Jurnal Risalah Kenotariatan
Volume 6, Issue 1, Januari-Juni 2025
open access at : http://risalah.unram.ac.id
Magister Kenotariatan Fakultas Hukum Universitas Mataram

TANTANGAN PENEGAKAN HUKUM SIBER DI ERA LINTAS NEGARA DAN UPAYA HARMONISASI GLOBAL

CHALLENGES OF CYBER LAW ENFORCEMENT IN THE ERA OF CROSS-NATIONAL COMMERCIALS AND GLOBAL HARMONIZATION EFFORTS

Suntarajaya Kwangtama Tekayadi
Universitas Bumigora
Email: suntarajaya@universitasbumigora.ac.id

Sumerah
Universitas Bumigora
Email: sumerah@universitasbumigora.ac.id

Saparudin Efendi
Universitas Bumigora
Email: saparudin@universitasbumigora.ac.id

Abstrak:

Perkembangan teknologi informasi yang melampaui batas negara telah memunculkan tantangan baru dalam penegakan hukum, khususnya dalam menghadapi kejahatan siber. Karakter kejahatan siber yang bersifat transnasional membuat hukum nasional sering kali tidak mampu menjangkau atau menindak pelaku secara efektif. Artikel ini membahas urgensi tantangan penegakan hukum dan harmonisasi hukum siber dan strategi harmonisasi hukum siber secara global. Penelitian ini bertujuan untuk menganalisa penegakan hukum dan strategi harmonisasi hukum siber secara global. Metode yang digunakan adalah penelitian hukum normative dengan pendekatan perundang-undangna dengan konseptual. Hasil penelitian menunjukkan bahwa tantangan utama adalah sifat lintas batas dari kejahatan siber yang mengaburkan yuridiksi hukum antar negara dan keterbatasan kapasitas teknis dan infrastruktur penegakan hukum serta sumberdaya manusia yang memiliki keahlian. Kesimpulan dari penelitian ini adalah harmonisasi hukum siber menjadi penting untuk menciptakan sistem hukum yang responsif, kolaboratif, dan adaptif dalam menghadapi ancaman dunia digital yang terus berkembang.

Kata-kata kunci: ***hukum siber, harmonisasi, kejahatan siber, teknologi lintas negara,***

Abstract

The development of information technology that transcends national borders has raised new challenges in law enforcement, especially in dealing with cybercrime. The transnational character of cybercrime makes national laws often unable to reach or take action against perpetrators effectively. This article discusses the urgency of law enforcement challenges and cyber law harmonization and cyber law harmonization strategies globally. This research aims to analyze law enforcement and cyber law harmonization strategies globally. The method used is normative legal research with a legislative and conceptual approach. The results show that the main challenges are the cross-border nature of cybercrime that blurs legal jurisdiction between countries and

DOI : https://doi.org/10.29303/risalahkenotariatan.v6i1.361

the limited technical capacity and law enforcement infrastructure as well as skilled human resources. The conclusion of this research is that harmonization of cyber law is important to create a responsive, collaborative, and adaptive legal system in the face of the evolving threats of the digital world.

Keywords: cyber law, harmonization, cybercrime, transnational technology

A. PENDAHULUAN

Era digital yang terus berkembang pesat saat ini, yaitu berupa internet dan teknologi informasi telah menjadi bagian penting dari kehidupan sehari-hari. Namun, perkembangan tersebut juga tidak terlepas dari munculnya kejahatan dunia maya dikenal sebagai Kejahatan Siber muncul sebagai masalah baru seiring perkembangan teknologi dan memiliki akibat yang serius baik pada tingkat individu maupun kolektif [1].

Cybercrime atau kejahatan siber diartikan sebagai tindak kriminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Kejahatan ini memanfaatkan perkembangan teknologi komputer khususnya internet [2]. *Cybercrime* adalah tindak pidana yang memiliki beberapa karakteristik. Kejahatan ini mencakup akses tanpa izin yang bertujuan untuk memfasilitasi kejahatan. Selain itu, tindakan ini juga meliputi perubahan atau penghancuran data tanpa izin, serta mengganggu atau merusak operasi komputer. Tak kalah penting, *cybercrime* juga dapat mencakup tindakan yang mencegah atau menghambat akses ke komputer. Karakteristik-karakteristik ini menunjukkan betapa kompleks dan beragamnya bentuk kejahatan siber yang ada saat ini [3].

Kejahatan siber termasuk dalam kategori kejahatan transnasional karena sifatnya yang melibatkan tindakan kriminal yang melampaui batas-batas negara. Kejahatan ini sering kali dilakukan oleh pelaku yang berada di satu negara tetapi menargetkan korban di negara lain, seperti seoranghackerdi negara A yang dapat meretas sistem komputer di negara B tanpa harus berada di lokasi fisik tersebut. Perkembangan teknologi informasi dan komunikasi telah menciptakan ruang siber yang tidak terikat oleh batas-batas fisik, membuat pelaku dapat menggunakan internet untuk berkomunikasi, melakukan transaksi, dan menyembunyikan identitas mereka, sehingga menyulitkan penegakan hukum. Selain itu, banyak kejahatan siber melibatkan jaringan pelaku yang berkolaborasi secara internasional, berbagi informasi, alat, dan teknik untuk melakukan serangan, yang semakin memperkuat sifat transnasional kejahatan ini [4].

Dalam konteks Indonesia, serangan siber telah berdampak pada berbagai sektor, seperti pemerintahan, keuangan, pendidikan, dan kesehatan. Kondisi ini menjadi tantangan serius bagi pemerintah dalam menyusun kebijakan kriminal yang mampu menangani kejahatan siber secara optimal. Sebagai tanggapan atas meningkatnya ancaman tersebut, pemerintah Indonesia telah memberlakukan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Pelindungan Data Pribadi (UU PDP). Meski begitu, pelaksanaan kedua regulasi ini masih menghadapi sejumlah hambatan, antara lain belum selarasnya dengan hukum internasional, rendahnya tingkat literasi digital masyarakat, dan keterbatasan sumber daya teknis di kalangan aparat penegak hukum.

1 Fadhila Inas Pratiwi, "Analisis Ancaman Dan Respon Keamanan Siber Di Indonesia," Uniar News, 2024.
2 Agus Wibowo, Globalisasi Digital (Semarang: Yayasan Prima Agus Teknik, 2023).
3 Agus Wibowo.
4 Gianpiero Greco, Nicola Montinaro, "The Phenomenon Of Cybercrime: From The Transnational Connotation To The Need For Globalization Of Justice," European Journal of Social Sciences Studies 6, no. 1 (2021): 13.

Kondisi ini menegaskan perlunya penelitian lebih lanjut guna memperkuat kebijakan kriminal dalam menghadapi tantangan kejahatan siber di Indonesia.

Ancaman siber di Indonesia juga diperburuk oleh kurangnya kesadaran publik mengenai pentingnya keamanan digital dan praktik perlindungan data pribadi. Banyak individu dan organisasi yang masih belum mengimplementasikan protokol keamanan siber yang memadai, sehingga rentan terhadap serangan siber. Kesadaran dan edukasi mengenai pentingnya keamanan siber merupakan aspek yang krusial dalam menekan angka kejahatan siber dan menjaga kesejahteraan masyarakat di dunia maya [5]. Meskipun berbagai kebijakan telah diterapkan, tantangan utama dalam penanganan kejahatan siber di Indonesia mencakup rendahnya literasi digital masyarakat, keterbatasan kapasitas teknis aparat hukum, dan sulitnya menangani kasus yang bersifat lintas batas.

Perbedaan hukum terkait kejahatan siber di berbagai negara turut memperumit upaya penanggulangannya, karena seringkali tidak terdapat kesepakatan internasional yang solid mengenai penanganannya. Hal ini menciptakan celah hukum yang kerap dimanfaatkan oleh para pelaku kejahatan. Kejahatan siber sendiri dapat menimbulkan dampak luas dan merugikan, baik terhadap perekonomian global, keamanan nasional, maupun hubungan antarnegara. Sebagai contoh, serangan ransomware bisa mengganggu operasional perusahaan lintas negara dan merusak rantai pasok ekonomi internasional.

Sebagai negara hukum, Indonesia memiliki kewajiban melindungi warganya dari ancaman yang merugikan, termasuk kejahatan siber. Meskipun belum ada undang-undang khusus mengenai kejahatan siber, beberapa peraturan seperti Undang-undang Telekomunikasi No. 36 Tahun 1999, UU Hak Cipta No. 19 Tahun 2002, Undang-undang Pemberantasan Terorisme No. 15 Tahun 2003, dan Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur pencegahan dan penindakan kejahatan siber.

Kejahatan siber melibatkan segala tindakan kriminal yang menggunakan sistem elektronik, Seperti terorisme, perdagangan manusia, dan pencucian uang. Undang-undang ITE mengatur lebih spesifik tentang kejahatan siber, termasuk akses ilegal, penyebaran konten ilegal seperti pornografi dan fitnah, serta ancaman siber lainnya. Namun, perlu diingat bahwa permasalahan kejahatan siber lintas negara adalah salah satu tantangan terbesar dalam dunia digital saat ini. Kejahatan ini melibatkan pelaku dari berbagai negara yang melakukan serangan terhadap sistem elektronik atau data yang berada di negara lain. Kejahatan siber lintas negara bisa berupa serangan hacking, pencurian identitas, penyebaran malware, atau pembobolan data pribadi. Tantangan utamanya adalah bahwa pelaku kejahatan sering berada di yurisdiksi yang berbeda, sehingga sulit bagi negara. Oleh karena itu, penelitian ini penting untuk memberikan solusi strategis dalam memperkuat ekosistem keamanan siber, yang tidak hanya mencakup aspek hukum tetapi juga literasi digital dan kerja sama internasional.

Berdasarkan latar belakang yang telah dijabarkan sebelumnya, adapun rumusan masalah yang akan dikaji dalam penelitian ini adalah tantangan yang dihadapi dalam penegakan hukum siber di era tekhnologi lintas negara serta bagaimana strategi yang dapat ditempuh untuk mendorong harmonisasi hukum siber secara global.

5 Farah Diba Tanzilla, Margaretha Hanita, And Bondan Widiawan, "Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law'," *International Journal Of Progressive Sciences And Technologies* 40, no. 2 (2023): 160.

Adapun pendekatan penelitian yang digunakan untuk menyelesaikan masalah, adalah pendekatan perundang-undangan yang meliputi Undang-undang Telekomunikasi No. 36 Tahun 1999, UU Hak Cipta No. 19 Tahun 2002, Undang-undang Pemberantasan Terorisme No. 15 Tahun 2003, dan Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan pendekatan konseptual yang mengkaji konsep-konsep yang berkaitan dengan masalah yang sedang dikaji. Sedangkan tujuan penelitian ini adalah untuk memahami tantangan yang dihadapi dalam penegakan hukum siber di era tekhnologi lintas negara serta bagaimana strategi yang dapat ditempuh untuk mendorong harmonisasi hukum siber secara global. Perbedaan penelitian yang dilakukan peneliti dapat dilihat pada penelitian yang dilakukan oleh Ragma Agri Firdaus, fokus penelitian yang dilakukan Ragma Agri Firdaus adalah pada menganalisa *cyber crime* dalam konteks hukum positif indonesia sedangkan peneliti pada penelitian ini berfokus pada tantangan penegakan hukum siber dalam era tekhnologi lintas batas serta harmonisasi hukum siber secara global.

B. METODE PENELITIAN

Penelitian ini menggunakan metode Penelitian hukum normatif yaitu metode atau cara yang dipergunakan di dalam Penelitian hukum yang meletakkan hukum sebagai sebuah bangunan sistem norma. Adapun sistem norma yang dimaksud mencakup peraturan perundang-undangan, teori-teori hukum, norma-norma serta asas-asas hukum, putusan pengadilan serta doktrin hukum[6]. Metode pendekatan yang digunakan peneliti meliputi Pendekatan Perundang-undangan *(Statute Approach)* dan Pendekatan Konseptual *(Conceptual Approach)*. Adapun bahan hukum yang digunakan dalam Penelitian ini adalah Bahan Hukum Primer, Bahan Hukum Sekunder dan Bahan Hukum Tersier. Bahan hukum Primer adalah bahan hukum yang bersangkut paut dengan isu hukum dalam Penelitian ini yang bahannya bersumber dari peraturan perundang-undangan[7]. Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan mengenai bahan hukum primer. Adapun sumbernya diperoleh dari buku-buku, hasil-hasil Penelitian dalam jurnal dan makalah serta pendapat para ahli (doktrin) yang relevan dengan persoalan yang dibahas. Serta bahan hukum tersier adalah bahan hukum yang memberikan penjelasan terhadap bahan hukum primer maupun bahan hukum.

C. HASIL DAN PEMBAHASAN

1. Tantangan Yang Dihadapi Dalam Penegakan Hukum Siber Di Era Tekhnologi Lintas Negara

Perkembangan teknologi di era digital telah membawa banyak manfaat bagi kehidupan modern, namun juga diiringi dengan tantangan baru, salah satunya adalah meningkatnya ancaman kejahatan siber. Di Indonesia, kejahatan siber seperti peretasan, pencurian identitas, dan penipuan online menjadi isu yang semakin

6 Jonaedi Efendi, Jhonny Ibrahim, and Prasetijo Rijadi, "Metode Penelitian Hukum: Normatif Dan Empiris," 2016.

7 Soerjono Soekanto Sri Mamudji, *Penilitian Hukum Normatif (Suatu Tinjauan Singkat)* (Jakarta: Rajawali Pers, 2001).

mendesak untuk diatasi. Dampak dari kejahatan ini sangat luas, mulai dari kerugian finansial hingga ancaman terhadap privasi dan keamanan nasional. Pemerintah dan aparat hukum di Indonesia berusaha untuk merespons situasi ini melalui berbagai kebijakan dan regulasi, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) [8]. Namun, pelaksanaan penegakan hukum di bidang kejahatan siber di Indonesia masih menghadapi hambatan yang cukup besar. Berbagai kesulitan muncul akibat keterbatasan teknis, minimnya kerja sama lintas negara, serta rendahnya pemahaman masyarakat akan pentingnya perlindungan di ranah digital. Kondisi ini menunjukkan bahwa pencapaian sistem keamanan siber yang optimal memerlukan pendekatan yang menyeluruh dan bersifat kolaboratif. Pada bagian berikut, akan dibahas lebih lanjut berbagai tantangan utama dalam upaya penegakan hukum terhadap kejahatan siber di Indonesia. Indonesia memiliki Undang-Undang Nomor l l Tahun 2008 tentang Informasi dan Transaksi Elektronik pada 21 April 2008. Undang-undang ini adalah peraturan pertama di Indonesia yang mengatur aspek-aspek penggunaan teknologi informasi, termasuk transaksi elektronik, perlindungan data, dan penegakan hukum terhadap tindak pidana siber.

Pasal 30 Undang-Undang Nomor l l Tahun 2008 tentang Informasi dan Transaksi Elektronik telah menyatakan bahwa [9]:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

UU ITE sendiri telah mengalami dua kali perubahan sejak diundangkan, Pertama, perubahan menjadi Undang-Undang Nomor 19 Tahun 2016 yang menunjukkan dinamika dan keinginan masyarakat akan adanya penyempurnaan pasal-pasal UU ITE, khususnya akan ketentuan pidana konten ilegal. Kemudian, pada 21 November 2023, naskah Rancangan Undang-Undang tentang Perubahan Kedua atas UU ITE disahkan. Naskah ini kemudian ditandatangani pada tanggal 4 Januari 2024, sehingga Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi perubahan kedua UU ITE di Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam Pasal 27B Ayat (1) juga memuat pengaturan mengenai setiap orang yang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan informasi elektronik dan dokumen elektronik dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum.

Pasal 28 Ayat (1) UU ITE 2024 kemudian mengatur kembali larangan bagi setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan informasi elektronik dan dokumen elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan, yang dapat mengakibatkan kerugian materil bagi konsumen

8 Wildan Fahriza And Muhammad Arif Sahlepi, "Effectiveness OfLaw Enforcement Against Cybercrime In Indonesia On Hacking Crimes And The Role Of The Ite Law," *Law Synergy Conference* 1, no. 1 (2024): 178.

9 Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," no. September (2008): 1–2.

dalam transaksi elektronik. Aturan ini digunakan untuk melindungi konsumen dalam transaksi online.

Pasal 32 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi juga mengatur tentang larangan penyalahgunaan jaringan telekomunikasi, termasuk untuk kegiatan ilegal. Selanjutnya, Pasal 3 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga mengatur tentang penyelenggaraan sistem elektronik dan kewajiban penyelenggara dalam menjaga keamanan data. Undang- Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik juga mengatur akses masyarakat terhadap informasi publik dan sanksi bagi pihak yang melanggar hak atas informasi. Akan tetapi, aturan-aturan tersebut belum secara khusus mengatur kejahatan siber yang dilakukan oleh pelaku di luar Indonesia. Saat ini, masyarakat internasional telah mengenal Konvensi tentang Kejahatan Siber (*Convention on Cyber Crime*) yang dibuat pada tahun 2001 oleh Uni Eropa. Substansi konvensi ini telah mencakup berbagai aspek yang luas, termasuk kebijakan kriminal yang bertujuan melindungi masyarakat dari kejahatan siber, baik melalui undang-undang maupun kerja sama internasional. Langkah ini diambil dengan kesadaran akan meningkatnya digitalisasi, konvergensi, dan globalisasi teknologi informasi, yang berpotensi disalahgunakan untuk tindak pidana [10]. Prioritas utama perjanjian ini adalah mendorong kerja sama internasional untuk melindungi masyarakat dari kejahatan siber melalui regulasi yang sesuai. Konvensi ini telah melahirkan panduan untuk menyelaraskan kerangka hukum nasional.

Terdapat tiga tujuan utama Konvensi Budapest, termasuk penyelarasan kerangka nasional, peningkatan teknik penyelidikan kejahatan siber, dan perluasan kerja sama internasional. Sejak 2001, 66 negara non-Eropa telah meratifikasi perjanjian ini, menjadikannya acuan global dalam menangani kejahatan siber [11]. Indonesia sendiri telah meratifikasi konvensi ini di tahun 2009 [12]. Konvensi ini memberikan landasan hukum yang lebih luas serta kerangka kerja untuk koordinasi antarnegara dalam menghadapi kejahatan siber. Meskipun terdapat dasar hukum yang kuat, tantangan utama dalam penanganan kejahatan siber tetap terkait dengan peningkatan kapasitas, pelatihan personel, dan koordinasi yang efektif antara lembaga penegak hukum dan sektor swasta. Diperlukan pendekatan holistik dan berkelanjutan agar Indonesia mampu menghadapi dinamika kejahatan siber yang terus berubah. Penanganan kejahatan siber yang kompleks membutuhkan pendekatan melalui kerja sama bilateral, regional, dan multilateral. Kerja sama antara lembaga penegak hukum, pemerintah, dan masyarakat sangat penting untuk mengatasi ancaman kejahatan siber.

Beberapa rekomendasi untuk memperkuat upaya penanganankejahatan siber mencakup penguatan regulasi yang lebih komprehensif, peningkatan kerjasama internasional melalui perjanjian dan kolaborasi antarlembaga, serta peningkatan kesadaran masyarakat tentang bahaya kejahatan siber. Dengan langkah-langkah ini, diharapkan masyarakat dapat lebih efektif melindungi diri dari ancaman kejahatan siber yang terus berkembang [13]. Salah satu masalah utama dalam penegakan kejahatan

10 Akbar Kurnia Putra, "Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional," *Jurnal Ilmu Hukum* 3, no. 2 (2024): 47.

11 Agus Nilmada Azmi, Syarah Shabrina, "Challenges of Universal Adoption of The Budapest Convention on Cybercrime", Prosiding The 5th International Conference on Technology," *Education, And Social Science* 1, no. 1 (2023).

12 Agus Nilmada Azmi, Syarah Shabrina.

13 Akbar Kurnia Putra, "Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional."

siber yang bersifat transnasional adalah masalah yurisdiksi. Yurisdiksi sendiri merujuk pada kekuasaan suatunegara untuk menerapkan hukum dan mengadili tindakan yang dilakukan oleh individu atau entitas, terlepas dari lokasi atau kewarganegaraan mereka[14].

Dalam kejahatan siber yang pelakunya bisa bertempat di luar negara Indonesia, masalah dapat muncul ketika lebih dari satu negara mengklaim yurisdiksi atas tindakan yang sama. Hal ini dapat menyebabkan ketidakpastian hukum dan konflik antara negara-negara tersebut. Dalam situasi ini, negaranegara seringkali diharapkan untuk bernegosiasi dan menentukan yurisdiksi mana yang paling tepat untuk mengadili kasus tersebut. Dalam kejahatan siber, ada pengaturan lebih lanjut yang tercantum dalam Konvensi tentang Kejahatan Dunia Siber khususnya Pasal 22 yang mencakup lima paragraf.

Paragraf pertama menjelaskan bahwa negara-negara pihak konvensi dapat mengambil tindakan legislasi untuk melaksanakan yurisdiksi atas kejahatan siber yang terjadi di wilayah mereka atau di luar wilayah mereka. Paragraf kedua menyebutkan setiap negara memiliki hak untuk memilih apakah akan menerapkan ketentuan yurisdiksi atau tidak, dengan mempertimbangkan keadaan dan kasus kejahatan. Paragraf 3 menyebutkan jika pelaku kejahatan berada di wilayah negara dan ekstradisi tidak dilakukan karena statuskewarganegaraan mereka, negara tersebut masih dapat melaksanakan yurisdiksi Meskipun pasal-pasal tersebut memberikan kerangka untuk yurisdiksi dalam penanganan kejahatan siber, masih terdapat kemungkinan konflik yurisdiksi antara negara-negara yang mengklaim yurisdiksi atas suatu kejahatan, terutama ketika kejahatan tersebut melibatkan sistem komputer dan internet yang dapat menargetkan korban dari berbagai negara. Oleh karena itu, perlu ada kesepakatan dan kolaborasi antara negara untuk menentukan yurisdiksi yang paling tepat dalam menangani kejahatan siber [15].

2. Strategi Yang Dapat Ditempuh Untuk Mendorong Harmonisasi Hukum Siber Secara Global

Mengacu pada Alinea ke-4 Pembukaan UUD NRI 1945, diketahui bahwa salah satu tujuan Indonesia adalah ikut serta menjaga ketertiban dunia. Hal ini mengindikasikan bahwa Indonesia adalah salah satu dari 68 Negara Peserta CC dengan tekad dan tujuan kuat untuk secara aktif berperan mengupayakan terlaksanakanya perdamaian dan ketertiban dunia sebagai kontribusi selaku masyarakat dunia [16].

Di tengah disrupsi kemajuan teknologi, ada benarnya bahwa *maxim* menyatakan bahwa hukum itu selalu tertinggal dari peristiwa yang diaturnya—*Het Recht Hink Achter De Feiten Aan* [17]. Pada *cybercrime* misalnya, meskipun Indonesia sejatinya telah mengatur perihal itu dalam beberapa undang-undang termasuk yang paling anyar mengenai data pribadi, penegakan hukum kepada pelaku kejahatan jenis ini belum dapat dikatakan telah maksimal. Sebab, karakter *cybercrime* adalah *borderless* (tanpa batas) yang memungkinkan tindakan beserta efeknya itu melampaui lintas batas negara [18]. maka kebijakan mengenai data pribadi harus berusaha diperhatikan perkembangannya beserta upaya penanggulangnnya baik regional maupun internasional.

---

14 Septi Dyah Tirtawati, Joko Setiyono, "Menilik Penerapan Prinsip Yurisdiksi Universal Negara Terhadap Kejahatan Perompakan Di Laut Lepas Menurut Hukum Internasional," *Jurnal Al-Daulah* 10, no. 2 (2022).

15 Septi Dyah Tirtawati, Joko Setiyono.

16 Septi Dyah Tirtawati, Joko Setiyono.

17 Septi Dyah Tirtawati, Joko Setiyono.

18 H. Mustameer, "Penegakan Hukum Nasional Dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0.," *Jurnal Yustika: Media Hukum Dan Keadilan* 25, no. 1 (2022): 40–53.

Di belahan dunia lain, seperti kawasan Eropa, hukum teknologi dikembangkan untuk menjadi responsif dalam memberantas *cybercrime* melalui harmonisasi pengaturan nasional yang dilakukan dengan ratifikasi suatu instrumen hukum internasional [19], CC merupakan konvensi internasional khusus pada *cybercrime* yang terbentuk dengan berlandaskan perjanjian internasional. Konvensi ini berhakekat mengatur kebijakan yang diambil untuk mengatasi kriminalitas dan tindak pidana siber dengan tujuan melindungi masyarakat dari *cybercrime*. Selain itu konvensi ini juga dapat memfasilitasi dan mewadahi kerja sama antara negara satu sama lain untuk memberantas tindakan *cybercrime*. Konvensi yang dibuat atas inisiasi Uni Eropa tersebut memiliki partisipan sebanyak 68 negara termasuk Asia, Afrika dan Amerika Selatan.

Konvensi ini dibuat dengan adanya pertimbangan seperti: *Pertama*, untuk mencapai kesatuan yang erat antar negara anggota lainnya. *Kedua,* menyadari pentingnya peningkatan kerjasama dengan negara lain yang menjadi partisipan dalam konvensi ini. Ketiga, kebutuhan akan suatu perlindungan masyarakat terhadap serangan *cybercrime*[20].

Selanjutnya dianalisa bahwa, Konvensi ini tetap menjadi perjanjian internasional yang paling relevan mengenai *cybercrime*. Keanggotaan terus bertambah, sementara kualitas implementasi dan tingkat kerja sama antar para pihak terus meningkat, dan traktat itu sendiri terus berkembang untuk menghadapi tantangan-tantangan baru. CC dilengkapi dengan mekanisme tindak lanjut yang efektif dan dengan program peningkatan kapasitas, yang diberikan kembali kepada Komite, yang berkontribusi terhadap evolusi Konvensi. Motif utama dari pendekatan ini adalah "untuk melindungi hak-hak individu di dunia maya".

Berbagai bentuk perbuatan *cyber crime* dalam *European Convention on Cyber Crime*, yaitu:

1. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan system komputer, yaitu:
   a. Mengakses system computer tanpa hak (*illegal acces*);
   b. Tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*);
   c. Tanpa hak merusak data (*data interference*);
   d. Tanpa hak mengganggu system (*system interference*);
   e. Menyalahgunakan perlengkapan (*misuse of device*).
2. Delik-delik yang berhubungan dengan computer, pemalsuan, dan penipuan (*computer related pffences; forgery and fraud*);
3. Delik-delik yang bermuatan pornografi anak (*content-related offences, child pornography*);
4. Delik-delik yang berhubungan dengan hak cipta (*offences relate of infringements of copyrights*).

Berbagai perbuatan diatas menjadi sandaran untuk menilai pengaturan dalam UU ITE dan menilai sejauhmana terdapat harmonisasi hukum dalam pengaturan tersebut. Pengaturan cybercrime yang mengelompojkan berbagai perbuatan ke dalam dua klasifikasi besar, kemudian dibagi lagi dalam beberapa kelompok berdasarkan pasal-pasal di atas, dipedomani oleh pembuat UU ITE. Hanya saja pembuat UU ITE tidak mengelompokan perbuatan tersebut secara ekspisit sebagaimana terdapat dalam

19 Dewi, "Cybercrime Dalam Abad 21: Suatu Perspektif Menurut Hukum Internasional.," *Masalah-Masalah Hukum* 40, no. 4 (2011): 527.

20 Heidi Vandebosch and K. V Cleemput, "Defining Cyberbullying: A Qualitative Research into the Perceptions of Youngsters," *Cyberpsychology and Behavior* 11, no. 4 (2008): 449–503.

konvensi tersebut. Lebih jelasanya pengaturan cybercrime dalam UU ITE adalah sebagai berikut:

1. *Indecent Materials/ Illegal Content* (Konten Ilegal)

   Setiap orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, pencemaran nama baik serta pemerasan, pengancaman serta yang menimbulkan rasa kebencian berdasarkan atas SARA serta yang berisi ancaman kekerasan (Pasal 27, 28, dan 29 UU ITE)
2. *Illegal Acces* (Akses Ilegal)

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau Sistem Elektronik milik orang lain dengan cara apapun untuk memperoleh Informasi elektronik serta melanggar,menerobos, melampaui atau menjebol sistem pengamanan (Pasal 30 UU ITE).
3. *Illegal Interception* (Penyadapan Ilegal)

   Setiap orang dengan sengaja dan tanpa hak melakukan intersepsi atas Informasi Elektronik dan/ atau Dokumen Elektronik dalam suatu Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabka perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/ atau penghentian Informasi Elektronik dan/ atau Dokumen Elektronik yang sedang ditransmisikan (Pasal 31 UU ITE).
4. Data *Interference* (Gangguan Data)

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum engubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, atau mentransfer suatu Informasi Elektronik milik orang lain atau milik publik kepada Sistem Elektronik orang lain yang tidak berhak, sehingga mengakibatkan terbukanya suatu Informasi Elektronik dan/ atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. (Pasal 32 UU ITE).
5. *System Interference* (Gangguan Sistem)

   Setiap orang dengan sengaja dan tanpa hak melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/ atau mengakibatka Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya (Pasal 33 UU ITE).
6. *Misuse of Devices* (Penyalahgunaan Perangkat)

   Setiap orang dengan sengaja dan tanpa hak memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan yang dilarang dan sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu, yang ditujukan agar sistem elektronik menjadi dapat akses dengan tujuan memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE).
7. *Computer Related Fraud and Forgery* (Penipuan dan Pemalsuan yangberkaitan dengan Komputer)

   Setiap orang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan Informasi Elektronik dan/ atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik (Pasal 35 UU ITE).

Berlandaskan harmonisasi ketentuan sebagaimana dijelaskan diatas, CC mengatur kerja sama internasional yang harus ditaati oleh negara pihaknya. Inilah yang luput, atau setidak-tidaknya kurang, pada hukum di Indonesia. Pemberantasan *cybercrime*

tanpa mekanisme kerjasama dengan negara lain akan menjadi tidak efektif apabila kejahatan itu dilakukan secara ekstrateritorial. Sebab, pemberantasan kasus dengan tipologi yang demikian beririsan dengan suatu prinsip fundamental dalam hukum internasional; bahwa negara memegang kedaulatan tertinggi yang wajib dihormati oleh negara lainnya. Sehingga tidak mungkin Indonesia dapat secara semena-mena menangkap dan mengadili orang yang tidak dalam yuridiksinya. Padahal sebagaimana dikonfirmasi juga oleh pemerintah, Indonesia merupakan negara peringkat kedua kasus *cybercrime* di dunia, yang kemungkinan besar melibatkan pelaku kejahatan dari luar negeri. Menyadari kondisi yang demikian kerjasama internasional dalam memberantas *cybercrime* ini merupakan salah satu solusi yang dapat diambil.

Selanjutnya, CC memberikan opsi negara pihak untuk melakukan ekstradisi ataupun *Mutual Legal Assistance* (MLA) yang memungkinkan negara menuntut dan mengadili pelaku kejahatan. Mekanisme ini adalah suatu kewajiban yang mesti dijalankan oleh negara pihak. Dalam hal ekstradisi konvensi menentukan bahwa perbuatan kriminal yang dilarang dalam CC dimulai dari pasal 2 sampai pasal 11 adalah kejahatan yang dapat dilakukan ekstradisi. Kejahatan itu diancam dengan hukuman penjara maksimum satu tahun atau dengan hukuman yang lain. Jika antara dua negara yang menjadi anggota tidak terdapat perjanjian ekstradisi, maka antara kedua negara tersebut dapat menjadikan konvensi ini sebagai dasar untuk meminta ekstradisi pelaku kejahatan. Terlebih lagi, sebagaimana prinsip dalam hukum perjanjian internasional, *pacta sunt servanda*, kewajiban dalam suatu perjanjian internasional harus dilakukan dengan itikad baik. Karena itu, pelanggaran terhadapnya dapat menjadi suatu pelanggaran hukum internasional yang dapat dimintakan pertanggungjawabannya.

Mekanisme kerjasama yang tertuang dalam CC pada akhirnya menguntungkan Indonesia dalam memberantas *cybercrime*. Sebab, 68 negara pihak CC akan membantu pelaksanaan penegakan hukum terhadap pelaku *cybercrime,* selagi pelaku itu berada di yurisdiksi negara pihak. Alhasil, akan tercipta pola pemberantasan yang efektif. Penulis merekomendasikan agar Indonesia segera meratifikasi konvensi ini karena terdapat sejumlah manfaat strategis yang bisa diperoleh. Salah satunya adalah pemulihan citra Indonesia di mata dunia, khususnya dalam bidang teknologi informasi, yang selama ini dipandang kurang baik. Dengan meratifikasi konvensi tersebut, Indonesia dapat menunjukkan komitmennya yang kuat kepada komunitas internasional dalam memberantas kejahatan siber. Selain itu, berbagai fasilitas yang ditawarkan oleh Konvensi Budapest kepada negara-negara anggotanya memberikan peluang untuk bekerja sama secara efektif dalam memerangi cybercrime. Konvensi ini juga berupaya mengatasi hambatan yurisdiksi antarnegara yang kerap menjadi kendala dalam penegakan hukum siber lintas batas. Hal ini merupakan wujud respons global terhadap ancaman kejahatan siber yang merugikan masyarakat digital secara luas. Oleh karena itu, partisipasi aktif Indonesia dalam pelaksanaan konvensi ini dapat memperkuat langkah-langkah pencegahan dan penanganan kejahatan siber. Dalam praktiknya, Konvensi Budapest juga berpotensi menjadi dasar hukum yang penting ketika hukum nasional belum mampu mengatasi kompleksitas masalah cybercrime secara efektif.

D. KESIMPULAN

Dalam era teknologi digital yang semakin terintegrasi secara global, penegakan hukum siber menghadapi tantangan yang kompleks dan multidimensional. Salah satu

tantangan utama adalah sifat lintas batas dari kejahatan siber yang mengaburkan yurisdiksi hukum antarnegara. Penegakan hukum tidak lagi terbatas pada satu wilayah hukum nasional, melainkan harus menghadapi pelaku yang dapat beroperasi dari mana saja di dunia. Tantangan lain mencakup keterbatasan kapasitas teknis dan infrastruktur penegakan hukum, kurangnya sumber daya manusia yang memiliki keahlian di bidang forensik digital, serta minimnya kesadaran dan literasi masyarakat terhadap ancaman dan pentingnya keamanan siber

Dengan demikian, penanggulangan kejahatan siber di era teknologi lintas batas menuntut tidak hanya respons hukum yang kuat di tingkat nasional, tetapi juga sinergi global yang berlandaskan semangat kolaborasi, keadilan, dan perlindungan hak asasi manusia di dunia digital. Berdasarkan kesimpulan diatas diperlukan langkah untuk mengoptimalkannya adalah Menghadapi tantangan penegakan hukum siber di era teknologi lintas batas memerlukan langkah-langkah konkret dan berkelanjutan dari berbagai pihak. Pertama, pemerintah Indonesia perlu memperkuat regulasi nasional yang lebih adaptif terhadap perkembangan teknologi. Hukum yang terlalu kaku dan lambat mengikuti dinamika digital akan tertinggal dari modus kejahatan siber yang semakin canggih. Oleh karena itu, pembaruan regulasi harus dilakukan secara berkala, dengan melibatkan para pakar hukum, teknologi, dan keamanan siber, sehingga kebijakan yang dihasilkan mampu menjawab kebutuhan penegakan hukum secara efektif.

DAFTAR PUSTAKA

Agus Nilmada Azmi, Syarah Shabrina. “Challenges of Universal Adoption of The Budapest Convention on Cybercrime”, Prosiding The 5th International Conference on Technology.” *Education, And Social Science* 1, no. 1 (2023).

Agus Wibowo. *Globalisasi Digital*. Semarang: Yayasan Prima Agus Teknik, 2023.

Akbar Kurnia Putra. “Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional.” *Jurnal Ilmu Hukum* 3, no. 2 (2024): 47.

Dewi. “Cybercrime Dalam Abad 21: Suatu Perspektif Menurut Hukum Internasional.” *Masalah-Masalah Hukum* 40, no. 4 (2011): 527.

Efendi, Jonaedi, Jhonny Ibrahim, and Prasetijo Rijadi. “Metode Penelitian Hukum: Normatif Dan Empiris,” 2016.

Fadhila Inas Pratiwi. “Analisis Ancaman Dan Respon Keamanan Siber Di Indonesia.” Uniar News, 2024.

Farah Diba Tanzilla, Margaretha Hanita, And Bondan Widiawan. “Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law’,.” *International Journal Of Progressive Sciences And Technologies* 40, no. 2 (2023): 160.

Gianpiero Greco, Nicola Montinaro. “The Phenomenon Of Cybercrime: From The Transnational Connotation To The Need For Globalization Of Justice.” *European Journal of Social Sciences Studies* 6, no. 1 (2021): 13.

Mustameer, H. “Penegakan Hukum Nasional Dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0.” *Jurnal Yustika: Media Hukum Dan Keadilan* 25, no. 1 (2022): 40–53.

Republik Indonesia. "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," no. September (2008): 1–2.

Septi Dyah Tirtawati, Joko Setiyono. "Menilik Penerapan Prinsip Yurisdiksi Universal Negara Terhadap Kejahatan Perompakan Di Laut Lepas Menurut Hukum Internasional." *Jurnal Al-Daulah* 10, no. 2 (2022).

Sri Mamudji, Soerjono Soekanto. *Penilitian Hukum Normatif (Suatu Tinjauan Singkat)*. Jakarta: Rajawali Pers, 2001.

Vandebosch, Heidi, and K. V Cleemput. "Defining Cyberbullying: A Qualitative Research into the Perceptions of Youngsters." *Cyberpsychology and Behavior* 11, no. 4 (2008): 449–503.

Wildan Fahriza And Muhammad Arif Sahlepi. "Effectiveness OfLaw Enforcement Against Cybercrime In Indonesia On Hacking Crimes And The Role Of The Ite Law." *Law Synergy Conference* 1, no. 1 (2024): 178.