum bagi masyarakat dalam berinteraksi di dunia digital (Iswandi, 2017).

Sedangkan dari kelemahan yang ada pada UU ITE antara lain : (1) Pasal Multitafsir, Salah satu kelemahan utama UU ITE adalah keberadaan pasal-pasal multitafsir, seperti Pasal 27 Ayat (3) yang mengatur penghinaan dan pencemaran nama baik. Pasal ini kerap disalahgunakan untuk membatasi kebebasan berekspresi dan berpendapat (Susanti, 2018). (2) Ketiadaan Regulasi Khusus Perlindungan Data Pribadi, UU ITE belum mengatur secara rinci tentang perlindungan data pribadi, sehingga isu ini hanya diatur melalui peraturan menteri atau regulasi sektoral. Hal ini menyebabkan kurangnya standar yang seragam dalam perlindungan data pribadi (Wahyudi, 2019). (3) Keterbatasan Penegakan Hukum, Penegakan hukum terhadap kejahatan siber sering menghadapi kendala teknis dan sumber daya manusia. Kurangnya pemahaman aparat penegak hukum terhadap teknologi informasi menjadi hambatan signifikan dalam implementasi UU ITE (Rahman, 2016). (4) Tidak Responsif terhadap Perkembangan Teknologi, Sebagai produk hukum yang dirancang pada 2008, UU ITE tidak sepenuhnya mampu mengakomodasi perkembangan teknologi yang pesat, seperti *blockchain*, *artificial intelligence*, atau *metaverse*. Hal ini menyebabkan kebutuhan mendesak untuk pembaruan UU ITE (Fadilah, 2020). Kelemahan dalam UU ITE berimplikasi luas, termasuk meningkatnya kasus kriminalisasi masyarakat akibat pasal multitafsir, perlindungan data yang lemah, serta kurangnya kepercayaan masyarakat terhadap regulasi digital. Selain itu, kelemahan ini juga memengaruhi posisi

Indonesia dalam kerjasama internasional terkait kejahatan siber, seperti ASEAN *Cybersecurity Cooperation Strategy* (Nugraha, 2018).

Dari kelemahan yang ada pada UU ITE dan melihat kekuatan yang sudah ada pada UU ITE maka beberapa langkah strategis perlu dilakukan untuk memperkuat UU ITE : (1) Revisi Pasal Multitafsir, Revisi pasal multitafsir, khususnya yang terkait dengan pencemaran nama baik, dapat memberikan kejelasan hukum dan mencegah penyalahgunaan pasal tersebut (Anshori, 2019). (2) Pengesahan Undang-Undang Perlindungan Data Pribadi, Perlindungan data pribadi harus menjadi prioritas. Pengesahan Undang-Undang Perlindungan Data Pribadi yang terintegrasi dengan UU ITE dapat memperkuat perlindungan privasi masyarakat (Yusuf, 2020). (3) Peningkatan Kapasitas Penegak Hukum, Pelatihan dan pendidikan bagi aparat penegak hukum tentang teknologi informasi diperlukan untuk mendukung implementasi UU ITE secara efektif (Kusuma, 2017). (4) Harmonisasi dengan Hukum Internasional, UU ITE perlu disesuaikan dengan standar internasional, seperti Budapest Convention, untuk memperkuat kerjasama lintas negara dalam menghadapi kejahatan siber (Widodo, 2019).

Dalam kerangka hukum siber di kawasan ASEAN, tiga negara sering menjadi rujukan utama karena perkembangan legislasinya yang progresif, yaitu Singapura, Malaysia, dan Thailand. Ketiga negara ini memiliki undang-undang khusus yang mengatur berbagai aspek hukum siber, mulai dari keamanan informasi, perlindungan data pribadi, hingga penanganan kejahatan siber. Pembahasan berikut mengeksplorasi kerangka hukum siber di ketiga negara tersebut dengan fokus pada kelebihan, kelemahan, dan relevansi hukum yang mereka terapkan dalam konteks regional ASEAN.

Kerangka Hukum Siber di Singapura

Singapura diakui sebagai salah satu negara ASEAN dengan kerangka hukum siber yang paling maju. Peraturan-peraturan yang terkait dengan siber di Singapura mencerminkan komitmen negara ini untuk memastikan keamanan digital dan perlindungan data pribadi. Beberapa undang-undang utama di Singapura meliputi:

1. *Computer Misuse Act* (CMA)

   Computer Misuse Act (CMA) diperkenalkan pada tahun 1993 dan telah mengalami beberapa amandemen untuk mengakomodasi perkembangan teknologi terbaru. CMA bertujuan untuk mengatasi kejahatan siber seperti akses tidak sah ke sistem komputer, modifikasi data tanpa izin, dan penggunaan perangkat atau program yang dimaksudkan untuk pelanggaran hukum.

   Kelebihan CMA ialah memberikan definisi yang jelas terkait berbagai jenis kejahatan siber; mengakomodasi perkembangan ancaman keamanan teknologi, termasuk serangan ransomware dan malware. Sedangkan kelemahan dari CMA adalah fokus pada kejahatan berbasis teknologi informasi, dengan kurangnya regulasi terkait privasi pengguna di luar kerangka hukum perlindungan data.

2. *Personal Data Protection Act* (PDPA)

   Personal Data Protection Act (PDPA) adalah undang-undang yang mengatur pengelolaan data pribadi oleh organisasi. PDPA memberikan hak kepada individu atas data pribadi mereka, termasuk hak untuk memberikan persetujuan sebelum data dikumpulkan, digunakan, atau diungkapkan. Kelebihan dari PDPA ialah mendorong transparansi dan akuntabilitas organisasi dalam pengelolaan data pribadi; mencakup aturan ketat tentang transfer data lintas batas. Sedangkan kelemahan dari PDPA adalah terbatas pada entitas swasta, sehingga kurang menyentuh aspek penggunaan data oleh pemerintah.

Kerangka Hukum Siber di Malaysia

Malaysia adalah salah satu negara ASEAN yang memiliki regulasi hukum siber yang komprehensif. Peraturan yang relevan meliputi:

1. *Computer Crimes Act* 1997 (CCA)

   Computer Crimes Act (CCA) mengatur aktivitas ilegal yang menggunakan komputer atau jaringan komputer, seperti hacking, penyebaran virus, dan pencurian data elektronik. Kelebihan CCA antara lain : memberikan dasar hukum yang kuat untuk menindak pelaku kejahatan siber; mengatur dengan jelas sanksi pidana terhadap pelanggaran siber. Sedangkan kelemahan CCA adalah undang-undang ini tidak mencakup perlindungan data pribadi atau kerjasama internasional dalam mengatasi kejahatan siber lintas batas.

2. *Personal Data Protection Act* 2010 (PDPA)
   Personal Data Protection Act 2010 adalah undang-undang pertama di Malaysia yang secara khusus mengatur perlindungan data pribadi. PDPA menetapkan prinsip-prinsip penting dalam pengelolaan data pribadi, termasuk pemberitahuan, persetujuan, dan batasan penggunaan data. Kelebihan PDPA yaitu : mengadopsi prinsip-prinsip internasional dalam perlindungan data pribadi; memungkinkan mekanisme pengaduan bagi individu yang merasa haknya dilanggar. Sedangakan Kelemahan PDPA adalah Terbatas pada sektor swasta, sehingga ada celah regulasi di sektor publik.

Kerangka Hukum Siber di Thailand

Thailand telah membuat langkah besar dalam mengembangkan kerangka hukum siber melalui serangkaian undang-undang baru. Beberapa peraturan penting di Thailand antara lain:

1. *Computer Crime Act* 2007 (Revised in 2017)
   Computer Crime Act (CCA) adalah undang-undang utama yang mengatur aktivitas siber di Thailand. Versi terbaru dari CCA mencakup pengaturan terhadap konten ilegal, serangan siber, dan perlindungan data digital. Kelebihannya antara lain : mencakup berbagai aspek kejahatan siber, termasuk penyebaran berita palsu dan pelanggaran hak cipta digital; menekankan kerjasama internasional dalam penanganan kejahatan siber. Dan untuk Kelemahan CCA adalah sering kali dikritik karena dianggap membatasi kebebasan berekspresi secara online.
2. *Personal Data Protection Act* 2019 (PDPA)
   Thailand juga telah memberlakukan undang-undang perlindungan data pribadi, yaitu *Personal Data Protection Act* (PDPA). PDPA di Thailand mencakup perlindungan hak individu terhadap penggunaan data pribadi oleh sektor publik dan swasta. Kelebihan dari PDPA ialah : memberikan cakupan luas untuk perlindungan data pribadi, termasuk sektor publik; mengatur sanksi administratif dan pidana terhadap pelanggaran perlindungan data. Dan kelemahan PDPA adalah implementasi dan penegakan hukum masih memerlukan waktu dan dukungan yang lebih kuat.

Perbandingan Regulasi di Negara-Negara ASEAN

Ketiga negara ini menunjukkan pendekatan yang berbeda dalam membangun kerangka hukum siber mereka, meskipun terdapat beberapa kesamaan, seperti fokus pada keamanan digital dan perlindungan data pribadi. Singapura memiliki kerangka hukum yang lebih maju secara teknologi, sedangkan Malaysia dan Thailand masih dalam tahap memperkuat regulasi dan implementasi hukum. Dalam konteks ASEAN, kerangka hukum yang bervariasi ini menimbulkan tantangan harmonisasi, terutama dalam menghadapi kejahatan siber lintas batas. Oleh karena itu, diperlukan upaya kerjasama regional untuk menciptakan standar hukum siber yang lebih seragam.

Kawasan ASEAN memiliki keragaman dalam implementasi hukum siber yang mencerminkan kebutuhan, tantangan, dan prioritas nasional masing-masing negara. Indonesia, Singapura, Malaysia, dan Thailand adalah contoh negara ASEAN yang telah memiliki regulasi terkait hukum siber. Perbandingan

ini bertujuan untuk mengidentifikasi kesamaan, perbedaan, dan tingkat kompatibilitas hukum siber di kawasan, dengan fokus pada UU ITE di Indonesia, *Computer Misuse Act* (CMA) di Singapura, *Personal Data Protection Act* (PDPA) di Malaysia, dan *Computer Crime Act* (CCA)Thailand.

Persamaan dari regulasi yang ada pada keempat negara tersebut ialah : (1) Fokus pada Keamanan Siber, negara-negara ASEAN cenderung memprioritaskan keamanan siber dalam undang-undang mereka. UU ITE di Indonesia (UU No. 19 Tahun 2016), CMA Singapura, dan PDPA Malaysia mengatur tentang ancaman terhadap infrastruktur teknologi informasi, seperti akses ilegal, peretasan, dan sabotase. Regulasi ini seragam dalam pendekatan mereka untuk memberikan sanksi tegas terhadap pelanggaran yang melibatkan sistem teknologi informasi. (2) Perlindungan Data Pribadi, meskipun tidak seragam, perlindungan data pribadi menjadi perhatian utama di seluruh negara. Malaysia melalui PDPA telah menetapkan kerangka hukum perlindungan data pribadi sejak 2010, sementara Singapura dengan *Personal Data Protection Act* 2012 menawarkan perlindungan yang serupa. Indonesia belum memiliki UU perlindungan data pribadi yang komprehensif hingga 2022 tetapi menggunakan UU ITE sebagai dasar regulasi sementara. (3) Kolaborasi Internasional, kesamaan lainnya adalah keterlibatan dalam kerjasama internasional untuk penegakan hukum siber. Negara-negara ini terlibat dalam ASEAN Cybersecurity Cooperation Strategy dan mendukung upaya internasional dalam pencegahan kejahatan siber, seperti konvensi Budapest yang menjadi acuan global.

Selain dari persamaan diatas, perbedaan juga terdapat pada keempat regulasi pada negara ASEAN tersebut, yaitu : (1) Fokus Regulasi, Indonesia melalui UU ITE memiliki fokus yang luas, termasuk pengaturan transaksi elektronik, kejahatan siber, dan perlindungan konsumen. Di sisi lain, CMA Singapura lebih terpusat pada pencegahan dan penindakan kejahatan siber, tanpa mencakup aspek transaksi elektronik secara luas. (2) Tingkat Penegakan Hukum, Singapura dikenal memiliki kapasitas penegakan hukum yang sangat baik dengan tingkat keberhasilan yang tinggi dalam menangani kasus kejahatan siber. Sebaliknya, Indonesia menghadapi tantangan dalam penegakan UU ITE, terutama karena keterbatasan sumber daya manusia dan teknologi di tingkat kepolisian. (3) Harmonisasi dengan Standar Internasional, Malaysia dan Singapura cenderung lebih kompatibel dengan standar internasional, termasuk *General Data Protection Regulation* (GDPR) Uni Eropa, dibandingkan Indonesia dan Thailand. Hal ini terlihat dari kerangka perlindungan data pribadi mereka yang lebih maju dan komprehensif.

Dari persamaan dan perbedaan yang telah dikemukakan, maka regulasi yang ada bisa disesuaikan sebagai berikut : (1) Potensi Harmonisasi Regional, ada peluang besar untuk harmonisasi hukum siber di ASEAN, terutama dalam perlindungan data pribadi dan penanggulangan kejahatan siber. ASEAN *Framework on Personal Data Protection* yang diadopsi pada 2016 memberikan dasar untuk kerjasama regional. Meski demikian, perbedaan substansial dalam prioritas nasional menjadi tantangan untuk mencapai kompatibilitas penuh. (2) Kesenjangan Teknologi dan Infrastruktur, kompatibilitas hukum juga terhambat oleh kesenjangan teknologi dan infrastruktur di kawasan. Singapura memiliki infrastruktur yang jauh lebih maju dibandingkan Indonesia atau Thailand, yang memengaruhi tingkat efektivitas penerapan hukum siber. (3) Implikasi pada Kerjasama Regional, untuk mencapai kompatibilitas yang lebih baik, negara-negara ASEAN perlu menyelaraskan regulasi mereka dengan prinsip-prinsip yang diakui secara internasional, seperti prinsip dalam GDPR. Langkah ini tidak hanya meningkatkan efektivitas hukum siber di kawasan tetapi juga memperkuat posisi ASEAN dalam menghadapi tantangan global.

Tantangan dan Peluang Harmonisasi di ASEAN

Harmonisasi hukum siber di ASEAN menjadi kebutuhan mendesak seiring meningkatnya ancaman kejahatan siber lintas negara. Keragaman sistem hukum di ASEAN, yang meliputi sistem hukum *common law*, *civil law*, dan hukum adat, menciptakan tantangan dalam menyusun regulasi yang seragam. Namun, peluang harmonisasi tetap terbuka melalui pendekatan bertahap yang mempertimbangkan praktik terbaik di tingkat internasional, seperti *Budapest Convention on Cybercrime*.

Tantangan dalam Harmonisasi Hukum Siber di ASEAN yaitu : (1) Keragaman Sistem Hukum, setiap negara anggota ASEAN memiliki kerangka hukum berbeda, yang mencakup UU ITE (Indonesia), *Computer Misuse Act* (Singapura), dan *Personal Data Protection Act* (Malaysia). Ketidaksamaan ini menciptakan kesenjangan dalam definisi, cakupan, dan penerapan hukum siber. (2) Perbedaan Prioritas Nasional, negara-negara ASEAN sering kali memiliki prioritas nasional yang berbeda terkait regulasi teknologi. Misalnya, Singapura fokus pada keamanan data dan efisiensi digital, sementara Indonesia lebih banyak berfokus pada penegakan hukum terhadap ujaran kebencian di media sosial. (3) Kapasitas Penegakan Hukum, kapasitas penegakan hukum terhadap kejahatan siber di ASEAN masih bervariasi. Negara-negara maju, seperti Singapura, memiliki sumber daya teknologi dan tenaga ahli yang mumpuni, sementara negara berkembang menghadapi keterbatasan infrastruktur dan sumber daya manusia. (4) Kedaulatan Digital, kekhawatiran tentang pelanggaran kedaulatan digital sering menjadi penghalang dalam membentuk kerjasama regional. Negara-negara anggota cenderung mengutamakan kedaulatan masing-masing, terutama dalam pengelolaan data dan investigasi kejahatan siber.

Setelah tantangan yang ada, peluang harmonisasi hukum siber di ASEAN antara lain : (1) Standar Internasional sebagai Acuan, *Budapest Convention on Cybercrime* menyediakan kerangka yang dapat diadaptasi oleh ASEAN untuk menciptakan standar regional. Standar ini dapat menjadi dasar bagi perjanjian antarnegara ASEAN dalam menghadapi ancaman kejahatan siber. (2) Platform Regional ASEAN, ASEAN memiliki beberapa platform seperti ASEAN *Ministerial Conference on Cybersecurity* (AMCC) yang dapat dimanfaatkan untuk merumuskan kebijakan bersama. AMCC telah mendorong inisiatif seperti ASEAN *Cyber Capacity Programme* untuk meningkatkan kapabilitas hukum dan teknologi. (3) Kemitraan dengan Sektor Swasta, kerjasama antara pemerintah ASEAN dan sektor swasta dapat memperkuat ekosistem keamanan siber regional. Perusahaan teknologi global sering memiliki sumber daya dan keahlian yang dapat mendukung pembangunan kapasitas di kawasan. (4) Inisiatif Pendidikan dan Pelatihan, pendidikan dan pelatihan keamanan siber di kawasan ASEAN dapat meningkatkan kapasitas sumber daya manusia. ASEAN *Cybersecurity Training Centre* di Bangkok, misalnya, telah menjadi pusat pelatihan untuk penegak hukum di kawasan.

Implikasi hukum internasional dalam harmonisasi ASEAN, yaitu : (1) *Budapest Convention*, walaupun belum ada negara ASEAN yang meratifikasi *Budapest Convention*, prinsip-prinsipnya dapat diadopsi sebagai standar minimum. Konvensi ini menawarkan pendekatan sistematis terhadap kejahatan siber, mulai dari investigasi hingga pengadilan. (2) Kerjasama Ekstradisi, harmonisasi hukum juga membutuhkan kerjasama ekstradisi dalam kasus kejahatan siber. ASEAN *Treaty on Mutual Legal Assistance in Criminal Matters* dapat menjadi landasan untuk memperkuat ekstradisi lintas negara. (3) Keanggotaan di Organisasi Global, negara-negara ASEAN dapat memperkuat posisinya di organisasi global seperti Interpol dan UNODC (*United Nations Office on Drugs and Crime*) untuk mengakses panduan dan dukungan teknis.

Selain itu untuk menguatkan harmonisasi perlu adanya kerjasama regional guna : (1) Peningkatan Kapasitas Kolektif, melalui ASEAN *Cyber Capacity Programme*, negara-negara anggota dapat berbagi pengetahuan dan teknologi untuk memperkuat regulasi hukum siber. (2) Pembentukan *Framework* ASEAN tentang Hukum Siber, membentuk kerangka kerja hukum siber ASEAN yang melibatkan semua negara anggota dapat mengurangi ketimpangan regulasi. *Framework* ini dapat mencakup prinsip-prinsip dasar seperti perlindungan data, penegakan hukum, dan mekanisme penyelesaian sengketa. (3) Simulasi dan Latihan Keamanan Siber, ASEAN dapat mengadakan latihan regional untuk menguji kemampuan respon terhadap insiden siber. Simulasi ini dapat mengidentifikasi kelemahan dan memperkuat koordinasi antarnegara.

Harmonisasi hukum siber di ASEAN menghadapi tantangan signifikan, terutama terkait keragaman sistem hukum dan kapasitas penegakan. Namun, peluang besar terbuka melalui kerjasama

regional, adaptasi standar internasional, dan penguatan kapasitas. ASEAN harus memanfaatkan platform regional seperti AMCC untuk menyusun kerangka hukum yang komprehensif, sekaligus memperkuat hubungan dengan sektor swasta dan organisasi internasional.

KESIMPULAN

Hukum siber telah menjadi aspek penting dalam menghadapi dinamika digital di kawasan ASEAN, termasuk di Indonesia. Berdasarkan kajian normatif yang dilakukan, dapat disimpulkan bahwa Indonesia, melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), memiliki dasar hukum yang cukup untuk menangani berbagai isu terkait hukum siber. Namun, bila dibandingkan dengan kerangka hukum di negara-negara ASEAN lainnya, seperti Singapura, Malaysia, dan Thailand, terdapat sejumlah kelemahan yang perlu segera diatasi untuk memastikan kesesuaian dengan standar internasional dan praktik terbaik di kawasan.

Kekuatan utama UU ITE terletak pada cakupan regulasinya yang mencakup berbagai aspek, seperti perlindungan informasi elektronik, transaksi digital, dan penanganan tindak pidana siber. Namun, kelemahan mendasar muncul dalam penegakan hukum yang sering dianggap belum efektif dan konsisten. Rendahnya kapasitas penegak hukum serta minimnya harmonisasi antara peraturan perundang-undangan yang berkaitan dengan hukum siber menjadi kendala yang signifikan. Selain itu, perlindungan data pribadi di Indonesia masih kurang memadai, meskipun sudah ada UU Perlindungan Data Pribadi (UU PDP). Implementasi dan pengawasannya masih jauh tertinggal dibandingkan dengan Malaysia dan Singapura.

Indonesia perlu mengambil langkah-langkah strategis untuk memperkuat kerangka hukum sibernya, antara lain meliputi: (1) Pembaruan Legislasi, mengadopsi pendekatan yang lebih komprehensif dalam merevisi UU ITE agar mencakup isu-isu baru, seperti keamanan siber dan kejahatan lintas batas. (2) Peningkatan Kapasitas Penegak Hukum, melalui pelatihan khusus dan peningkatan teknologi yang mendukung investigasi siber. (3) Harmonisasi Regulasi, mengintegrasikan berbagai undang-undang terkait teknologi informasi untuk menciptakan sistem hukum yang lebih konsisten. (4) Kerja Sama Regional, mendorong kolaborasi dengan negara-negara ASEAN dalam membangun mekanisme penegakan hukum siber yang terpadu.

Meskipun hukum siber di Indonesia telah memiliki fondasi yang baik, terdapat kebutuhan mendesak untuk meningkatkan efektivitas dan relevansinya. Dengan mengambil pelajaran dari negara-negara tetangga di ASEAN dan memperkuat kolaborasi regional, Indonesia dapat memposisikan diri sebagai pemimpin dalam pengembangan hukum siber yang responsif dan adaptif terhadap tantangan era digital. Hal ini tidak hanya penting untuk melindungi warga negaranya tetapi juga untuk meningkatkan daya saing di kancah internasional.

DAFTAR PUSTAKA

Ang, P. H., & Nadarajan, B. (2018). Cybersecurity in ASEAN: Regional Cooperation and National Strategies. Singapore: NUS Press.

Anshori, M. (2019). Revisi Pasal Kontroversial UU ITE: Analisis Hukum dan Dampaknya. Jakarta: Pustaka Hukum.

ASEAN Secretariat. (2019). ASEAN Cybersecurity Cooperation Strategy. Jakarta: ASEAN Secretariat.

ASEAN. (2016). ASEAN Framework on Personal Data Protection. Retrieved from https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.

ASEAN. (2020). ASEAN Digital Economy Framework. ASEAN Secretariat.

Council of Europe. (2001). Budapest Convention on Cybercrime. Strasbourg: Council of Europe.

Direktorat Jenderal Aplikasi Informatika. (2016). Panduan UU ITE. Jakarta: Kementerian Komunikasi dan Informatika.

Fadilah, R. (2020). Hukum dan Teknologi di Era Digital. Bandung: Nuansa Cendekia.
Handayani, T. (2018). Pengakuan Alat Bukti Elektronik dalam UU ITE. Jurnal Hukum dan Teknologi Informasi, 12(3), 145–156.
Idris, M. (2019). Personal Data Protection in Malaysia: An Analysis. Journal of ASEAN Studies, 7(2), 45-60.
Iswandi, D. (2017). Perlindungan Konsumen dalam Transaksi Elektronik. Jurnal Hukum Digital, 9(2), 45–60.
Kusuma, A. (2017). Tantangan Penegakan Hukum Siber di Indonesia. Yogyakarta: Deepublish.
Lim, J. (2018). Cybersecurity Regulations in Singapore: A Model for ASEAN? Asian Journal of Law and Technology, 12(3), 221-240.
Malaysia Personal Data Protection Act. (2010). PDPA 2010. Retrieved from https://www.malaysia.gov.my/portal/content/654.
Marzuki, P. M. (2017). Penelitian Hukum: Edisi Revisi. Jakarta: Kencana Prenada Media Group.
Ministry of Communications and Information. (2021). Singapore Cybersecurity Strategy. Singapore: Government of Singapore.
Mukaddas, M. (2015). Perlindungan Hukum Data Pribadi di Era Digital. Jakarta: Prenada Media.
Nugraha, B. (2018). Kerjasama ASEAN dalam Penanggulangan Kejahatan Siber. Jurnal Politik dan Hukum Internasional, 7(4), 77–90.
Pratama, A. (2020). Evaluasi UU ITE dalam Penanganan Kejahatan Siber. Jurnal Hukum dan Teknologi, 15(4), 56-73.
Purbo, O. W. (2017). Keamanan Siber di Indonesia: Tantangan dan Solusi. Jakarta: Elex Media Komputindo.
Rahardjo, S. (2009). Cyberlaw dan Kebijakan Hukum. Jakarta: Kompas.
Raharjo, S. (2019). Penegakan Hukum Siber di Indonesia. Jurnal Hukum dan Masyarakat, 20(2), 102-118.
Rahayu, S. (2017). Perkembangan Hukum Teknologi Informasi di Indonesia. Surabaya: UPT Press.
Rahman, H. (2016). Hukum Siber Indonesia: Implementasi dan Hambatan. Jakarta: Prenada Media.
Singapura. (1993). Computer Misuse Act. Retrieved from https://sso.agc.gov.sg/Act/CMA1993.
Soerjono Soekanto. (2007). Pengantar Penelitian Hukum. Jakarta: UI Press.
Suryani, M. (2016). Kerangka Hukum Siber di Indonesia. Jurnal Hukum Nasional, 15(1), 99–120.
Susanti, D., & Wahyuni, A. (2016). Perkembangan Hukum Siber di Indonesia. Jakarta: Prenada Media.
Susanti, I. (2018). Pasal Multitafsir dalam UU ITE. Jurnal Hukum dan Kebijakan Publik, 10(2), 34–50.
Tan, J. (2019). Legal Approaches to Cybercrime in ASEAN. International Review of Law, 7(1), 15-28.
Thailand. (2017). Computer Crime Act. Retrieved from https://www.mdes.go.th/law/detail/3618-COMPUTER-RELATED-CRIME-ACT-B-E--2550--2007-.
UU No. 19 Tahun 2016 tentang Perubahan UU ITE.
Wahyudi, A. (2019). Kekurangan UU ITE dalam Melindungi Data Pribadi. Jurnal Hukum Privasi dan Teknologi, 8(3), 199–213.
Watson, A. (1974). Legal Transplants: An Approach to Comparative Law. Edinburgh: Scottish Academic Press.
Widodo, H. (2019). Harmonisasi Hukum Siber Indonesia dengan Standar Internasional. Bandung: Graha Ilmu.
Yusuf, F. (2020). Urgensi Perlindungan Data Pribadi di Indonesia. Jakarta: Kencana Prenada Media.