ISSN: 2338 4638
Volume 8 Nomor 7 (2024)

'ADALAH
Buletin Hukum & Keadilan

Kerja Sama Internasional dalam Penanggulangan Kejahatan Siber: Urgensi Ratifikasi Konvensi Budapest dan Pembentukan Rezim Kolaboratif bagi Indonesia

Gilang Rizki Aji Putra*
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v8i7.51882

Abstract:
Cybercrime transcends territorial boundaries, constituting a transnational threat that demands coordinated international responses. This article analyzes the framework of international cooperation in combating cybercrime, evaluates Indonesia's position within the global architecture, and formulates strategic measures to strengthen its engagement. Using normative legal research with statutory, conceptual, and comparative approaches, the study finds that the Budapest Convention on Cybercrime (2001) remains the most comprehensive multilateral instrument, providing a foundation for harmonizing substantive and procedural law as well as enabling rapid cooperation mechanisms. As Indonesia currently holds observer status, structural limitations persist, including delays in Mutual Legal Assistance (MLA) processes and lack of direct access to the 24/7 point-of-contact network. Analysis of cross-border cyber incidents affecting Indonesia demonstrates that without seamless cooperation, enforcement efforts frequently stall at issues of attribution and jurisdiction. The article concludes that accession to the Budapest Convention, coupled with domestic legal harmonization and proactive cyber diplomacy, is essential.

Keywords: Transnational Cybercrime, Budapest Convention, Mutual Legal Assistance, International Cooperation, Jurisdiction.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

A. PENDAHULUAN

Revolusi digital telah melahirkan dunia yang saling terhubung, di mana arus informasi melintasi benua dalam hitungan milidetik. Namun, konektivitas ini juga memberikan panggung baru bagi aktor kriminal. Kejahatan siber, dalam sifatnya yang paling esensial, menolak gagasan tentang perbatasan. Seorang pelaku yang duduk di depan komputer di sebuah negara dapat, dalam sekejap, meretas sistem perbankan di negara lain, mencuri data warga negara ketiga, dan menyimpan hasil kejahatannya dalam dompet digital di yurisdiksi keempat. Kejahatan semacam ini tidak bisa ditanggulangi oleh satu negara saja. Upaya unilateral hampir selalu gagal karena kunci bukti, saksi, atau pelaku berada di luar jangkauan yurisdiksi nasional. Oleh karena itu, kerja sama internasional dalam penanggulangan *cybercrime* bukan lagi pilihan, melainkan sebuah keniscayaan.

Masyarakat internasional telah merespons tantangan ini dengan berbagai instrumen, mulai dari perjanjian multilateral hingga jaringan kerja sama kepolisian. Di antara semuanya, Konvensi Dewan Eropa tentang Kejahatan Siber (*Convention on Cybercrime*), yang lebih dikenal sebagai Konvensi Budapest (2001), adalah yang paling berpengaruh. Konvensi ini menyediakan kerangka komprehensif yang mencakup harmonisasi hukum pidana materiil, hukum acara, serta mekanisme kerja sama internasional yang difasilitasi oleh jaringan 24/7 *point*

of contact yang beroperasi sepanjang waktu. Hingga saat ini, lebih dari 68 negara telah meratifikasinya, sementara banyak negara lain, termasuk Indonesia, masih berada di pinggiran sebagai pengamat atau observer (Council of Europe, 2023).

Posisi Indonesia yang belum meratifikasi Konvensi Budapest merupakan persoalan serius. Di satu sisi, Indonesia adalah salah satu pasar digital terbesar dengan tingkat kejahatan siber yang tinggi, menjadikannya sangat membutuhkan akses cepat terhadap bantuan hukum timbal balik. Di sisi lain, ketidakikutsertaan dalam rezim formal ini menempatkan aparat penegak hukum Indonesia pada posisi yang kurang menguntungkan ketika harus meminta data dari penyedia layanan global atau mengejar pelaku yang berlindung di negara pihak. Rumusan masalah dalam artikel ini adalah: pertama, bagaimana kerangka kerja sama internasional yang tersedia dalam penanggulangan cybercrime, khususnya di bawah Konvensi Budapest? Kedua, apa implikasi dari posisi Indonesia yang belum meratifikasi konvensi tersebut, dan langkah apa yang harus ditempuh? Tujuannya untuk memberikan argumentasi akademik tentang urgensi aksesi Indonesia ke dalam rezim kerja sama siber global, sekaligus menawarkan peta jalan persiapan yang diperlukan.

B. REZIM INTERNASIONAL DAN PRINSIP KERJA SAMA DALAM *CYBERCRIME*

Untuk memahami kerja sama internasional dalam penanggulangan *cybercrime*, perspektif teori rezim internasional yang dikemukakan oleh Stephen Krasner (1983) sangat relevan. Rezim internasional didefinisikan sebagai seperangkat prinsip, norma, aturan, dan prosedur pengambilan keputusan yang implisit maupun eksplisit, di mana ekspektasi para aktor bertemu dalam suatu isu tertentu. Konvensi Budapest adalah contoh konkret dari sebuah rezim internasional di bidang kejahatan siber. Ia tidak hanya menetapkan definisi bersama tentang apa yang dimaksud dengan akses ilegal, intersepsi ilegal, dan gangguan data, tetapi juga menyediakan prosedur baku tentang bagaimana negara-negara pihak harus bekerja sama dalam penyelidikan dan penuntutan.

Teori ini menjelaskan bahwa negara bersedia menyerahkan sebagian kecil kedaulatannya dan tunduk pada aturan bersama karena adanya keuntungan kolektif yang lebih besar, yaitu keamanan siber global. Tanpa rezim, setiap negara akan bertindak sendiri-sendiri, yang hasilnya tidak efisien dan penuh konflik yurisdiksi. Dalam konteks cybercrime, ketidakterlibatan dalam rezim justru merugikan karena negara tersebut tidak dapat menikmati fasilitas kerja sama cepat yang hanya tersedia bagi sesama anggota. Lebih jauh, prinsip *aut dedere aut judicare* (ekstradisi atau adili) yang sering muncul dalam konvensi kejahatan internasional juga

mulai bergema di ranah siber, meskipun penerapannya masih terbatas.

Di sisi lain, dalam ranah hukum pidana internasional, dikenal dua pendekatan yurisdiksi terhadap kejahatan transnasional: *territoriality principle* yang menjadi andalan utama, dan *universality principle* yang memungkinkan negara mengadili pelaku tanpa memandang lokasi kejadian untuk kejahatan tertentu. *Cybercrime* masih didominasi oleh pendekatan teritorialitas, sehingga kolaborasi lintas batas menjadi jembatan vital. *Mutual Legal Assistance* (MLA) adalah wujud paling operasional dari kolaborasi tersebut, yaitu mekanisme formal di mana satu negara meminta bantuan negara lain untuk mengumpulkan bukti, memeriksa saksi, atau membekukan aset demi kepentingan proses pidana. Efektivitas MLA sangat bergantung pada eksistensi landasan hukum, baik bilateral maupun multilateral, yang mendasarinya. Tanpa landasan itu, permohonan MLA bisa terkatung-katung dalam saluran diplomatik yang lambat, yang tentunya tidak cocok dengan kecepatan *cybercrime* (Brenner, 2022).

C. ARSITEKTUR KERJA SAMA DAN POSISI INDONESIA

1. Konvensi Budapest sebagai Pilar Utama Rezim *Cybercrime*

Konvensi Budapest, yang mulai berlaku pada 1 Juli 2004, adalah perjanjian internasional pertama

dan paling komprehensif yang secara khusus menargetkan kejahatan siber. Tiga pilar utamanya adalah: (1) harmonisasi hukum pidana nasional, di mana negara pihak harus mengkriminalisasi sembilan jenis perbuatan yang dikelompokkan ke dalam tindak pidana terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem, tindak pidana yang berkaitan dengan komputer, tindak pidana yang berkaitan dengan konten, dan tindak pidana terkait pelanggaran hak cipta; (2) penyediaan kewenangan hukum acara yang memadai bagi aparat penegak hukum untuk melakukan penggeledahan dan penyitaan data komputer, pengumpulan data real-time, dan intersepsi konten; serta (3) pembentukan mekanisme kerja sama internasional yang efektif, yang menekankan pada kecepatan. Pasal 35 secara spesifik mewajibkan setiap negara pihak untuk menunjuk *point of contact* yang tersedia 24 jam sehari, tujuh hari seminggu, untuk memberikan bantuan segera dalam investigasi.

Keberhasilan rezim ini terletak pada pragmatismenya. Ia tidak mendiktekan satu model hukum pidana yang seragam, melainkan menetapkan minimum baseline yang harus diadopsi, dengan memberikan fleksibilitas kepada negara untuk membuat reservasi pada ketentuan tertentu. Protokol Tambahan Pertama Konvensi Budapest yang diadopsi pada 2021 bahkan memperluas cakupannya ke ranah *cyber-enabled hate crime*,

menandakan bahwa rezim ini hidup dan terus beradaptasi. Bagi Indonesia, meratifikasi konvensi ini berarti menyelaraskan UU ITE dengan standar internasional, memperkuat kewenangan penyidik, dan yang terpenting, membuka pintu akses ke jaringan kerja sama eksklusif yang selama ini tertutup.

2. Mekanisme *Mutual Legal Assistance* dan 24/7 *Network*

Salah satu kelemahan paling akut dalam penanganan *cybercrime* di Indonesia adalah lambatnya proses MLA. Selama ini, permintaan data atau pembekuan aset kepada yurisdiksi asing dilakukan secara ad hoc, seringkali melalui jalur diplomatik atau Interpol. Prosesnya bisa memakan waktu berbulan-bulan, sementara data digital yang dicari mungkin sudah dihapus oleh penyedia layanan sesuai kebijakan retensi mereka. Konvensi Budapest menyediakan solusi melalui jaringan 24/7. Negara pihak dapat langsung menghubungi point of contact di negara lain untuk mengajukan preservasi data darurat (*emergency data preservation*), yang kemudian dapat ditindaklanjuti dengan MLA formal. Kecepatan ini adalah nyawa dari investigasi siber.

Indonesia, sebagai non-pihak, tidak memiliki hak untuk menggunakan saluran khusus ini. Ketika Polri meminta data dari penyedia layanan di Amerika Serikat, mereka harus melalui proses MLA

berdasarkan *Treaty on Mutual Legal Assistance in Criminal Matters bilateral*, yang tidak dirancang khusus untuk kecepatan era digital. Sementara itu, aparat dari negara pihak Konvensi Budapest dapat memperoleh data yang sama jauh lebih cepat karena adanya kerangka kerja sama yang lebih responsif. Inilah salah satu bentuk kerugian konkret akibat belum ratifikasi.

3. Kendala Kedaulatan dan Perlindungan Data Pribadi

Tantangan terbesar dalam kerja sama internasional selalu bersinggungan dengan isu kedaulatan dan perlindungan data. Negara seringkali enggan memberikan akses kepada penyidik asing terhadap data yang tersimpan di servernya karena dianggap melanggar kedaulatan hukum nasional. Munculnya *Cloud Act* di Amerika Serikat, yang memungkinkan penegak hukum AS mengakses data di server mana pun yang dimiliki perusahaan AS, memicu perdebatan tentang ekstrateritorialitas. Konvensi Budapest dan Protokol Tambahan Keduanya (2022) berupaya mengatasi ini dengan mengatur tentang akses langsung terhadap data yang tersimpan di luar negeri dengan persyaratan yang ketat, termasuk jaminan perlindungan HAM dan notifikasi kepada negara tempat data berada.

Indonesia memiliki kepentingan ganda di sini. Ia perlu melindungi kedaulatan datanya dari akses

asing yang sewenang-wenang, tetapi pada saat yang sama memerlukan kemampuan untuk mengakses data pelaku yang berada di luar negeri. Dengan berada di dalam rezim, Indonesia dapat ikut serta dalam merumuskan aturan main, memastikan bahwa standar perlindungan data pribadi dan hak asasi manusia dihormati dalam setiap permintaan bantuan. Di luar rezim, Indonesia hanya bisa menjadi penonton yang terpaksa menerima praktik negara lain tanpa kemampuan untuk memprotes secara efektif (Kusumawardhani, 2024).

D. KEGAGALAN KOLEKTIF DAN KEBUTUHAN KONVENSI

Peretasan oleh "Bjorka" dan Upaya Atribusi (2022-2023)

Aktor anonim yang dikenal dengan nama "Bjorka" pada tahun 2022 meretas sejumlah situs pemerintah Indonesia dan membocorkan data pejabat publik. Modus operandinya mencakup penggunaan *Tor network*, VPN luar negeri, dan penyimpanan data curian di paste sites internasional. Upaya atribusi untuk mengidentifikasi pelaku sangat sulit. Diduga kuat pelaku beroperasi dari luar negeri, namun tanpa kerja sama cepat dengan negara tempat server VPN berada, penyelidikan tidak bisa berlanjut. Permohonan informasi melalui MLA ke negara-negara tersebut berjalan lambat. Bjorka masih bebas hingga kini. Kasus ini adalah demonstrasi nyata dari kegagalan sistem: tanpa akses langsung dan kewajiban kerja

sama yang terstandarisasi, pelaku anonim dapat terus menari di atas puing-puing yurisdiksi nasional (ID-SIRTII, 2023).

Serangan *Ransomware WannaCry* dan Pembelajaran Global (2017)

Serangan *WannaCry* yang melumpuhkan ratusan ribu komputer di 150 negara pada tahun 2017, termasuk rumah sakit di Indonesia, adalah serangan siber global yang memerlukan respons kolektif. Investigasi internasional yang dipimpin oleh FBI, Europol, dan lembaga lainnya berhasil mengaitkan serangan tersebut dengan aktor di Korea Utara. Keberhasilan atribusi ini dimungkinkan oleh adanya kolaborasi intelijen dan teknis yang intens, yang difasilitasi oleh kerangka kerja sama internasional termasuk hubungan informal di luar Konvensi Budapest sekalipun. Namun, untuk negara seperti Indonesia yang hanya menjadi korban pasif, kapasitas untuk berkontribusi dalam investigasi dan memperoleh akses ke temuan global sangat terbatas. Peristiwa ini menunjukkan bahwa dalam ekosistem siber global, tidak ada satu negara pun yang dapat melindungi dirinya sendirian, dan partisipasi aktif dalam setiap forum adalah kunci untuk setidaknya mengetahui apa yang mengancam dirinya (Brenner, 2022).

Operasi Gabungan Internasional Melawan Jaringan Dark Web

Beberapa operasi penegakan hukum global, seperti *Operation DisrupTor* dan *Operation Dark HunTor*, berhasil menutup pasar gelap narkoba dan senjata di *dark web* serta menangkap ratusan tersangka di berbagai negara. Operasi ini adalah hasil kerja sama multi-yurisdiksi yang melibatkan Jerman, Belanda, Amerika Serikat, Australia, dan negara-negara Eropa lainnya, yang semuanya adalah pihak pada Konvensi Budapest. Indonesia, yang warganya mungkin menjadi pelaku atau korban di pasar tersebut, tidak terlibat aktif dalam operasi ini karena keterbatasan akses informasi dan ketiadaan kerangka kerja sama formal. Partisipasi dalam operasi semacam ini tidak hanya membantu penegakan hukum, tetapi juga memberikan pengalaman berharga bagi aparat dalam menangani kejahatan siber canggih. Ketidakhadiran Indonesia berarti hilangnya kesempatan belajar dan membangun kapasitas (Council of Europe, 2023).

E. PETA JALAN INDONESIA: DARI OBSERVER MENJADI PIHAK

Menyadari urgensi tersebut, sejumlah langkah strategis harus segera diambil. Pertama, ratifikasi Konvensi Budapest harus dimasukkan ke dalam prioritas legislatif nasional. Pemerintah bersama DPR perlu segera membahas dan menyetujui aksesi ini. Proses ini tidak hanya memerlukan pengesahan di tingkat parlemen, tetapi juga persiapan harmonisasi legislasi. UU ITE, UU PDP, KUHAP, dan RUU Keamanan dan Ketahanan Siber harus

diselaraskan dengan kewajiban yang akan diemban pasca-ratifikasi. Pemerintah perlu membentuk tim antar-kementerian yang khusus menangani persiapan ratifikasi ini, termasuk mengkaji kemungkinan reservasi terhadap pasal-pasal tertentu sesuai dengan kepentingan nasional dan konstitusi.

Kedua, Indonesia harus memanfaatkan masa transisi untuk meningkatkan kapasitas aparat penegak hukum. Pelatihan bahasa Inggris hukum, forensik digital, dan pemahaman tentang prosedur MLA internasional harus digencarkan. Tidak ada gunanya memiliki akses ke jaringan 24/7 jika tidak ada personel yang mampu mengoperasikannya. Ketiga, diplomasi siber harus ditingkatkan di forum bilateral, ASEAN, dan PBB. Indonesia dapat mempelopori pembentukan ASEAN *Cybercrime Cooperation Agreement* yang menjadi jembatan sebelum seluruh anggota ASEAN meratifikasi Budapest, sekaligus memperkuat posisi tawar kolektif kawasan.

Terakhir, keterlibatan aktif dalam diskursus internasional tentang kejahatan siber tidak boleh diabaikan. Perkembangan terbaru seperti negosiasi Konvensi PBB tentang Kejahatan Siber (yang sedang berlangsung di New York) adalah momentum bagi Indonesia untuk tidak hanya menjadi pengikut, tetapi juga pembentuk norma global. Dengan meratifikasi Budapest dan terlibat di PBB, Indonesia dapat memastikan bahwa tata kelola siber global tidak hanya dikendalikan oleh negara-negara maju,

tetapi juga merepresentasikan kepentingan negara berkembang.

F. KESIMPULAN

Kerja sama internasional dalam penanggulangan kejahatan siber merupakan pilar yang tidak tergantikan, dan Konvensi Budapest berdiri sebagai instrumen multilateral paling matang untuk mewujudkannya. Menjawab rumusan masalah pertama, kerangka kerja sama yang tersedia mencakup harmonisasi hukum pidana substantif dan prosedural, mekanisme *Mutual Legal Assistance* formal, dan jaringan 24/7 yang memungkinkan respons cepat. Menjawab rumusan kedua, posisi Indonesia sebagai observer merugikan secara operasional karena menghambat akses terhadap bukti digital yang berada di luar negeri, menghalangi partisipasi dalam operasi gabungan, dan melemahkan posisi tawar dalam isu kedaulatan data. Studi kasus menegaskan bahwa pelaku kejahatan siber kerap lolos karena celah-celah yurisdiksi yang hanya dapat ditutup melalui kerja sama internasional yang erat.

Sebagai rekomendasi, Indonesia harus segera meratifikasi Konvensi Budapest dengan persiapan yang matang, termasuk harmonisasi legislasi nasional, peningkatan kapasitas penegak hukum, dan pengembangan infrastruktur MLA elektronik. Selain itu, diplomasi siber perlu diperkuat di semua lini agar Indonesia tidak hanya menjadi konsumen

aturan global, tetapi juga arsiteknya. Di dunia yang semakin terhubung dan semakin rentan, tidak ada tempat bagi isolasi. Keamanan siber Indonesia adalah inseparabel dari keamanan siber global.

REFERENSI:

Brenner, S. W. (2022). Cybercrime: Criminal Threats from Cyberspace (2nd ed.). Praeger.

Council of Europe. (2023). Convention on Cybercrime (ETS No. 185): State of Signatures and Ratifications. https://www.coe.int/en/web/conventions/full-list

ID-SIRTII. (2023). Laporan Aktivitas Kejahatan Siber terhadap Pengguna Indonesia 2022. Indonesia Security Incident Response Team on Internet Infrastructure.

Krasner, S. D. (Ed.). (1983). International Regimes. Cornell University Press.

Kusumawardhani, A. (2024). Implikasi Non-Ratifikasi Konvensi Budapest terhadap Penegakan Hukum Siber di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Shearing, C., & Wood, J. (2003). Nodal Governance, Democracy, and the New 'Denizens'. Journal of Law and Society, 30(3), 400–419.

United Nations Office on Drugs and Crime. (2023). Cybercrime and International Cooperation. UNODC.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

World Economic Forum. (2024). Global Risks Report 2024. WEF.

Konvensi Budapest tentang Kejahatan Siber (Convention on Cybercrime), Budapest, 23 November 2001, ETS No. 185.