



Tantangan Penegakan Hukum Siber Terhadap Kejahatan Lintas Batas Negara (*Transnational Cybercrime*) dalam Perspektif Hukum Internasional

Yudhitiya Dyah Sukmadewi¹

¹ Fakultas Hukum, Universitas Semarang, Indonesia

Korespondensi: yudhitiyasukmadewi@usm.ac.id

Informasi Artikel

Riwayat artikel:

Received Sept 8th, 2026

Revised Oct 5th, 2026

Accepted Oct 21th, 2026

Keyword:

Kejahatan siber; Kejahatan lintas batas negara; Hukum internasional; Mutual Legal Assistance; Budapest Convention; Sistem hukum.

ABSTRAK

Mengingat ruang siber merupakan ruang tanpa batas dan sangat dimungkinkan banyak kejahatan siber yang dilakukan lintas batas negara. Dengan demikian, perlu dikaji lebih lanjut mengenai tantangan penegakan hukum siber terhadap kejahatan lintas batas negara (*transnational cybercrime*) dalam perspektif hukum internasional agar dapat dilakukan upaya pencegahan dan penyelesaiannya secara komprehensif. Teori tersebut digunakan untuk menjelaskan tantangan yang dihadapi dalam penegakan hukum siber terhadap kejahatan lintas batas negara dari aspek substansi hukum (*legal substance*), struktur hukum (*legal structure*) serta budaya hukum (*legal culture*). Mekanisme seperti Mutual Legal Assistance (MLA), keberadaan Budapest Convention 2001, serta peran Interpol menjadi sarana penting dalam menjembatani keterbatasan yurisdiksi antar negara. Solusi yang dapat digunakan untuk menghadapi berbagai tantangan tersebut menuntut pendekatan yang komprehensif dan terintegrasi. Dengan demikian, sinergi antara pembaruan regulasi, penguatan kelembagaan, dan peningkatan kesadaran masyarakat menjadi faktor utama dalam mewujudkan penegakan hukum siber yang efektif terhadap kejahatan lintas batas negara.



© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

PENDAHULUAN

Guna memenuhi kebutuhan hidup yang semakin meningkat, manusia dituntut untuk berinovasi. Salah satunya yaitu adanya kecanggihan teknologi yang dapat memudahkan akses kehidupan manusia dari semula bersifat manual menjadi serba digital. Internet (*interconnected networking*) merupakan contoh dari kecanggihan teknologi yang dapat menghubungkan jutaan perangkat di seluruh dunia untuk saling berkomunikasi, bertukar informasi, akses layanan digital secara cepat tanpa batas ruang dan waktu. Sebagai contoh, dengan adanya internet, pendidikan dapat dilakukan jarak jauh hingga antar negara tanpa perlu bertemu secara langsung dengan menggunakan aplikasi seperti *zoom meeting*, *microsoft teams* dan *google meet*. Pada bidang ekonomi, internet dapat dimanfaatkan untuk mengakses layanan perbankan digital seperti penggunaan *mobile banking*, *internet banking* hingga *e-wallet*, serta di bidang kesehatan, internet juga dapat digunakan untuk melakukan konsultasi dengan Dokter maupun pembelian obat secara *online*. Dengan adanya kecanggihan teknologi tersebut, manusia dituntut untuk cepat beradaptasi agar dapat mengoperasikannya. Disisi lain, keberadaan internet juga dapat menimbulkan dampak negatif seperti terjadinya kejahatan siber (*cyber crime*). Bahkan kejahatan siber dapat terjadi dengan melibatkan antar negara seperti *phising*, *ransomware*, *hacking*, *cyber bullying* hingga penipuan secara *online* yang tentu penegakan hukumnya tidak mudah.

Pada tahun 2024, Indonesia mengalami serangan siber terhadap Pusat Data Nasional Sementara (PDNS) (BBC Indonesia, t.t.) yang mengakibatkan gangguan pada layanan publik dari 282 instansi pemerintah. Layanan publik yang terdampak salah satunya layanan imigrasi dan layanan Penerimaan Peserta Didik Baru (PPDB). Melalui penelusuran BSSN (Badan Siber dan Sandi Negara), serangan

ini merupakan serangan siber perangkat keras perusak / *ransomeware brain chipper* varian dari *ransomeware lockbit* 3.0 yang merupakan grup peretas dari Rusia. *Ransomeware* merupakan program yang dirancang dengan tujuan untuk merusak atau menyusup sistem komputer yang menyebabkan data penting dapat diblokir sehingga penyerang dapat menuntut pembayaran tebusan kepada korban agar data dapat dibuka kembali. Dampak dari data yang diretas tersebut tentu dapat membahayakan masyarakat karena dimungkinkan terjadi penyalahgunaan identitas pribadi hingga penipuan terstruktur. Kejahatan siber atau kejahatan dunia maya merupakan tantangan serius bagi masyarakat dan berbahaya bagi individu atau organisasi yang menjadi korban. Kejahatan dunia maya juga dapat merugikan pribadi, organisasi dan pemerintah walaupun di satu sisi memberikan manfaat besar dalam hal efisiensi dan efektifitas (Butarbutar, 2023) Kasus tersebut merupakan contoh dari kejahatan siber yang terjadi di Indonesia dengan melibatkan negara lain atau disebut sebagai kejahatan lintas batas negara.

Kejahatan siber (*cyber crime*) merupakan konsekuensi dari perkembangan teknologi yang semakin canggih dan mempunyai dampak buruk bagi kehidupan manusia. *Cyber crime* didefinisikan sebagai suatu bentuk penggunaan fasilitas komputer atau sistem elektronik yang digunakan untuk menyebabkan kerusakan pada sistem elektronik yang dituju oleh pelaku dengan memaksa masuk ke dalam sistem elektronik tersebut secara melawan hukum. (Akbar dkk., 2025) Banyaknya bermunculan jenis kejahatan yang berbasis teknologi harus pula diiringi dengan berkembangnya kemampuan dibidang hukum dalam upaya pencegahan dan penanggulangannya. Kejahatan berbasis teknologi modern memiliki karakteristik yang berbeda dengan kejahatan tradisional, sehingga diperlukan adanya kebijakan hukum yang benar-benar dapat menjangkau dan menanggulangnya. (Haryadi, 2012, hlm. 109) Adapun penegakan hukum *cyber crime* di Indonesia telah diakomodasi antara lain dengan adanya Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah direvisi terakhir pada tahun 2014 serta Undang-Undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi. Regulasi tersebut merupakan dasar yang dapat digunakan untuk memberikan kepastian hukum guna menyelesaikan kasus-kasus *cyber crime*. Selain itu, didukung pula dengan adanya Direktorat Tindak Pidana Siber yang berada dibawah Kepolisian sebagai Aparat Penegak Hukum.

Meskipun upaya penegakan hukum terhadap *cyber crime* telah dilaksanakan di Indonesia, namun tingkat kejahatan tersebut masih marak terjadi. Berdasarkan data yang dihimpun oleh pemerintah, hingga pertengahan 2025 terdapat 1,2 juta laporan penipuan digital yang masuk ke sistem pengaduan publik. Selain itu, sepanjang November 2024 hingga Januari 2025 tercatat kerugian finansial akibat kejahatan siber mencapai Rp.476 Miliar. (Kementerian Komunikasi dan Digital, t.t.-a) Mengingat ruang siber merupakan ruang tanpa batas dan sangat dimungkinkan banyak kejahatan siber yang dilakukan lintas batas negara. Tentu hal tersebut tidak hanya berpedoman pada regulasi nasional saja melainkan juga menggunakan regulasi internasional. Dengan demikian, perlu dikaji lebih lanjut mengenai tantangan penegakan hukum siber terhadap kejahatan lintas batas negara (*transnational cybercrime*) dalam perspektif hukum internasional agar dapat dilakukan upaya pencegahan dan penyelesaiannya secara komprehensif. Dalam melakukan kajian, ini akan digunakan teori yang relevan dengan pembahasan yaitu Teori Sistem Hukum oleh Larence M.Friedman. Teori tersebut digunakan untuk menjelaskan tantangan yang dihadapi dalam penegakan hukum siber terhadap kejahatan lintas batas negara dari aspek substansi hukum (*legal substance*), struktur hukum (*legal structure*) serta budaya hukum (*legal culture*).

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka terdapat tiga rumusan masalah yang akan dilakukan pembahasan, yaitu :

Bagaimana penegakan hukum siber terhadap kejahatan lintas batas negara (*transnational cybercrime*) dalam perspektif hukum internasional ?

Bagaimana tantangan penegakan hukum siber terhadap kejahatan lintas batas negara (*transnational cybercrime*) dalam perspektif hukum internasional ?

Bagaimana solusi yang digunakan guna menghadapi tantangan penegakan hukum siber terhadap kejahatan lintas batas negara (*transnational cybercrime*) dalam perspektif hukum internasional ?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum doktrinal (*doctrinal legal research*) yang berfokus pada kajian terhadap norma, asas, dan prinsip hukum yang berkaitan dengan penegakan hukum siber terhadap kejahatan lintas batas negara (*transnational cybercrime*) dalam perspektif hukum internasional. Penelitian dilakukan melalui pendekatan perundang-undangan (*statute approach*),

pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan hukum (*comparative approach*). Pendekatan tersebut digunakan untuk mengkaji kesesuaian antara ketentuan hukum nasional dan instrumen hukum internasional, sekaligus mengidentifikasi persoalan yurisdiksi serta hambatan dalam pelaksanaan kerja sama penegakan hukum antarnegara.

Bahan hukum yang digunakan terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer meliputi peraturan perundang-undangan nasional yang berkaitan dengan kejahatan siber, antara lain Undang-Undang tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang tentang Perlindungan Data Pribadi, Undang-Undang tentang Bantuan Timbal Balik dalam Masalah Pidana, serta instrumen hukum internasional seperti *Budapest Convention on Cybercrime 2001* dan perjanjian kerja sama bantuan hukum timbal balik antarnegara. Adapun bahan hukum sekunder diperoleh melalui penelusuran literatur hukum, buku, artikel jurnal ilmiah, hasil penelitian terdahulu, serta publikasi lembaga terkait yang relevan dengan permasalahan penelitian.

Analisis bahan hukum dilakukan secara kualitatif dengan menggunakan metode deskriptif-analitis dan penalaran hukum untuk menjelaskan hubungan antara ketentuan normatif dengan persoalan penegakan hukum siber lintas negara. Analisis tersebut menggunakan teori sistem hukum Lawrence M. Friedman sebagai landasan untuk mengidentifikasi tantangan penegakan hukum melalui tiga unsur utama, yaitu substansi hukum (*legal substance*), struktur hukum (*legal structure*), dan budaya hukum (*legal culture*). Hasil analisis selanjutnya digunakan untuk merumuskan solusi terhadap berbagai hambatan penegakan hukum siber lintas negara, khususnya dalam penguatan harmonisasi hukum, kapasitas aparat penegak hukum, serta kerja sama internasional.

HASIL DAN PEMBAHASAN

Penegakan Hukum Siber Terhadap Kejahatan Lintas Batas Negara (*Transnational Cybercrime*) dalam Perspektif Hukum Internasional

Internet merupakan kebutuhan primer di era yang serba digital seperti saat ini, karena internet digunakan sebagai sarana untuk memudahkan akses kehidupan manusia seperti berkomunikasi dan mencari informasi secara cepat, mudah dan tanpa batas. Namun pada prakteknya, penggunaan internet tidak diiringi dengan pemahaman mengenai pentingnya akses keamanan dalam penggunaannya sehingga dapat dimanfaatkan oleh oknum – oknum tertentu untuk melakukan tindakan kejahatan demi mencari keuntungan. Kejahatan ini bukan merupakan kejahatan biasa melainkan jenis kejahatan baru yang terjadi di dunia siber / dunia maya seperti peretasan data, penipuan, perundungan, pencurian, penyebaran berita bohong dan jenis kejahatan lainnya. Kejahatan ini dikenal dengan istilah kejahatan siber (*cyber crime*), dimana kecanggihan teknologi yang seharusnya dapat dimanfaatkan dengan maksimal justru digunakan dengan itikad tidak baik.

Dalam dua dokumen kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan Wina Austria pada tahun 2000 menjelaskan adanya dua istilah yang terkait dengan pengertian *cyber crime* yaitu *cyber crime* dan *computer related crime*. *Cyber crime* dalam arti sempit (*in a narrow sense*) disebut sebagai *computer crime* “*Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them.*”. Sedangkan dalam arti luas (*in a broader sense*) disebut sebagai *computer related crime* “*Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possess Pion, offering or distributing information by means of a computer system or network*” (Arief, 2007, hlm. 24).

Terdapat pendapat lain yang menyatakan bahwa kejahatan komputer atau kejahatan di dunia *cyber* (*cyber crime*) adalah upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut. (Mansur & Gultom, 2009, hlm. 8) Dengan demikian, secara sederhana *cyber crime* atau kejahatan siber dapat disimpulkan sebagai bentuk kejahatan dengan menggunakan teknologi informasi yang dilakukan dalam ruang siber dan mengakibatkan kerugian bagi target kejahatan tersebut. Dengan kata lain, dapat dimaknai pula sebagai kejahatan yang berhubungan dengan dunia siber (dunia maya).

Dunia *cyber* atau dalam istilah Indonesia dikenal dengan dunia maya (atau disebut juga ruang siber atau mayantara; bahasa inggris : *cyber space*) merupakan sebuah media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal balik secara

online (terhubung langsung). (Susanto dkk., 2023) Kata "*cyberspace*" (dari *cybernetics* dan *space*) berasal dan pertama kali diperkenalkan oleh penulis novel fiksi ilmiah, William Gibson dalam buku ceritanya, "*Burning Chrome*", 1982 dan menjadi populer pada novel berikutnya, *Neuromancer*, 1984 yang menyebutkan bahwa "*Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding*". (Susanto dkk., 2023)

Cyber crime sendiri memiliki karakteristik yang khas jika dibandingkan dengan kejahatan konvensional, yaitu : (Hukumonline, t.t.)

Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang atau wilayah maya (*cyber space*) sehingga tidak dapat dipastikan yurisdiksi hukum mana yang berlaku terhadapnya Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet Perbuatan tersebut mengakibatkan kerugian materiil maupun immaterial yang cenderung lebih besar dibandingkan kejahatan konvensional. Pelakunya adalah orang menguasai penggunaan internet beserta aplikasinya. Perbuatan tersebut seringkali dilakukan secara trans-nasional / melintasi batas negara.

Adapun jenis kejahatan siber dapat dikategorikan meliputi pertama, rekayasa sosial dan tipu daya (*social engineering and trickery*); kedua, pelecehan daring (*online harassment*); ketiga, kejahatan terkait identitas (*identify-related crimes*); keempat, peretasan (*hacking*) serta terakhir penolakan layanan dan informasi (*denial of service and information*) (Butarbutar, 2023, hlm. 311). Mengingat pelaku dari kejahatan siber tersebut sering dilakukan secara trans-nasional sehingga penegakan hukumnya juga harus disesuaikan. Penegakan hukum lintas negara tentu membutuhkan kolaborasi antar negara untuk menindak kejahatan dengan menggunakan mekanisme secara internasional.

Penegakan hukum siber terhadap kejahatan lintas batas negara (*transnational cybercrime*) dalam perspektif hukum internasional dapat dilakukan dengan melibatkan regulasi dan aparat penegak hukumnya. Adapun penjelasannya sebagai berikut :

Mekanisme Bantuan Timbal Balik / *Mutual Legal Assistance* (MLA)

Perkembangan kejahatan transnasional yang semakin kompleks menuntut adanya mekanisme kerjasama internasional yang efektif dalam penegakan hukum. Indonesia sebagai negara yang aktif dalam pergaulan internasional telah menembangkan kerangka hukum yang komprehensif untuk menangani berbagai bentuk kejahatan lintas batas negara melalui instrumen Bantuan Hukum Timbal Balik. Keberadaan landasan hukum yang kuat menjadi prasyarat fundamental dalam implementasi Kerjasama penegakan hukum internasional yang efektif dan berkelanjutan. (Asnawi & Natamiharja, 2025) MLA ini merupakan bentuk kerjasama internasional yang memungkinkan negara saling membantu berkaitan dengan penyidikan, penuntutan dan pemeriksaan di sidang peradilan terhadap pengungkapan kejahatan antar negara. Ketentuan Peraturan Perundang-undangan yang digunakan menyesuaikan dengan regulasi yang berlaku pada negara yang diminta. Indonesia memiliki landasan hukum MLA melalui Undang-Undang No.1 Tahun 2006 tentang bantuan Timbal Balik dalam Masalah Pidana. Undang-Undang tersebut bertujuan sebagai pedoman bagi Indonesia dalam meminta maupun memberikan bantuan timbal balik dalam masalah pidana. Selain itu, Undang-Undang ini juga dapat digunakan sebagai pedoman dalam membuat perjanjian dengan negara lain terkait bantuan timbal balik dalam masalah pidana.

Pada bagian penjelasan disebutkan bahwa asas atau prinsip bantuan timbal balik terhadap masalah pidana didasarkan pada ketentuan hukum acara pidana, perjanjian antar negara, konvensi serta kebiasaan internasional. Bantuan timbal balik ini dilakukan berdasarkan suatu perjanjian dan jika belum ada perjanjian maka bantuan dapat dilakukan atas dasar hubungan baik. Dengan demikian, MLA merupakan instrumen yang sangat penting dalam penegakan hukum terhadap tindak pidana transnasional karena memungkinkan Aparat Penegak Hukum untuk mengatasi hambatan yurisdiksi dalam proses pengungkapan tindak kejahatan. Bantuan timbal balik dapat berupa (Republik Indonesia, 2006, Pasal 13 ayat (2)), Mengidentifikasi dan mencari orang; Mendapatkan pernyataan atau bentuk lainnya; Menunjukkan dokumen atau bentuk lainnya; Mengupayakan kehadiran orang untuk memberikan keterangan atau membantu penyidikan; Menyampaikan surat; Melaksanakan permintaan pengeledahan dan penyitaan; Perampasan hasil tindak pidana; Memperoleh kembali sanksi denda berupa uang sehubungan dengan tindak pidana; Melarang transaksi kekayaan, membekukan asset yang

dapat dapat dilepaskan atau disita atau yang mungkin diperlukan untuk memenuhi sanksi denda yang dikenakan, sehubungan dengan tindak pidana serta bantuan lain yang sesuai dengan Undang-Undang.

Prinsip timbal balik atau disebut sebagai prinsip resiprokal menjadi fokus utama dalam implementasi bantuan hukum, dimana setiap negara anggota mempunyai kewajiban hukum untuk memberikan bantuan serupa apabila diminta oleh penerima permintaan bantuan di masa mendatang. Meskipun antar negara saling membantu berdasarkan perjanjian yang telah ada, namun tetap menghormati kedaulatan hukum dan kedaulatan negara masing-masing serta peraturan perundang-undangan yang berlaku di tiap negara. Dalam MLA ini, biasanya juga diatur mengenai ketentuan penolakan bantuan, khususnya terkait tindak pidana yang belatar belakang politik, tindak pidana militer, penuntutan yang telah kedaluarsa dan *ne bis in idem*. Berikut, beberapa perjanjian internasional terkait dengan MLA baik secara bilateral maupun multilateral, meliputi :

ASEAN Treaty on Mutual Legal Assistance

Perjanjian ini muncul sebagai upaya penting untuk menjembatani kesenjangan kerja sama antara negara-negara anggota ASEAN (Brunei Darussalam, Kamboja, Indonesia, Laos, Malaysia, Myanmar, Filipina, Singapura, Thailand dan Vietnam). Perjanjian ini diratifikasi oleh Indonesia pada tahun 2004 dan kemudian dituangkan dalam UU No.1 Tahun 2006, menunjukkan komitmen Indonesia untuk menegakkan kerja sama hukum internasional dalam menjaga hubungan diplomatik dan memfasilitasi permintaan bantuan hukum antara negara-negara anggota ASEAN. (Asnawi & Natamiharja, 2025, hlm. 434) Perjanjian tersebut merupakan Kerjasama multilateral yang berpedoman pada harmonisasi prosedur hukum pidana internasional dengan tetap menggunakan prinsip-prinsip kedaulatan nasional pada setiap negara peserta. Terdapat 32 Pasal dalam perjanjian tersebut yang intinya mengatur mengenai ruang lingkup bantuan seperti penyidikan, penuntutan dan pemeriksaan di pengadilan. Kemudian mengatur ketentuan mengenai prosedur permintaan, pengambilan barang bukti, pelacakan dan perampasan aset serta penolakan bantuan.

Mutual Legal Assistance Republik Indonesia dan Swiss

Pemerintah Indonesia melalui Menteri Hukum dan HAM menandatangani MLA pada tahun 2019 di Bern, Swiss. Perjanjian ini terdiri dari 39 Pasal yang antara lain mengatur bantuan hukum mengenai pelacakan, pembekuan, penyitaan hingga perampasan aset hasil tindak kejahatan. Atas usulan Indonesia, perjanjian yang ditandatangani tersebut menganut prinsip retroaktif. Prinsip tersebut memungkinkan untuk menjangkau tindak pidana yang telah dilakukan sebelum berlakunya perjanjian sepanjang putusan pengadilannya belum dilaksanakan. Hal ini sangat penting guna menjangkau kejahatan yang dilakukan sebelum perjanjian ini. (Kementerian Komunikasi dan Digital, t.t.-a)

Mutual Legal Assistance Republik Indonesia dan Australia

Indonesia melakukan perjanjian MLA dengan Australia yang ditandatangani pada Oktober 1995 yang kemudian disahkan melalui Undang-Undang No.1 Tahun 1999 tentang pengesahan Perjanjian antara Republik Indonesia dan Australia mengenai Bantuan Timbal Balik dalam Masalah Pidana. Perjanjian tersebut dilaksanakan dengan tujuan untuk meningkatkan Kerjasama dalam rangka penegakan hukum dan pelaksanaan peradilan antara Indonesia dan Australia terkait (Republik Indonesia, 1999) Pengambilan alat bukti/barang bukti dan untuk mendapatkan pernyataan dari orang, termasuk pelaksanaan surat rogatoir; Pemberian dokumen dan catatan lain; Lokasi dan identifikasi dari orang; Pelaksanaan permintaan untuk pencarian dan penyitaan; Upaya-upaya untuk mencari, menahan dan menyita hasil kejahatan; Mengusahakan persetujuan dari orang-orang yang bersedia memberikan kesaksian atau membantu penyidikan di negara peminta, dan jika orang itu dalam tahanan, mengatur pemindahan sementara ke negara tersebut; Penyampaian dokumen dan Bantuan lain yang sesuai dengan tujuan perjanjian ini yang tidak bertentangan dengan hukum negara diminta.

Dapun pelaksanaan prinsip-prinsip umum hukum internasional yang menitikberatkan pada asas penghormatan kedaulatan hukum dan kedaulatan negara harus mengacu pada asas tindak pidana ganda (*double criminality*). (Republik Indonesia, 1999) Beberapa hal penting dalam perjanjian juga diatur terkait penolakan pemberian bantuan, perlindungan terhadap kerahasiaan dan pembatasan penggunaan alat-alat bukti dan barang bukti serta informasi, mekanisme pemberian kesaksian atau membantu penyidikan, jaminan perlindungan keselamatan serta berlaku dan berakhirnya perjanjian.

Budapest Convention on Cybercrime 2001

Konvensi ini disebut sebagai Konvensi tentang Kejahatan Siber yang merupakan perjanjian internasional pertama yang secara spesifik mengatur mengenai kejahatan siber. Adapun tujuannya sebagai kerangka kerjasama internasional guna harmonisasi pengaturan terkait kejahatan siber dan

untuk memfasilitasi pemberantasan tindak pidana yang berkaitan dengan jaringan komputer seperti peretasan ilegal, pelanggaran hak cipta, penipuan terkait komputer dan pornografi menggunakan komputer. Konvensi ini juga dapat disebut sebagai pionir dan standar global untuk menyelesaikan kasus kejahatan siber yang kian marak. Perjanjian ini dibentuk pada tanggal 23 November 2001 di Budapest, Hungaria dan digagas oleh Negara Uni Eropa. Konvensi ini terbuka bagi negara lain untuk melakukan ratifikasi, namun Indonesia sampai dengan saat ini belum meratifikasi konvensi tersebut.

Konvensi Budapest mengatasi tantangan penegakan hukum siber melalui tiga pilar mekanisme utama yang terintegrasi yaitu harmonisasi hukum, kewenangan prosedur dan kerangka Kerjasama internasional. Pilar pertama, terdapat harmonisasi hukum substantif dimana mewajibkan negara-negara pihak untuk mengkriminalisasi serangkaian perilaku siber melalui Undang-undang domestik mereka. Ketentuan tersebut mencakup pertama, pelanggaran terhadap kerahasiaan, integritas dan ketersediaan data serta sistem komputer. Kedua, pelanggaran terkait komputer, ketiga, pelanggaran terkait konten dan terakhir pelanggaran terkait hak cipta dan hak terkait. (Novianto & Arfiani, 2025) Serta mencakup pula tanggungjawab tambahan dan sanksi termasuk tanggung jawab perusahaan atas pelanggaran yang dialokasikan atas nama badan hukum. Adapun pilar kedua adalah kewenangan procedural yang efektif dan dipercepat. Pilar ini mensyaratkan negara pihak untuk memiliki serangkaian kewenangan investigasi yang diperlukan untuk menghadapi sifat unik dari bukti digital. Pilar ketiga adalah kerangka Kerjasama internasional yang cepat dan responsif. Inti dari mekanisme yaitu setiap negara pihak wajib menunjuk sebuah poin kontak yang tersedia 24 jam sehari, 7 hari seminggu untuk memberikan bantuan *real time* dan memfasilitasi investigasi siber. Jaringan ini merupakan jaringan khusus yang berfokus pada kejahatan siber dan bukti elektronik, dan terdiri dari tim-tim multidisiplin yang terpercaya. Jaringan 24/7 memungkinkan penegak hukum dari berbagai negara untuk berkomunikasi dan berkoordinasi secara instan, memotong birokrasi yang melekat pada saluran diplomatic tradisional. Kecepatan ini sangat penting untuk menangkap bukti yang cepat hilang dan melacak pelaku yang bergerak cepat melintasi yurisdiksi. (Novianto & Arfiani, 2025)

International Criminal Police Organization (INTERPOL)

Interpol merupakan organisasi polisi dan lembaga penegak hukum internasional yang berperan dalam mengatasi masalah kejahatan dan pelanggaran hukum internasional yang berpusat di Lyon, Prancis, dengan nama ICPO INTERPOL dan memiliki jumlah anggota mencapai 190 negara serta merupakan organisasi internasional terbesar kedua setelah PBB (Perserikatan Bangsa-Bangsa). (Siti Aura F. dkk., 2023) Indonesia termasuk negara yang telah bergabung menjadi anggota Interpol sejak tahun 1954. Interpol memiliki peran penting dalam menangani kasus-kasus yang bersifat trans nasional, dimana setiap negara anggota Interpol harus bekerjasama dengan negara anggota lainnya dan Kerjasama tersebut dilakukan melalui *National Central Bureau*.

NCB Interpol Indonesia berada dibawah Divisi Hubungan Internasional kepolisian Negara Republik Indonesia yang menangani kejahatan transnasional termasuk kejahatan siber. Polri bekerjasama dengan kepolisian dari negara lain untuk menangani kejahatan transnasional dan Indonesia sering memanfaatkan jaringan interpol untuk menerbitkan *Red Notice* guna mencari dan menangkap buronan internasional yang melarikan diri keluar negeri maupun sebaliknya. Interpol Indonesia membawahi empat bagian yaitu (Interpol Indonesia, t.t.) pertama bagian kejahatan internasional, bertugas melaksanakan kegiatan Kerjasama Interpol dalam rangka pencegahan dan pemberantasan kejahatan internasional/transnasional serta pelayanan umum internasional dalam kaitannya dengan kejahatan, pelaku kejahatan dan bantuan hukum internasional, disamping itu juga melaksanakan perlindungan terhadap WNI di luar negeri. Kedua, bagian komunikasi internasional yang bertugas melaksanakan penyelenggaraan dan pengembangan sistem pertukaran informasi dalam upaya pencegahan dan pemberantasan kejahatan internasional/transnasional melalui sarana jaringan Interpol, ASEANPOL dan sarana informasi lainnya, serta mengumpulkan informasi dan pengolahan data, publikasi dan dokumentasi terhadap hasil kegiatan Divhubinter. Ketiga, bagian konvensi internasional yang bertugas mempersiapkan pelaksanaan perjanjian internasional dan penyelenggaraan pertemuan internasional baik di dalam maupun di luar negeri dalam rangka penanggulangan kejahatan internasional/transnasional dan Pembangunan kapasitas sumber daya manusia maupun sarana prasarana. Keempat, bagian *liaison officer* (LO) yang bertugas melaksanakan pembinaan para Atase Polri/SLO dan Staf Teknis/LO Polri di luar negeri, serta Kerjasama penegakan hukum di wilayah perbatasan.

Tantangan Penegakan Hukum Siber Terhadap Kejahatan Lintas Batas Negara (*Transnational Cybercrime*) dalam Perspektif Hukum Internasional

Kejahatan siber merupakan kejahatan yang bersifat transnasional, dimana pelaku kejahatan mudah untuk menyembunyikan identitasnya yang berakibat menyulitkan Aparat Penegak Hukum dalam melakukan pelacakan. Dengan demikian, penegakan hukum yang dilakukan untuk menyelesaikan kasus kejahatan siber tentu tidak mudah dan menghadapi berbagai tantangan. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), kasus kejahatan siber pada tahun 2024 meningkat sebesar 30% dibandingkan tahun sebelumnya. Kejahatan siber yang paling sering terjadi meliputi *phishing*, peretasan sistem, *ransomware* hingga penyebaran *malware*. (Kukar Kabupaten, t.t.) Berdasarkan data yang dihimpun pemerintah, sepanjang November 2024 hingga Januari 2025 tercatat kerugian finansial akibat kejahatan siber mencapai Rp.476 Miliar. Sementara itu, hingga pertengahan 2025 terdapat 1,2 juta laporan penipuan digital yang masuk ke sistem pengaduan publik (Portal Komdigi, t.t.). Termasuk kasus peretasan yang dialami oleh Indonesia pada tahun 2024 terhadap Pusat Data Nasional Sementara (PDNS) yang mengakibatkan gangguan pada layanan publik dari 282 instansi pemerintah. Layanan publik yang terdampak salah satunya layanan imigrasi dan layanan Penerimaan Peserta Didik Baru. Serangan tersebut merupakan serangan siber perangkat keras perusak / *ransomware brain chipper* varian dari *ransomware lockbit* 3.0 yang merupakan grup peretas dari Rusia.

Berdasarkan fenomena tersebut, maka penegakan hukum terhadap kasus kejahatan siber ini menghadapi tantangan yang serius. Merujuk pada Teori Lawrence M.Friedman, menekankan bahwa kepatuhan hukum dalam suatu masyarakat dipengaruhi oleh tiga elemen utama yaitu struktur hukum, substansi hukum dan budaya hukum (Mulyadi dkk., 2025). Artinya, dalam melakukan penegakan hukum harus dilihat dari sub-sub sistem yang menjalankan suatu sistem itu sendiri (hukum). Struktur hukum dilihat dari kelembagaan dalam hal ini Aparat Penegak Hukumnya, sedangkan substansi dilihat dari produk hukum yang ada baik secara tertulis maupun tidak tertulis. Sementara budaya hukum merupakan sikap, nilai, kebiasaan dan cara pandang masyarakatnya. Apabila dikaji dengan menggunakan teori tersebut, maka tantangan penegakan hukum siber terhadap kejahatan lintas batas negara meliputi :

Perbedaan Yurisdiksi dan Hukum Nasional Antar Negara (Perspektif Substansi Hukum)

Bahwa terdapat mekanisme MLA dalam penegakan hukum siber antar negara dengan penerapan asas resiprokal atau asas timbal balik. Namun, Kerjasama tersebut dapat berlaku hanya dengan negara-negara yang telah melakukan perjanjian MLA, sehingga yang menjadi kendala adalah bagaimana jika kejahatan siber terjadi antara Indonesia dengan negara yang belum melakukan kerjasama MLA karena sangat dimungkinkan dikategorikan sebagai kejahatan siber di suatu negara namun legal di negara lain. Dalam kondisi lain, dapat dimungkinkan terdapat Kerjasama MLA namun terdapat perbedaan kerangka hukum antar negara yang tidak sama. Hal tersebut tentu menyebabkan penegakan hukum terhadap kejahatan siber tersebut sulit untuk ditindak atau tidak maksimal. Tiap negara memiliki pengaturan mengenai kejahatan siber yang tidak sama dan berlaku sebagai hukum nasional di negara masing-masing. Dengan demikian kejahatan siber dirumuskan sesuai karakteristik sistem hukum dan nilai ideologi tiap negara. Bahkan sangat dimungkinkan terdapat negara-negara yang belum memiliki pengaturan yang jelas mengenai kejahatan siber.

Sebagai perbandingan, Singapura memiliki regulasi mengenai kejahatan siber yaitu *Computer Misuse Act (CMA)* dengan tujuan berfokus mengatasi kejahatan siber seperti akses tidak sah ke sistem komputer, modifikasi tanpa izin dan penggunaan perangkat atau program yang dimaksudkan untuk pelanggaran hukum. Kelebihan CMA memberikan definisi yang jelas terkait berbagai 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 (Rusydi, 2025).

Indonesia memiliki regulasi yang mengatur mengenai kejahatan siber yang salah satunya diatur dalam Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah beberapa kali diamandemen terakhir pada tahun 2024. UU ini memiliki beberapa kekuatan yang signifikan yaitu pertama, cakupan 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. Kedua, pengakuan alat bukti elektronik sebagai alat bukti hukum yang sah dan terakhir

penekanan pada perlindungan konsumensehingga melindungi dari potensi penyalahgunaan teknologi seperti pencurian identitas dan penipuan daring. Sedangkan dari kelemahan utama UU ITE ini yaitu pertama, keberadaan pasal-pasal multitafsir yang mengatur mengenai penghinaan dan pencemaran nama baik yang kerap disalahgunakan untuk membatasi kebebasan berekspresi dan berpendapat. UU ini juga tidak sepenuhnya mampu menagkomodasi perkembangan teknologi yang pesat seperti *blockchain*, *artificial intelligence* atau *metaverse*. (Rusydi, 2025) Dengan demikian, UU ITE tidak hanya mengatur mengenai kejahatan siber semata, melainkan mengatur pula terkait transaksi elektronik dan perlindungan konsumen sehingga memungkinkan kejahatan-kejahatan yang terkait seperti penipuan secara *online* dapat dijerat. Sedangkan apabila dibandingkan dengan CMA Singapura, hanya berfokus pada pencegahan dan penindakan kejahatan siber tanpa mencakup aspek transaksi *online*.

Merujuk pada fenomena lampau, penegakan hukum kejahatan siber yang mengalami hambatan, yaitu kasus *Yahoo Data Breach* yang melibatkan peretasan terhadap lebih dari 500 juta akun pengguna. Pelaku diduga berbasis di Rusia, sedangkan korban tersebar di Amerika Serikat dan Eropa. Proses investigasi mengalami kebuntuan karena Rusia menolak mengekstradisi warganya meskipun FBI telah mengeluarkan dakwaan resmi. Kasus ini menggambarkan keterbatasan MLAT dan lemahnya efektivitas Kerjasama internasional ketika berbenturan dengan kepentingan politik dan prinsip kedaulatan negara (Cakra & Arianty, 2025). Fenomena lain yaitu terjadinya konflik yurisdiksi dalam *Cloud Act* dengan GDPR (*General Data Protection Regulation*), dimana *Cloud Act* memungkinkan otoritas AS untuk meminta data dari Perusahaan teknologi meskipun data tersebut berada di wilayah Uni Eropa. Namun GDPR secara ketat membatasi transfer data lintas batas tanpa perlindungan yang memadai. Situasi ini membuat perusahaan multinasional berada dalam dilema hukum yang sulit dihindari (Cakra & Arianty, 2025) GDPR ini merupakan regulasi yang berlaku di negara – negara Eropa dalam hal perlindungan data pribadi. Sedangkan *Cloud Act (Clarifying Lawful Overseas use of Data Act)* merupakan regulasi yang berlaku di Amerika Serikat yang berfokus pada perlindungan terhadap infrastruktur kritis nasional, pencegahan terhadap serangan dari aktor negara asing dan kebebasan perusahaan teknologi dalam mengatur data pengguna, selama tidak melanggar hukum federal. Pengaturan tersebut dalam perspektif tersebut berseberangan dengan GDPR yang berlaku di Uni Eropa, dimana akses otoritas AS terhadap data di luar negeri tidak sesuai dengan regulasi GDPR yang melarang transfer data tanpa mekanisme hukum tertentu.

Selain adanya perbedaan kerangka hukum, terdapat regulasi suatu negara yang mengatur ketentuan mengenai penolakan bantuan terkait kerjasama penegakan hukum terhadap kejahatan tertentu. Sebagai contoh, Indonesia memiliki regulasi UU tentang Bantuan Timbal Balik dalam Masalah Pidana namun terdapat ketentuan mengenai penolakan penerimaan bantuan. Pada Pasal 6 UU tersebut intinya mengatur mengenai permintaan bantuan ditolak karena beberapa alasan. Alasan yang dimaksud seperti terhadap tindak pidana yang dianggap sebagai tindak pidana politik, tindak pidana berdasarkan hukum militer, persetujuan pemberian bantuan atas permintaan bantuan yang akan merugikan kedaulatan, keamanan, kepentingan dan hukum nasional serta penolakan terhadap negara asing yang tdianggap tidak dapat memberikan jaminan pengembalian barang bukti yang diperoleh berdasarkan bantuan apabila diminta. Selanjutnya dalam Pasal 7 terdapat pula ketentuan yang menjelaskan mengenai permintaan bantuan dapat ditolak karena beberapa alasan. Salah satunya terkait permintaan bantuan tersebut akan merugikan penyidikan, penuntutan dan pemeriksaan di sidang Pengadilan di Indonesia, membahayakan keselamatan orang atau membebani kekayaan negara. Meskipun kedua Pasal tersebut mengatur mengenai penolakan bantuan, namun memiliki makna yang berbeda. Permintaan bantuan ditolak bermakna otomatis pemerintah Indonesia dapat secara mutlak melakukan penolakan, sedangkan permintaan bantuan dapat ditolak bermakna pilihan. Artinya, permintaan bantuan dalam pertimbangan tertentu dapat ditolak atau diterima. Termasuk kaitannya dengan kasus kejahatan siber yang apabila masuk dalam kategori Pasal 6 dan Pasal 7 maka penegakan hukumnya menjadi terhambat, mengingat pembuktian dalam kejahatan siber tidak membutuhkan biaya yang sedikit dan waktu yang singkat.

Disisi lain, pada dasarnya telah ada ketentuan secara global yang secara spesifik mengatur mengenai kejahatan siber yang disebut dengan *Budapest Convention 2001*. Konvensi ini digunakan sebagai pedoman internasional untuk menyelesaikan kasus kejahatan siber antar negara dengan mewajibkan negara-negara yang meratifikasi untuk menyelaraskan hukum nasional tentang kejahatan siber mereka termasuk. Dalam Konvensi Budapest memuat 48 *Article* / Pasal dan terdiri dari 4 *Chapter* yang meliputi *use of terms*, *measures to be taken at the national level*, *internasional co-operation*, serta *final provisions*. Konvensi tersebut justru mempermudah negara-negara dalam penegakan hukum atas

kejahatan siber karena hukum yang berlaku menjadi seragam dan wajib untuk dilaksanakan. Terlebih lagi salah satu ketentuannya mengatur mengenai ekstradisi yang diatur dalam *Article 24*, dimana ekstradisi dapat dilakukan terhadap pelaku kejahatan siber dan harus dilaksanakan oleh negara-negara anggota. Ketentuan tersebut justru memudahkan dalam penegakan hukum terhadap kejahatan siber karena mengakomodasi regulasi mengenai kejahatan siber yang berbeda-beda antar negara sehingga menyulitkan dalam implementasi penegakan hukumnya.

Kejahatan siber merupakan kejahatan yang dikategorikan sebagai kejahatan internasional, karena dapat terjadi dan dilakukan secara trans nasional atau lintas negara yang penegakan hukumnya juga harus menyesuaikan regulasi yang berlaku secara internasional. Salah satu prinsip yang berlaku dalam hukum internasional adalah prinsip “*Aut Dedere Aut Judicare*” (Fahamsyah dkk., 2022) yang dilahirkan dari pemikiran Cherif Bassiouni, yang artinya setiap negara memiliki kewajiban untuk menuntut dan untuk mengadili pelaku kejahatan internasional dan melakukan erjasama dengan negara lain untuk menangkap serta mengadili pelaku kejahatan internasional.

Pada dasarnya, jika seseorang tersangka kriminal ditemukan di suatu negara tertentu, negara tersebut harus memilih antara mengekstradisi individu tersebut untuk diadili di negara lain atau di hadapan pengadilan pidana internasional, atau mengadili individu itu sendiri. Menurut *International Law Commission* (ILC), tujuan mendasar dari prinsip ini adalah “untuk memastikan bahwa individu yang bertanggung jawab atas kejahatan yang sangat serius dibawa ke pengadilan dengan menyediakan penuntutan dan penghukuman yang efektif terhadap individu tersebut oleh yurisdiksi yang kompeten”. Sehingga dapat disimpulkan bahwa pemberlakuan prinsip *Aut Dedere Aut Judicare* dimaksudkan untuk para pelaku yang melakukan kejahatan internasional, maupun transnasional harus diadili tanpa adanya impunitas atau alasan apapun (Fahamsyah dkk., 2022). Namun pada prakteknya, meskipun terdapat Konvensi Budapest yang dapat dijadikan sebagai pedoman yang berlaku secara internasional terhadap penegakan hukum kejahatan siber, tetapi tidak bisa secara serempak digunakan oleh negara-negara di dunia. Mengingat apabila ingin menggunakan ketentuan tersebut maka negara-negara wajib meratifikasi terlebih dahulu dan menyesuaikannya kedalam hukum nasional negara tersebut sebagaimana diatur dalam *chapter IV* mengenai *Final Provisions* meliputi *Article 36* sampai dengan *Article 39*. Hal tersebut tentu menjadi hambatan sekaligus tantangan bagi negara-negara yang belum melakukan ratifikasi Konvensi Budapest termasuk negara Indonesia yang sampai saat ini belum melakukan ratifikasi.

Keterbatasan Kemampuan Aparat Penegak Hukum (Perspektif Struktur Hukum)

Apabila ditarik ke dalam kerangka struktur hukum (legal structure) menurut Lawrence M Friedman, persoalan penegakan hukum kejahatan siber lintas negara tidak berhenti pada soal ada atau tidaknya lembaga penegakan hukumnya, melainkan pada bagaimana lembaga tersebut bekerja, berkoordinasi, dan memiliki kapasitas yang memadai untuk menangani kasus-kasus yang ada. Dalam konteks Indonesia, kendala struktural pertama yang cukup menonjol adalah keterbatasan kapasitas aparat penegak hukum, baik dari sisi kualitas sumber daya manusia maupun dukungan teknologi. Penanganan kejahatan siber menuntut keahlian digital forensik, analisis jaringan, hingga pemahaman terhadap enkripsi dan sistem informasi yang terus berkembang. Namun dalam praktiknya, tidak semua aparat memiliki kompetensi yang seragam, sehingga sering kali terjadi ketergantungan pada unit-unit tertentu seperti Direktorat Tindak Pidana Siber Polri. Kondisi ini menunjukkan bahwa struktur hukum belum sepenuhnya terdistribusi secara merata dalam menghadapi ancaman yang sifatnya kompleks dan teknologis. Hal ini juga pernah disoroti oleh Badan Siber dan Sandi Negara (BSSN) yang menyatakan bahwa peningkatan kapasitas SDM dan infrastruktur keamanan siber menjadi kebutuhan mendesak seiring meningkatnya eskalasi serangan siber di Indonesia. (Badan Siber dan Sandi Negara, 2024) Kendala struktural juga dapat muncul dari pola koordinasi antar lembaga, baik di tingkat nasional maupun internasional. Dalam lingkup domestik, penanganan kejahatan siber melibatkan berbagai institusi seperti Kepolisian, Kementerian terkait, hingga lembaga seperti BSSN, yang masing-masing memiliki kewenangan berbeda. Terdapat potensi tumpang tindih fungsi atau bahkan ego sektoral yang memperlambat respon penegakan hukum. Ketika kasus tersebut berkembang menjadi kejahatan lintas negara, kompleksitasnya meningkat, karena harus melibatkan mekanisme kerja sama internasional seperti Mutual Legal Assistance atau koordinasi melalui Interpol. Dalam praktiknya, proses ini tidak selalu berjalan cepat karena terikat pada prosedur formal dan birokrasi antarnegara. Sebagaimana dikemukakan oleh Sigid Suseno, hambatan struktural dalam penegakan hukum siber salah satunya

terletak pada belum optimalnya koordinasi antar aparat penegak hukum serta lemahnya integrasi sistem penanganan perkara berbasis teknologi. (Indradjaja dkk., 2024)

Lebih lanjut, keterbatasan struktur hukum juga berkaitan erat dengan persoalan yurisdiksi dan kedaulatan negara. Sebagai contoh, Aparat Penegak Hukum Indonesia tidak memiliki kewenangan langsung untuk melakukan tindakan di wilayah negara lain, sehingga harus bergantung pada kerja sama internasional. Dalam kondisi tertentu, hal ini menjadi kendala serius, terutama ketika negara tempat pelaku berada tidak kooperatif atau memiliki kepentingan politik tertentu. Barda Nawawi Arief, menegaskan bahwa dalam penanggulangan kejahatan transnasional, efektivitas penegakan hukum sangat ditentukan oleh kemampuan aparat penegak hukum untuk bekerja sama secara internasional, namun kerja sama tersebut sering kali terhambat oleh perbedaan sistem hukum dan kepentingan nasional masing-masing negara. (Arief, 2018, sebagaimana dikutip dalam Maaliki, 2024) Akibatnya, struktur hukum yang ada menjadi terfragmentasi dan tidak mampu bekerja secara optimal dalam menghadapi kejahatan yang justru bersifat tanpa batas.

Kendala lain yang tidak kalah penting adalah keterbatasan sarana dan prasarana pendukung penegakan hukum. Digital forensik membutuhkan perangkat lunak dan perangkat keras yang canggih serta biaya yang tidak sedikit. Dalam beberapa kasus, proses pembuktian menjadi terhambat karena keterbatasan alat untuk menelusuri jejak digital atau mengamankan barang bukti elektronik secara cepat. Edmon Makarim juga menekankan bahwa dalam rezim hukum siber, keberhasilan penegakan hukum tidak hanya bergantung pada norma hukum, tetapi juga pada kesiapan infrastruktur teknologi dan sistem pembuktian elektronik yang andal. (Makarim, 2005, sebagaimana dikutip dalam Sugiarti, 2023) Dengan kata lain, struktur hukum dalam arti kelembagaan tidak dapat dipisahkan dari dukungan teknologi yang menyertainya.

Menurut Fadhila, sebagaimana dikutip oleh Risma menjelaskan bahwa, berdasarkan survey yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN), kurang dari setengah lembaga pemerintah di Indonesia memiliki kebijakan keamanan siber yang memadai, yang menunjukkan adanya kesenjangan signifikan dalam infrastruktur keamanan digital negara. Masalah ini semakin terasa ketika mengingat kasus-kasus seperti serangan siber terhadap database pemerintah atau kebocoran data besar, seperti insiden kebocoran data pengguna *platform e-commerce* besar di Indonesia pada tahun 2020 (Risma Siti M., 2024)

Dengan demikian, apabila dilihat secara utuh, kendala penegakan hukum kejahatan siber transnasional dari sisi struktur hukum dalam perspektif Friedman menunjukkan adanya persoalan yang bersifat sistemik. Keterbatasan kapasitas aparat, belum optimalnya koordinasi kelembagaan, hambatan yurisdiksi lintas negara, serta kurangnya dukungan sarana teknologi menjadi faktor yang saling berkaitan dan memperlemah efektivitas penegakan hukum. Struktur hukum yang seharusnya menjadi “mesin” dari sistem hukum justru belum sepenuhnya adaptif terhadap karakter kejahatan siber yang cepat, lintas batas, dan berbasis teknologi tinggi.

Perbedaan Kesadaran Masyarakat Mengenai Kejahatan Siber (Perspektif Budaya Hukum)

Kejahatan siber merupakan kejahatan yang dapat dilakukan antar negara dan berdampak merugikan masyarakat secara luas. Sebagai contoh di Indonesia, sepanjang Januari hingga Agustus 2025 tercatat 2.597 laporan polisi (Direktorat Reserse Siber) terkait tindak pidana siber dengan total kerugian masyarakat mencapai Rp.24,3 Miliar yang didominasi kejahatan *online scam*, *phising* serta pinjaman *online* ilegal (Pinjol). Selain melibatkan pelaku lokal, penyidik juga mengidentifikasi jaringan internasional yang beroperasi di Indonesia, Malaysia dan Kamboja. Di dalam negeri, sindikat biasanya mencari *nominee* untuk membuka rekening bank atau dompet kripto yang kemudian dijual ke jaringan penipuan luar negeri. Server pengendali sebagian besar berada di Kamboja, tempat operator menjalankan skema kejahatan lintas negara tersebut. Berdasarkan hasil penelusuran, platform yang paling sering digunakan untuk menipu adalah *WhatsApp* (486 kasus); *Instagram* (98 kasus); *Facebook* (66 kasus) dan *e-commerce* (30 kasus) (Media Hub Polri, t.t.). Hal tersebut terjadi bukan tanpa alasan, mengingat masyarakat Indonesia memanfaatkan kecanggihan teknologi yang ada namun belum disertai dengan pengetahuan literasi digital yang memadai.

Hal tersebut tidak terlepas dari tingkat pemahaman masyarakat Indonesia mengenai keamanan siber masih rendah, sehingga kesadaran akan pentingnya perlindungan siber bagi pengguna internet masih terbatas (Risma Siti M., 2024) Penggunaan internet yang didominasi oleh generasi muda, berdampak pula dengan mudahnya identitas pribadi hingga aktivitas pribadi di kehidupan sehari-hari dipublikasikan melalui akun sosial media. Hal tersebut terkadang tidak disadari sebagai bentuk

ancaman terhadap celah kejahatan karena informasi data pribadi dapat diakses oleh semua orang, tanpa batasan ruang dan waktu. Kebiasaan demikian kemudian membentuk pola dan diikuti oleh mayoritas masyarakat, seperti budaya *oversharing* di media sosial. Apabila data pribadi dengan mudah diakses, maka dengan mudah pula kejahatan siber ini dilakukan, seperti peretasan terhadap akun perbankan secara *online* maupun akun penting lainnya.

Data pribadi menjadi sasaran potensial kejahatan siber. Keberadaan data pribadi dalam konsep digitalisasi di era disrupsi menghadirkan pertanyaan penting mengenai privasi, keamanan, dan bagaimana data tersebut dikelola. Mudah-mudahan mengakses data pribadi seseorang dan membagikannya tanpa kontrol dari si pemilik data memunculkan beberapa kasus terkait kebocoran data pribadi yang meliputi munculnya promosi produk properti, asuransi, fasilitas pribadi yang secara langsung menyasar si pemilik data pribadi padahal si pemilik data tidak pernah menyerahkan data pribadi tersebut kepada instansi yang mempromosikan. Ada pun dalam beberapa kasus pelanggaran privasi data pribadi dan berujung pada aksi penipuan (Santosa dkk., 2025)

Selain itu, rendahnya kesadaran masyarakat sebagai pengguna internet dalam memberikan akses keamanan pada akun yang dimiliki menyebabkan kejahatan siber semakin meningkat, seperti peretasan dan penipuan *online*. Hal tersebut didukung pula oleh survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) (Asosiasi Penyelenggara Jasa Internet Indonesia, t.t.) pada tahun 2023 dengan hasil 66,82% masyarakat Indonesia enggan untuk mengganti *password* akun yang dimiliki dan hanya 5,97% Responden mengganti *password* mereka satu kali dalam sebulan. Survei tersebut melibatkan 8.510 Responden.

Rendahnya kesadaran hukum terhadap regulasi yang mengatur mengenai penggunaan internet juga memiliki peran penting terkait penegakan hukum kejahatan siber. Secara garis besar, masyarakat cenderung memanfaatkan internet tanpa mengetahui batasan dan etika dalam penggunaannya yang diatur dalam regulasi. Rendahnya kesadaran hukum dapat dilatarbelakangi karena ketidaktahuan mengenai instrumen hukum maupun rendahnya pemahaman mengenai regulasi tersebut. Disisi lain, pemerintah Indonesia telah melakukan upaya untuk membuat regulasi yang dapat dijadikan sebagai pedoman dalam penggunaan internet melalui pengesahan Undang-Undang tentang Informasi dan Transaksi Elektronik (ITE) dan Undang-Undang tentang Perlindungan Data Pribadi. Namun kesadaran hukum yang masih rendah menjadi potensi kian maraknya kejahatan siber terjadi di Indonesia. Meskipun terdapat asas "*fictie hukum*" yang menyatakan bahwa setiap orang dianggap mengetahui hukum yang berlaku, namun pada prakteknya tidak demikian. Hal tersebut didukung oleh penelitian yang dilakukan oleh Arsyad Hoshi dkk (Hoshi dkk., 2023), yang menunjukkan bahwa pemahaman etika dan nilai kebahasaan dalam media sosial di masyarakat masih sangat rendah. Implementasi pemahaman etika dan nilai kebahasaan masyarakat dalam penggunaan media sosial dirasa sangat kurang efektif dan efisien dalam mewujudkan lingkungan positif di media sosial. Penggunaan bahasa kasar atau tidak etis seringkali ditemukan di berbagai aplikasi media sosial. Hal tersebut tentu memicu kejahatan siber seperti berita *hoax* hingga *cyber bullying*.

Sebagai perbandingan, penelitian yang dilakukan oleh WJP (*World Justice Project*) (Tempo, t.t.) pada tahun 2022 dengan judul "*Rule of Law Index 2022*" menunjukkan bahwa Indonesia menempati urutan ke-64 dari 140 negara sebagai negara paling taat hukum. Dalam skala 10 besar, Denmark merupakan negara yang menduduki peringkat pertama, disusul Norwegia, Finlandia, Swedia, Belanda, Jerman, diakses pada tanggal 28 April 2026, Pukul 21.00 WIB

Selandia Baru, Luksemburg, Estonia dan terakhir Irlandia. Berdasarkan hasil penelitian tersebut menunjukkan bahwa perbedaan kesadaran hukum antar negara khususnya dalam hal ini mengenai regulasi tentang siber, akan berpengaruh pula pada penegakan hukumnya. Negara dengan masyarakat yang memiliki tingkat kesadaran hukum yang tinggi maka berpeluang rendah menjadi pelaku maupun korban dalam kejahatan siber. Sebaliknya, bahwa negara dengan tingkat kesadaran hukum yang rendah maka berpeluang besar sebagai pelaku maupun korban dalam kejahatan siber, karena kebiasaan untuk mengabaikan aturan yang ada sudah menjadi pola masyarakat. Pola yang demikian membentuk budaya masyarakat sebagai masyarakat yang mudah melakukan pelanggaran aturan maupun kejahatan. Disisi lain, rendahnya kesadaran hukum masyarakat juga berdampak pada mudahnya masyarakat sebagai korban kejahatan.

Solusi Penegakan Hukum Siber Terhadap Kejahatan Lintas Batas Negara (*Transnational Cybercrime*) dalam Perspektif Hukum Internasional

Berdasarkan tantangan yang telah dibahas sebelumnya, maka dibutuhkan solusi dalam menghadapi tantangan tersebut. Adapun solusi yang dapat dilakukan meliputi :

Harmonisasi Regulasi tentang Kejahatan Siber secara Internasional

Sebagaimana diketahui bahwa kejahatan siber merupakan kejahatan yang dapat terjadi antar negara dan penegakan hukumnya tidak mudah. Salah satu tantangan yang dihadapi dari perspektif substansi hukum adalah beragamnya regulasi mengenai kejahatan siber yang dimiliki tiap negara sebagai hukum nasional. Namun, perbedaan regulasi tersebut akan menjadi kendala apabila kejahatan siber terjadi dengan melibatkan negara asing dalam penegakan hukumnya. Meskipun terdapat mekanisme kerjasama mengenai bantuan timbal balik / MLA, tetapi belum tentu antar negara melakukan kerjasama tersebut. Dalam hal kerjasama dapat dilakukan, maka terdapat kondisi-kondisi tertentu yang mengakibatkan penegakan hukum menjadi terhambat atau bahkan tidak dapat dilaksanakan. Diantaranya, karena terjadi gesekan / kesenjangan ketentuan dalam regulasi yang berbeda antar negara. Selain itu prinsip *double criminality* juga harus ada dalam kerjasama MLA dimana kejahatan harus dianggap sama baik menurut hukum Indonesia maupun hukum negara yang diminta, sedangkan hal tersebut belum tentu diatur sama.

Sebagai contoh, terdapat pengaturan mengenai transaksi elektronik dalam UU tentang ITE yang dimiliki oleh Indonesia, namun tidak diatur ketentuan serupa dalam *Computer Misuse Act (CMA)* yang dimiliki oleh Singapura. Kemudian, tidak adanya ketentuan mengenai ekstradisi dalam UU tentang ITE, sehingga harus menggunakan regulasi lain apabila negara yang melakukan permintaan, mengajukan permohonan ekstradisi. Tentu hal tersebut menjadi kendala yang membutuhkan solusi penyelesaian. Berdasarkan tantangan tersebut, maka sangat penting dilakukan harmonisasi mengenai ketentuan kejahatan siber secara internasional dengan menggunakan satu pedoman hukum yang sama dan berlaku sama di semua negara di dunia.

Harmonisasi ketentuan tersebut akan sangat bermanfaat untuk memudahkan penegakan hukum antar negara karena berpedoman pada satu regulasi yang sama, sehingga makna kejahatan siber hingga sanksinya bersifat seragam. Pada dasarnya telah ada ketentuan secara internasional mengenai kejahatan siber yang diatur dalam *Budapest Convention 2001*. Dalam Konvensi tersebut telah diatur secara rinci mengenai apa yang dimaksud dengan kejahatan siber, kategori tindak pidana hingga ketentuan sanksi, termasuk mekanisme ekstradisi. Namun, Konvensi tersebut membutuhkan mekanisme ratifikasi terlebih dahulu dari negara-negara yang ingin bergabung, sedangkan ketentuan tersebut tidak bisa digunakan apabila negara yang bersangkutan belum melakukan ratifikasi.

Indonesia menjadi salah satu negara yang sampai saat ini belum melakukan ratifikasi terhadap *Budapest Convention 2001* sehingga ketentuan ini belum dapat digunakan sebagai pedoman dalam penegakan hukum terhadap kejahatan siber yang melibatkan Indonesia. Dengan demikian, Pemerintah Indonesia wajib mempertimbangkan untuk segera melakukan ratifikasi terhadap Konvensi tersebut karena sifatnya sangat penting untuk memperkuat substansi hukum terhadap ketentuan mengenai kejahatan siber dalam skala internasional. Mengingat, kejahatan siber merupakan kejahatan yang dikategorikan sebagai kejahatan internasional, maka sangat penting membutuhkan instrumen hukum internasional yang mumpuni seperti *Budapest Convention 2001*.

Pentingnya upaya ratifikasi tersebut juga dikemukakan oleh Ermanto Fahamsyah, dkk (Fahamsyah dkk., 2022, hlm. 156) yang menyatakan bahwa adanya upaya ratifikasi Konvensi tersebut maka terjalinlah kerjasama internasional yang akan memudahkan ekstradisi, investigasi, keterbukaan informasi, alat bukti dan pelaksanaan secara efektif prinsip yurisdiksi ekstra territorial. Mekanisme ratifikasi instrumen internasional menunjukkan kesediaan untuk mengikuti standar global (Aswar dkk., 2025, hlm. 4742). Penelitian yang dilakukan oleh Moeso dan Nur Arfiani juga memperkuat untuk mengadopsi Konvensi Budapest, yang menyatakan bahwa untuk memperkuat ketahanan siber nasional, Indonesia perlu memperbaiki implementasi hukum nasional yang ada, membentuk otoritas perlindungan data yang independent, serta mempertimbangkan ratifikasi *Budapest Convention* agar mampu berkolaborasi secara efektif dalam menanggulangi kejahatan siber transnasional. (Novianto & Arfiani, 2025, hlm. 8265)

Sehingga apabila Indonesia beserta negara-negara lain melakukan ratifikasi terhadap *Budapest Convention 2001* maka ketentuan tersebut harus disesuaikan sebagai hukum nasional yang berlaku di

Indonesia. Sebagaimana tunduk pula terhadap prinsip hukum internasional yaitu "*pacta sunt servanda*". Apabila negara-negara di dunia melakukan ratifikasi maka segera terwujud harmonisasi hukum yang menciptakan keselarasan antara hukum internasional dengan hukum nasional setempat mengenai kejahatan siber. Apabila menggunakan pedoman yang sama sebagai landasan hukum, maka diharapkan penegakan hukumnya lebih maksimal. Saat ini, telah lebih dari 70 negara meratifikasi *Budapest Convention 200*, sehingga Indonesia diharapkan segera menyesuaikan.

Penguatan Kapasitas dan Integrasi Aparat Penegak Hukum

Penyelesaian perkara kejahatan transnasional memiliki kendala struktural dalam penegakan hukumnya terutama muncul dari ketidakseimbangan antara sifat kejahatan yang lintas batas dengan sistem penegakan hukum yang masih berbasis kedaulatan negara. Aparat penegak hukum bekerja dalam batas yurisdiksi nasional, sementara pelaku kejahatan memanfaatkan perbedaan sistem hukum dan celah antarnegara untuk menghindari proses hukum. Kondisi ini menyebabkan penegakan hukum seringkali tidak efektif, baik dalam tahap penyidikan, penuntutan, maupun eksekusi putusan. Penulis sepakat dengan pendapat Retno Hariati dan Irwan Triadi yang menegaskan bahwa tantangan utama penegakan hukum terhadap kejahatan transnasional terletak pada keterbatasan koordinasi antarnegara dan kapasitas institusional aparat penegak hukum, khususnya di wilayah perbatasan. (Hariati & Triadi, 2024)

Guna mengatasi problem tersebut, terdapat beberapa Solusi yang dapat diaplikasikan, solusi pertama yang harus ditempuh adalah memperkuat kerja sama internasional melalui instrumen hukum yang telah tersedia. Dalam konteks ini, United Nations melalui United Nations Convention against Transnational Organized Crime menyediakan kerangka kerja komprehensif bagi negara-negara dalam melakukan ekstradisi, bantuan hukum timbal balik (*mutual legal assistance*), serta kerja sama investigasi. Andreas Schloenhardt menjelaskan bahwa UNTOC membentuk kerangka luas kerja sama internasional yang mencakup ekstradisi dan bantuan hukum timbal balik sebagai instrumen kunci dalam pemberantasan kejahatan terorganisir lintas negara. (Schloenhardt, 2021, sebagaimana dikutip dalam Boister, 2025) Dengan demikian, optimalisasi implementasi UNTOC menjadi langkah strategis untuk mengatasi keterbatasan struktural antarnegara.

Harmonisasi sistem hukum nasional disisi lain juga menjadi solusi penting. Perbedaan definisi tindak pidana, standar pembuktian, serta prosedur hukum yang berpotensi menghambat proses ekstradisi dan penuntutan lintas negara. Cut Yeni Meutia dan Redyanto Sidi mengemukakan bahwa perbedaan sistem hukum dan yurisdiksi antarnegara merupakan hambatan utama dalam pelaksanaan ekstradisi dan penegakan hukum kejahatan transnasional. (Meutia & Sidi, 2024) Oleh karena itu, negara perlu melakukan reformasi hukum nasional dengan mengadopsi standar internasional agar tercipta keselarasan normatif yang mendukung kerja sama lintas batas. Selanjutnya, penguatan kapasitas dan integrasi kelembagaan penegak hukum merupakan langkah yang tidak kalah penting. Struktur kelembagaan yang terfragmentasi seringkali menghambat koordinasi antarinstansi, baik di tingkat nasional maupun internasional. Mhd Rifki (Rifki, 2024) menunjukkan bahwa dinamika kejahatan transnasional menuntut adanya sistem penegakan hukum yang terintegrasi dan koordinasi kelembagaan yang kuat agar respons yang diberikan menjadi efektif. Hal ini menegaskan pentingnya pembentukan mekanisme koordinasi terpadu seperti *joint task force* lintas negara dan sistem pertukaran data bersama.

Lebih lanjut, optimalisasi mekanisme bantuan hukum timbal balik / MLA menjadi bagian integral dari solusi struktural. Sona Asnawi dan Rudi Natamiharja berpendapat bahwa MLA efektif dalam memfasilitasi pertukaran alat bukti, pelacakan aset hasil kejahatan, serta koordinasi penegakan hukum lintas yurisdiksi. (Asnawi & Natamiharja, 2025) Dengan demikian, keberadaan MLA memungkinkan negara mengatasi hambatan yurisdiksi dan meningkatkan efisiensi proses pembuktian dalam perkara kejahatan transnasional. Di samping itu, penguatan kerja sama regional juga menjadi strategi yang relevan, khususnya dalam konteks kawasan seperti ASEAN. Sona Asnawi dan Rudi Natamiharja (Asnawi & Natamiharja, 2025) menegaskan bahwa kerangka kerja regional seperti ASEAN Treaty on Mutual Legal Assistance memiliki peran penting dalam menghadapi tantangan kejahatan transnasional di Kawasan.

Pada akhirnya, solusi terhadap kendala struktural penegakan hukum dalam kejahatan transnasional menuntut perubahan paradigma dari pendekatan nasional menuju pendekatan kolaboratif dan terintegrasi. Integrasi kerja sama internasional, harmonisasi hukum, penguatan kelembagaan, serta optimalisasi instrumen seperti ekstradisi dan MLA merupakan satu kesatuan yang tidak dapat dipisahkan. Hal ini sejalan dengan pandangan Jaime Cubides-Cárdenas dkk (Cubides-Cardenas dkk.,

2025) yang menegaskan bahwa kerja sama regional dan internasional tetap menjadi kunci dalam menghadapi dinamika kejahatan transnasional yang terus berkembang.

Penguatan Prinsip *Mutual Trust* sebagai Budaya Hukum

Prof. dr Romli Atmasasmita, SH. LLM, pernah menyampaikan bahwa sampai saat ini tidak ada tolok ukur termasuk dinegara maju sekalipun tentang perkembangan kesadaran hukum masyarakat, kecuali semua masalah ketidak patuhan terhadap hukum dikembalikan kepada bunyi ketentuan undang-undang. Persoalan hukum dan sosial selanjutnya dari sumber ketidak patuhan masyarakat terhadap hukum adalah, kemungkinan terbesar bagi Indonesia, disebabkan konten undang-undang itu sendiri yang tidak cocok dengan nilai-nilai keadilan yang hidup dalam masyarakat. (Atmasasmita, 2013, sebagaimana dikutip dalam Jawardi, t.t.) Kendala budaya hukum dalam penanganan kejahatan transnasional pada dasarnya tidak dapat dipisahkan dari perbedaan nilai, cara pandang, dan praktik penegakan hukum antarnegara. Perbedaan ini berimplikasi langsung pada rendahnya kepercayaan (*mutual trust*), ketidaksinkronan prosedur, serta resistensi dalam melaksanakan kerja sama internasional. Oleh karena itu, solusi terhadap problem ini tidak cukup bersifat normatif, melainkan harus menyentuh aspek transformasi budaya hukum secara bertahap dan terstruktur.

Solusi pertama adalah mendorong harmonisasi nilai dan standar dasar hukum antarnegara tanpa menghapus keberagaman sistem hukum nasional. Dalam konteks budaya hukum, harmonisasi tidak berarti menyeragamkan seluruh system hukum, tetapi menyepakati standar minimum yang dapat diterima bersama, khususnya terkait pembuktian, perlindungan hak asasi manusia, dan prosedur kerja sama lintas negara. Penelitian oleh Sona Asnawi dan Rudi Natamiharja menunjukkan bahwa salah satu hambatan utama kerja sama penegakan hukum di kawasan ASEAN adalah “disparitas sistem hukum antar negara... dan kompleksitas prosedur birokrasi,” sehingga diperlukan “harmonisasi regulasi domestik dan standardisasi prosedur operasional” untuk meningkatkan efektivitas kerja sama. (Asnawi & Natamiharja, 2025) Dengan demikian, harmonisasi menjadi langkah awal untuk menjembatani perbedaan budaya hukum yang terlalu kontras.

Solusi kedua, penguatan prinsip *mutual trust* antarnegara menjadi kunci dalam mengatasi perbedaan budaya hukum. Dalam praktik, kerja sama hukum internasional hanya dapat berjalan efektif apabila terdapat kepercayaan bahwa sistem hukum negara lain mampu menjamin keadilan dan *due process*. Tanpa kepercayaan tersebut, negara cenderung menolak atau memperlambat permintaan ekstradisi maupun *mutual legal assistance*. Oleh karena itu, negara perlu meningkatkan transparansi sistem peradilan, akuntabilitas aparat penegak hukum, serta kepatuhan terhadap standar internasional. Upaya ini secara tidak langsung akan membangun legitimasi sistem hukum suatu negara di mata negara lain, sehingga kerja sama lintas yurisdiksi menjadi lebih efektif.

KESIMPULAN

Bahwa penegakan hukum siber terhadap kejahatan lintas batas negara (*transnational cybercrime*) dalam perspektif hukum internasional pada dasarnya telah memiliki landasan melalui berbagai instrumen kerja sama internasional. Mekanisme seperti *Mutual Legal Assistance* (MLA), keberadaan *Budapest Convention* 2001, serta peran Interpol menjadi sarana penting dalam menjembatani keterbatasan yurisdiksi antar negara. Melalui mekanisme tersebut, negara-negara dapat saling membantu dalam proses penyidikan, penuntutan, hingga penegakan putusan, sehingga penanganan kejahatan siber yang bersifat transnasional dapat dilakukan secara lebih terkoordinasi. Namun demikian, implementasi mekanisme tersebut belum sepenuhnya optimal, terutama karena tidak semua negara terikat dalam perjanjian yang sama serta adanya perbedaan kepentingan nasional antar negara.

Tantangan penegakan hukum siber terhadap kejahatan lintas batas negara, dapat dipahami bahwa hambatan yang dihadapi bersifat kompleks dan mencakup berbagai aspek dalam sistem hukum. Dari perspektif substansi hukum, perbedaan regulasi antar negara serta belum adanya harmonisasi hukum internasional menjadi kendala utama, terlebih dengan belum diratifikasinya *Budapest Convention* oleh negara-negara berpotensi menghambat penanganan kejahatan lintas negara. Kemudian dari perspektif struktur hukum, keterbatasan kapasitas aparat penegak hukum, belum optimalnya koordinasi antar lembaga, serta keterbatasan sarana dan prasarana teknologi turut menghambat efektivitas penegakan hukum. Lebih lanjut, dari perspektif budaya hukum, terdapat perbedaan kesadaran hukum di tiap negara. Rendahnya kesadaran dan literasi digital masyarakat menyebabkan tingginya potensi terjadinya kejahatan siber, baik sebagai pelaku maupun korban. Keseluruhan tantangan tersebut menunjukkan

bahwa penegakan hukum siber tidak hanya bergantung pada keberadaan aturan, tetapi juga pada kesiapan institusi dan masyarakat dalam menghadapi perkembangan teknologi.

Solusi yang dapat digunakan untuk menghadapi berbagai tantangan tersebut menuntut pendekatan yang komprehensif dan terintegrasi. Upaya harmonisasi regulasi melalui adopsi standar internasional, khususnya dengan mempertimbangkan ratifikasi *Budapest Convention* 2001, menjadi langkah penting dalam memperkuat substansi hukum. Selain itu, penguatan kapasitas aparat penegak hukum serta peningkatan kualitas infrastruktur teknologi menjadi kunci dalam memperbaiki aspek struktur hukum. Di sisi lain, peningkatan kesadaran hukum dan literasi digital masyarakat juga harus menjadi prioritas guna memperbaiki budaya hukum masing-masing negara dan didukung oleh *mutual trust* antar negara guna meminimalkan terjadinya perbedaan pemahaman akan kejahatan transnasional. Dengan demikian, sinergi antara pembaruan regulasi, penguatan kelembagaan, dan peningkatan kesadaran masyarakat menjadi faktor utama dalam mewujudkan penegakan hukum siber yang efektif terhadap kejahatan lintas batas negara.

DAFTAR PUSTAKA

- Akbar, M. F., Ismansyah, & Rembrandt. (2025). Penyidikan Tindak Pidana Pencurian Informasi Data Melalui Skimming ATM Bank BNI Cabang Padang. *Unes Law Review*, 8(2).
- Arief, B. N. (2007). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Kencana Prenada Media Group.
- Asnawi, S., & Natamiharja, R. (2025). Penanganan Kasus Kejahatan Transnasional bagi Indonesia Ditinjau dari ASEAN Treaty on Mutual Legal Assistance. *Jurnal Keadilan*, 23(3). <https://jurnal.utb.ac.id/index.php/keadilan/article/view/2857>
- Asosiasi Penyelenggara Jasa Internet Indonesia. (t.t.). *Survei APJII: 66,8 Persen Warga RI Enggan Ganti Password*. <https://apjii.or.id/berita/d/survei-apjii-668-persen-warga-ri-ogah-ganti-password-akun>
- Aswar, M., dkk. (2025). Instrumen Hak Asasi Manusia Internasional (Perbandingan Ratifikasi & Implementasi Indonesia vs Malaysia/Thailand). *Journal of Artificial Intelligence and Digital Business (RIGGS)*, 4(4).
- Atmasasmita, R. (2013). *Perencanaan Pembangunan Hukum Bidang Kesadaran Masyarakat dan Aparatur Hukum 2015–2019*. [Dikutip dalam dokumen Jawardi yang dirujuk naskah asli].
- Badan Siber dan Sandi Negara. (2024). *Lanskap Keamanan Siber Indonesia 2024*. <https://alika.pesisirbaratkab.go.id/files/272/E-BOOK/262/Lanskap-Keamanaan-Siber-Indonesia-2024--BSSN.pdf>
- BBC Indonesia. (t.t.). *Serangan Siber PDNS*. <https://www.bbc.com/indonesia/articles/cxee2985jrvo>
- Boister, N. (2025). The UNTOC and International Cooperation. *Transnational Criminal Law Review*, 4. <https://doi.org/10.22329/tclr.v4i1.9646>
- Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis dan Perkembangannya. *Technology and Economics Law Journal*, 2(2).
- Cakra, A., & Arianty, A. M. (2025). Dilema Yurisdiksi di Ruang Siber: Tantangan dan Strategi Penegakan Keamanan Lintas Negara. *Judicatum: Jurnal Dimensi Cakra Hukum*, 3(1).
- Council of Europe. (2001). *Budapest Convention on Cybercrime*.
- Cubides-Cardenas, J., Hernández-Alvarado, C. E., Jimenez-Reina, J., & Roncancio-Bedoya, A. F. (2025). Regional cooperation against transnational organized crime: Challenges and opportunities in the Western Hemisphere. *Frontiers in Political Science*, 7, 1657969. <https://doi.org/10.3389/fpos.2025.1657969>
- Fahamsyah, E., Taniady, V., dkk. (2022). Penerapan Prinsip Aut Dedere Aut Judicare terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention. *De Jure: Jurnal Hukum dan Syari'ah*, 14(1).
- Hariati, R., & Triadi, I. (2024). Tantangan Penegakan Hukum pada Tindak Kejahatan Transnasional di Kawasan Perbatasan Laut Indonesia. *Jurnal Panorama Hukum*, 9(2).
- Haryadi, D. (2012). *Kebijakan Integral Penanggulangan Cyberporn di Indonesia*. Penerbit Lima.
- Hoshi, A., dkk. (2023). Krisis Pemahaman Moral dan Etika dalam Penggunaan Media Sosial. *Artikulasi: Jurnal Pendidikan Bahasa dan Sastra Indonesia*, 3(1).

- Hukumonline. (t.t.). *Dasar Hukum Cybercrime Secara Internasional dan Nasional*. <https://www.hukumonline.com/klinik/a/dasar-hukum-cybercrime-secara-internasional-dan-nasional-lt68369a29bbb93/>
- Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementasi Penyidikan terhadap Tindak Pidana Siber dalam Perspektif Perbandingan Hukum: Indonesia dan Inggris Raya. *Jurnal Ilmiah Penegakan Hukum*, 11(2).
- Interpol Indonesia. (t.t.). *Profil Interpol Indonesia*. <https://interpol.go.id/profil.php>
- Jawardi. (t.t.). *Strategi Pengembangan Budaya Hukum*. https://lsc.bphn.go.id/uploads/63367_STRATEGI%20PENGEMBANGAN%20BUDAYA%20HUKUM%20Jawardi.pdf
- Kementerian Komunikasi dan Digital. (t.t.-a). *Kejahatan Siber Capai Kerugian Rp 476 Miliar*. <https://www.komdigi.go.id/berita/siaran-pers/detail/kejahatan-siber-capai-kerugian-rp-476-m-ai-diperkuat-untuk-cegah-ancaman-di-ruang-digital>
- Kementerian Komunikasi dan Digital. (t.t.-b). *Perjanjian MLA RI-Swiss*. <https://www.komdigi.go.id/berita/berita-pemerintahan/detail/pemerintah-ri-swiss-sepakati-perjanjian-bantuan-hukum-timbal-balik-dalam-masalah-pidana>
- Kukar Kabupaten. (t.t.). *Lonjakan Kejahatan Siber di Era Digital*. <https://ttis.kukarkab.go.id/berita/lonjakan-kejahatan-siber-di-era-digital>
- Maaliki, N. E. (2024). Analysis Of Cybersecurity Regulations In Addressing Hacking Activities In The Digital Era Based On Justice Value. *Jurnal Meta-Yuridis*.
- Makarim, E. (2005). *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. RajaGrafindo Persada.
- Mansur, D. M. A., & Gultom, E. (2009). *Cyber Law: Aspek Hukum Teknologi Informasi*. PT Refika Aditama.
- Media Hub Polri. (t.t.). *Laporan Kejahatan Siber Januari–Agustus 2025*. <https://mediahub.polri.go.id/in/image/detail/279752-januariagustus-2025-ada-2597-laporan-masuk-terkait-kejahatan-siber>
- Meutia, C. Y., & Sidi, R. (2024). Transnational Crime and Extradition Challenges of Criminal Law in the Global Era. *Law Sinergy Conference*, 1(1), 359–365. <https://conference.sinergilp.com/index.php/lsc/article/view/50>
- Mulyadi, D., Yanuaria, T., & Firman. (2025). Model Kepatuhan Hukum Pendaftaran Perkawinan: Konstruksi Budaya Hukum Masyarakat Sereh Berdasarkan Teori Friedman. *Semarang Law Review*, 6(2).
- Novianto, M., & Arfiani, N. (2025). Kejahatan Siber dan Perdagangan Data Gelap (Dark Web): Tantangan Hukum Indonesia dalam Konteks Budapest Convention. *Journal of Innovation Research and Knowledge*, 5(7).
- Portal Komdigi. (t.t.). *Data Kejahatan Siber*. <https://portal.komdigi.go.id/kanal-publik/berita-kini/9525>
- Republik Indonesia. (1999). Undang-Undang Nomor 1 Tahun 1999 tentang Pengesahan Perjanjian antara Republik Indonesia dan Australia mengenai Bantuan Timbal Balik dalam Masalah Pidana.
- Republik Indonesia. (2006). Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana.
- Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (beserta perubahannya).
- Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Rifki, M. (2024). Dynamics of Transnational Crime Law Enforcement in The Era of Globalization Challenges, Opportunities and Prospects Towards a Safer Future. *Proceedings: International Forum Research on Education, Social Sciences Technology and Humanities*, 1(2), 263–268. <https://journal.berpusi.co.id/index.php/POE/article/view/878>
- Risma Siti M. (2024). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(2).
- Rusydi, M. T. (2025). Perbandingan Hukum Siber Indonesia dengan Negara ASEAN: Suatu Kajian Normatif. *Jurnal Kolaboratif Sains*, 8(1).
- Santosa, M. H., dkk. (2025). Proyeksi Kedudukan dan Fungsi Lembaga PDP dalam Menjamin Sekuritas Data Digital di Era Disrupsi. *Unes Journal of Swara Justisia*, 9(1).

- Schloenhardt, A. (2021). International Cooperation under the United Nations Convention Against Transnational Organized Crime. *Brill Research Perspectives in Transnational Crime*. https://brill.com/view/journals/rptc/3/4/article-p3_2.xml
- Siti Aura F., Michelle S. A., & Britney W. B. M. (2023). Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest on Cybercrimes. *Journal on Education*, 5(4).
- Sugiarti, I. (2023). Kepastian Hukum terhadap Penerapan dan Pemanfaatan Konsep Cyber Notary di Indonesia. *Officium Notarium*, 2(1).
- Susanto, E., Antira, L., dkk. (2023). Manajemen Keamanan Cyber di Era Digital. *Jurnal Bisnis dan Kewirausahaan*, 11(1).
- Tempo. (t.t.). *Daftar Negara Paling Taat Hukum*. <https://www.tempo.co/hukum/inilah-daftar-10-negara-paling-taat-hukum-indonesia-peringkat-berapa--264579>