

ANALISIS YURIDIS TERHADAP KEJAHATAN SIBER (CYBER CRIME) LINTAS NEGARA DAN KETERBATASAN YURISDIKSI HUKUM PIDANA INTERNASIONAL DI INDONESIA

Bagas Prithajaya Putra¹, Wevy Efticha Sary²

^{1,2}Universitas Bengkulu

bagas.pritajaya2020@gmail.com¹, wesary@unib.ac.id²

ABSTRACT; *The development of information technology has led to the emergence of transnational cyber crime, creating challenges in law enforcement, particularly in terms of jurisdiction. This study aims to analyze the application of territorial, active nationality, passive nationality, and protective principles, as well as the limitations of Indonesia's international criminal jurisdiction. This research uses a normative juridical method. The results show that although these principles provide legal authority, their implementation faces obstacles such as cross-border digital evidence, extradition limitations, jurisdictional conflicts, and weak international cooperation. Therefore, strengthening international cooperation and legal harmonization is necessary to improve law enforcement effectiveness.*

Keywords: *Cyber Crime, Jurisdiction, Criminal Law.*

ABSTRAK; Perkembangan teknologi informasi telah melahirkan kejahatan siber (cyber crime) yang bersifat lintas negara dan menimbulkan tantangan dalam penegakan hukum, khususnya terkait yurisdiksi. Penelitian ini bertujuan menganalisis penerapan asas teritorial, nasional aktif, nasional pasif, dan protektif dalam menangani kejahatan siber lintas negara, serta mengkaji keterbatasan yurisdiksi hukum pidana internasional Indonesia. Metode yang digunakan adalah yuridis normatif. Hasil penelitian menunjukkan bahwa meskipun asas-asas tersebut memberikan dasar kewenangan, implementasinya masih terkendala pembuktian digital lintas negara, keterbatasan ekstradisi, konflik yurisdiksi, serta lemahnya kerja sama internasional. Oleh karena itu, diperlukan penguatan kerja sama internasional dan harmonisasi hukum guna meningkatkan efektivitas penegakan hukum.

Kata Kunci: Kejahatan Siber, Yurisdiksi, Hukum Pidana.

PENDAHULUAN

Berkembangnya ilmu pengetahuan, teknologi informasi dan komunikasi telah cukup memberikan dampak terhadap kejahatan yang memiliki kompleksitas tinggi dan bersifat lintas negara. Kejahatan siber atau *cyber crimes* kini tidak lagi hanya sebatas kejahatan yang berlaku di suatu negara tertentu, melainkan dapat terjadi dan melibatkan

negara lain sehingga hal ini dapat menimbulkan dampak hukum bagi negara-negara terkait secara simultan.¹

Berdasarkan konsep klasik terhadap yurisdiksi dalam hukum pidana, fenomena kejahatan siber ini bertentangan dengan prinsip-prinsip dasar hukum pidana yakni prinsip teritorial, prinsip nasionalitas, dan prinsip kedaulatan negara.² Secara kontekstual, kejahatan siber lintas negara membawakan persoalan kritis dalam penegakkan hukum, khususnya berkenaan dengan penentuan yurisdiksi terkait kewenangan untuk menyelidiki, menuntut, dan mengadili pelaku kejahatan.³

Negara Indonesia sebagai bagian daripada Masyarakat internasional yang tidak terbebas dari ancaman kejahatan siber lintas negara seperti penipuan daring, peretasan sistem elektronik, pencurian data pribadi, sampai dengan kejahatan-kejahatan siber yang terorganisir dan sistematis yang melibatkan pelaku dan korban dari berbagai negara.

Realitas empiris menunjukkan bahwa keterlibatan Warga Negara Indonesia (WNI) dalam jaringan *cyber crime* internasional semakin meningkat. Data dari Antara menyebutkan bahwa sejak tahun 2020 hingga 2025 terdapat sekitar 6.800 WNI yang terlibat dalam aktivitas penipuan daring (*online fraud/scam*) di luar negeri, terutama di kawasan Asia Tenggara seperti Kamboja, Myanmar, dan Filipina.⁴ Selain itu, Kepolisian Indonesia juga mengonfirmasi adanya 699 WNI yang menjadi korban perdagangan orang dan dipaksa bekerja dalam operasi *scam online* di Kamboja sepanjang tahun 2025.⁵ Fenomena ini menunjukkan bahwa *cyber crime* tidak hanya berkaitan dengan aspek kriminalitas digital, tetapi juga beririsan dengan tindak pidana perdagangan manusia, eksploitasi tenaga kerja, serta kejahatan transnasional terorganisir.

Meskipun secara instrumen hukum, Indonesia telah memiliki undang-undang informasi dan transaksi elektronik, undang-undang perlindungan data pribadi, dan yang terbaru kitab undang-undang hukum pidana nasional. Namun pengaturan tersebut masih membuka ruang bagi pelaku kejahatan siber yang berada di luar wilayah negara

¹ Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Jakarta: Kencana, 2013), 4.

² Eddy O.S. Hiarij, *Prinsip-Prinsip Hukum Pidana* (Yogyakarta: Cahaya Atma Pustaka, 2016), 115.

³ Sigid Suseno, "Yurisdiksi dalam Kejahatan Siber," *Jurnal Hukum Ius Quia Iustum* 17, no. 3 (2010): 345.

⁴ ANTARA News, "Kemlu catat 6.800 WN Indonesia terlibat kasus penipuan online," tanggal publikasi, diakses pada 10 April 2026, melalui <https://www.antaranews.com/>

⁵ Tempo.co, "699 WNI Jadi Korban Industri Scam di Kamboja," diakses pada 10 April 2026, melalui <https://www.tempo.co/hukum/699-wni-jadi-korban-industri-scam-di-kamboja-2108944>

Indonesia.⁶ Kondisi ini memperlihatkan adanya kesenjangan antara perkembangan modus kejahatan siber dan kemampuan hukum nasional dalam menegakkan hukum secara efektif.

Dalam perspektif teori hukum, kondisi tersebut memperlihatkan adanya kesenjangan nyata antara *das sein* (kenyataan yang terjadi) dan *das sollen* (ketentuan hukum yang seharusnya berlaku).⁷ Secara ideal, hukum pidana Indonesia seharusnya mampu memberikan perlindungan efektif kepada warga negara, menegakkan keadilan, serta menindak pelaku *cyber crime* lintas negara melalui mekanisme yurisdiksi internasional dan kerja sama antarnegara. Namun pada praktiknya, penegakan hukum terhadap *cyber crime* transnasional sering terkendala oleh keterbatasan yurisdiksi, perbedaan sistem hukum antarnegara, lemahnya mekanisme ekstradisi, serta sulitnya pembuktian digital lintas negara.

Hal ini berkaitan erat dengan tujuan hukum menurut Gustav Radbruch, yang menekankan bahwa hukum harus mengandung tiga nilai utama, yakni keadilan, kemanfaatan, dan kepastian hukum.⁸ Dalam konteks *cyber crime* lintas negara, nilai kepastian hukum menjadi problematik karena batas-batas yurisdiksi tidak selalu jelas. Ketika pelaku berada di luar negeri, hukum Indonesia sering mengalami hambatan untuk menjangkau dan menuntut secara efektif, sehingga kepastian hukum bagi korban maupun masyarakat menjadi kabur.

Dalam hukum pidana internasional, yurisdiksi negara terhadap tindak pidana lintas batas dikenal melalui beberapa asas, di antaranya asas nasionalitas (*nationality principle*) dan asas universal (*universal jurisdiction*). Asas nasionalitas memberikan kewenangan kepada negara untuk menuntut warganya yang melakukan tindak pidana di luar negeri. Namun penerapan asas ini dalam kasus *cyber crime* menghadapi tantangan besar, terutama dalam hal kerja sama internasional dan pengumpulan alat bukti digital. Sementara itu, asas universal memungkinkan negara menindak kejahatan tertentu yang dianggap mengancam komunitas internasional, meskipun *cyber crime* belum sepenuhnya diakui sebagai kejahatan universal seperti genosida atau perbudakan. Hal ini

⁶ Budi Suhariyanto, "Kebijakan Hukum dalam Penanggulangan Cyber Crime," *Jurnal Rechts Vinding* 2, no. 2 (2013): 201.

⁷ Satjipto Rahardjo, *Ilmu Hukum* (Bandung: Citra Aditya Bakti, 2006), 53.

⁸ Bernard L. Tanya et al., *Teori Hukum: Strategi Tertib Manusia Lintas Ruang dan Generasi* (Yogyakarta: Genta Publishing, 2010), 130.

memperlihatkan adanya kekosongan dan keterbatasan hukum internasional dalam merespons kejahatan digital global.

Kajian ini bertujuan untuk menganalisis secara yuridis penerapan yurisdiksi hukum pidana internasional Indonesia dalam menangani kejahatan siber (*cyber crime*) lintas negara, serta mengidentifikasi berbagai keterbatasan hukum dan tantangan penegakan hukum yang muncul akibat perbedaan yurisdiksi, kendala pembuktian digital, dan lemahnya kerja sama antarnegara. Selain itu, penelitian ini juga bertujuan mengkaji relevansi asas-asas yurisdiksi seperti asas nasionalitas dan asas universal dalam menghadapi fenomena *cyber crime* transnasional, termasuk kasus-kasus nyata yang melibatkan WNI sebagai pelaku maupun korban online scam di Kamboja dan Myanmar. Pada akhirnya, Kajian ini diharapkan dapat merumuskan rekomendasi yuridis guna memperkuat kepastian hukum, perlindungan warga negara, dan efektivitas sistem hukum pidana Indonesia dalam merespons perkembangan kejahatan siber lintas batas.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (yuridis normatif) yang berfokus pada analisis terhadap norma hukum positif serta prinsip-prinsip hukum pidana internasional dalam menangani kejahatan siber (*cyber crime*) lintas negara. Penelitian hukum normatif dilakukan dengan cara menelaah bahan pustaka atau data sekunder sebagai sumber utama dalam mengkaji permasalahan hukum yang diteliti.⁹

Pendekatan yang digunakan dalam penelitian ini meliputi beberapa pendekatan, yaitu:

1. Pendekatan perundang-undangan (*statute approach*), yang dilakukan dengan menelaah berbagai peraturan perundang-undangan yang relevan, baik dalam hukum nasional seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana, maupun instrumen hukum internasional yang berkaitan dengan kejahatan siber;
2. Pendekatan konseptual (*conceptual approach*), yang digunakan untuk memahami dan menganalisis konsep-konsep hukum seperti *cyber crime*, yurisdiksi

⁹ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: RajaGrafindo Persada, 2001), hlm. 13.

ekstrateritorial, serta kejahatan terorganisir lintas negara (*transnational organized crime*);

3. Pendekatan kasus (*case approach*), yang dilakukan dengan menelaah kasus-kasus empiris terkait praktik kejahatan siber lintas negara, khususnya fenomena scam online di kawasan Asia Tenggara yang melibatkan Warga Negara Indonesia sebagai pelaku maupun korban.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas:

1. Bahan hukum primer, yaitu peraturan perundang-undangan dan instrumen hukum internasional yang relevan;
2. Bahan hukum sekunder, berupa buku, jurnal ilmiah, serta laporan organisasi internasional;
3. Bahan hukum tersier, berupa kamus hukum dan ensiklopedia yang mendukung penjelasan konsep.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan cara menelusuri dan mengkaji berbagai sumber hukum secara sistematis. Selanjutnya, bahan hukum yang telah dikumpulkan dianalisis menggunakan metode kualitatif dengan pendekatan deskriptif-analitis dan preskriptif, yaitu dengan menggambarkan permasalahan hukum yang ada, kemudian memberikan argumentasi hukum sebagai solusi terhadap keterbatasan yurisdiksi dalam penegakan hukum kejahatan siber lintas negara.¹⁰

HASIL DAN PEMBAHASAN

A. Peranan Asas Teritorial, Asas Nasional Aktif, Asas Nasional Pasif, Dan Asas Protektif Dalam Penegakan Hukum Terhadap Kejahatan Siber Lintas Negara Yang Berdampak Pada Kepentingan Hukum Indonesia

Perkembangan pesat ilmu pengetahuan, teknologi informasi, serta komunikasi digital telah membawa perubahan fundamental dalam pola interaksi sosial, ekonomi, dan politik masyarakat global. Namun, di sisi lain, kemajuan tersebut juga menciptakan ruang baru bagi berkembangnya bentuk-bentuk kejahatan modern yang semakin kompleks,

¹⁰ Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2017), hlm. 35.

terorganisir, dan melintasi batas-batas negara.¹¹ Kejahatan siber (cyber crime) kini menjadi salah satu fenomena kriminalitas kontemporer yang paling menantang karena karakteristiknya yang bersifat tanpa batas (borderless), anonim, serta melibatkan penggunaan infrastruktur digital global.

Berbeda dengan kejahatan konvensional yang dapat dengan relatif mudah ditentukan tempat kejadian perkaranya, cyber crime sering kali tidak dapat dipetakan secara jelas dalam kerangka geografis negara. Pelaku dapat melakukan tindak pidana dari luar negeri, menggunakan server di negara ketiga, sementara korban berada di negara lain. Kompleksitas ini menjadikan cyber crime sebagai bentuk kejahatan lintas negara (transnational crime) yang secara simultan menimbulkan dampak hukum bagi beberapa negara sekaligus.

Dalam perspektif hukum pidana klasik, yurisdiksi negara dibangun berdasarkan prinsip dasar seperti asas teritorial, asas nasionalitas, dan asas kedaulatan negara. Namun, fenomena cyber crime lintas negara memperlihatkan adanya pertentangan konseptual dengan prinsip-prinsip tersebut. Cyber crime tidak mengenal batas teritorial secara fisik, sehingga menimbulkan persoalan kritis dalam penegakan hukum, khususnya terkait penentuan yurisdiksi: negara mana yang berwenang melakukan penyelidikan, penuntutan, serta mengadili pelaku tindak pidana.

Indonesia sebagai bagian dari masyarakat internasional tidak terbebas dari ancaman cyber crime transnasional. Berbagai bentuk kejahatan digital seperti penipuan daring (online fraud), peretasan sistem elektronik, pencurian data pribadi, serangan ransomware, hingga operasi cyber crime terorganisir semakin sering terjadi dan berdampak langsung terhadap kepentingan hukum nasional Indonesia.

Realitas empiris menunjukkan bahwa keterlibatan Warga Negara Indonesia (WNI) dalam jaringan cyber crime internasional juga mengalami peningkatan signifikan. Data yang dilansir Antara menyebutkan bahwa sejak tahun 2020 hingga 2025 terdapat sekitar 6.800 WNI yang terlibat dalam aktivitas penipuan daring di luar negeri, terutama di kawasan Asia Tenggara seperti Kamboja, Myanmar, dan Filipina. Selain itu, Kepolisian Republik Indonesia juga mengonfirmasi adanya 699 WNI yang menjadi korban

¹¹ S. J. Lesmana, I. Sofia, dan F. Felina, "Law Enforcement in Efforts to Combat Cyber Crime in Indonesia," *International Journal of Law Review* 1, no. 3 (2023): 120.

perdagangan orang dan dipaksa bekerja dalam operasi scam online di Kamboja sepanjang tahun 2025. Fakta ini menegaskan bahwa cyber crime bukan hanya berkaitan dengan aspek kriminalitas digital semata, tetapi juga beririsan dengan tindak pidana perdagangan manusia, eksploitasi tenaga kerja, serta kejahatan transnasional terorganisir.

Meskipun Indonesia telah memiliki instrumen hukum nasional seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta KUHP Nasional terbaru, pengaturan tersebut masih menghadapi keterbatasan ketika pelaku kejahatan berada di luar wilayah negara Indonesia. Hal ini mencerminkan adanya kesenjangan nyata antara perkembangan modus cyber crime yang semakin global dengan kemampuan hukum nasional dalam menegakkan hukum secara efektif.

Dalam perspektif teori hukum, kondisi tersebut memperlihatkan adanya gap antara *das sein* (kenyataan empiris yang terjadi) dan *das sollen* (ketentuan hukum ideal yang seharusnya berlaku). Secara ideal, hukum pidana Indonesia seharusnya mampu memberikan perlindungan efektif kepada warga negara, menegakkan keadilan, serta menjamin kepastian hukum dalam menghadapi ancaman cyber crime lintas batas. Namun pada praktiknya, penegakan hukum sering terkendala oleh keterbatasan yurisdiksi, perbedaan sistem hukum antarnegara, lemahnya mekanisme ekstradisi, serta kesulitan pembuktian digital lintas negara.

Problem tersebut berkaitan erat dengan tujuan hukum menurut Gustav Radbruch, yang menekankan bahwa hukum harus mengandung tiga nilai utama, yakni keadilan, kemanfaatan, dan kepastian hukum. Dalam konteks cyber crime transnasional, nilai kepastian hukum menjadi problematik karena batas yurisdiksi negara sering kali tidak jelas. Ketika pelaku berada di luar negeri, hukum Indonesia sering mengalami hambatan untuk menjangkau dan menuntut secara efektif, sehingga perlindungan hukum bagi korban maupun masyarakat menjadi kabur.

Dalam hukum pidana internasional, yurisdiksi negara terhadap tindak pidana lintas batas dikenal melalui beberapa asas yurisdiksi, di antaranya asas teritorial, asas nasional aktif, asas nasional pasif, dan asas protektif. Keempat asas ini memiliki peranan strategis dalam menentukan ruang lingkup kewenangan Indonesia dalam menegakkan hukum terhadap cyber crime lintas negara yang berdampak pada kepentingan hukum nasional.

1. Asas Teritorial sebagai Pilar Utama Yurisdiksi dalam Cyber Crime

Asas teritorial merupakan prinsip dasar yang menyatakan bahwa suatu negara berwenang menegakkan hukum pidana terhadap tindak pidana yang terjadi di wilayah kedaulatannya. Dalam sistem hukum pidana Indonesia, asas ini tercermin dalam Pasal 2 KUHP yang menegaskan bahwa hukum pidana Indonesia berlaku bagi setiap orang yang melakukan tindak pidana di wilayah Indonesia.

Namun, penerapan asas teritorial dalam konteks cyber crime lintas negara menghadapi kompleksitas karena kejahatan digital sering kali tidak dapat ditentukan locus delicti-nya secara konvensional. Kejahatan dapat dilakukan dari luar negeri, tetapi menyerang sistem elektronik di Indonesia atau menimbulkan akibat hukum di Indonesia. Oleh karena itu, asas teritorial dalam cyber crime perlu dipahami dalam arti luas, mencakup:

1. tempat sistem elektronik yang diserang berada,
2. tempat kerugian atau akibat hukum muncul,
3. tempat korban mengalami dampak.

Sebagai contoh, apabila seorang pelaku di luar negeri melakukan peretasan terhadap server bank nasional Indonesia atau mencuri data pribadi warga negara Indonesia melalui platform digital, maka Indonesia tetap dapat mengklaim yurisdiksi berdasarkan asas teritorial karena akibat tindak pidana terjadi dalam wilayah hukum Indonesia. Dengan demikian, asas teritorial tetap relevan, tetapi memerlukan reinterpretasi modern melalui konsep objective territoriality.

2. Asas Nasional Aktif dalam Menjangkau WNI sebagai Pelaku Cyber Crime

Asas nasional aktif (active nationality principle) memberikan kewenangan kepada negara untuk menuntut warga negaranya yang melakukan tindak pidana di luar wilayah negara tersebut.¹² Dalam konteks cyber crime transnasional, asas ini menjadi sangat penting mengingat meningkatnya keterlibatan WNI dalam jaringan scam internasional di Kamboja, Myanmar, dan Filipina.

Melalui asas nasional aktif, Indonesia memiliki dasar yuridis untuk menuntut WNI yang menjadi pelaku cyber crime di luar negeri. Hal ini penting untuk

¹² Yoga Dwi Cahya Sejati dan Muhammad Awal Satrio Nugroho, "Upaya Peningkatan Kompetensi Penyidik Cyber Crime," *Jurnal Riset Manajemen Akuntansi Indonesia* 1, no. 2 (2023): 380.

mencegah terbentuknya ruang impunitas (safe haven) bagi pelaku yang memanfaatkan perbedaan yurisdiksi negara. Asas ini juga mencerminkan kewajiban negara untuk memastikan bahwa warganya tidak menjadi bagian dari kejahatan transnasional yang merugikan masyarakat internasional.

Namun, efektivitas penerapan asas nasional aktif sangat bergantung pada kerja sama internasional, khususnya dalam hal ekstradisi pelaku serta bantuan hukum timbal balik (mutual legal assistance) untuk memperoleh alat bukti digital.

3. Asas Nasional Pasif sebagai Mekanisme Perlindungan Korban WNI

Asas nasional pasif (passive nationality principle) memberikan kewenangan kepada negara untuk menegakkan hukum pidananya apabila korban tindak pidana adalah warga negara negara tersebut, meskipun perbuatan dilakukan di luar negeri.¹³

Dalam cyber crime lintas negara, asas ini relevan karena korban kejahatan digital sering kali merupakan warga negara Indonesia yang menjadi target phishing, pencurian identitas, atau penipuan daring oleh pelaku asing. Dengan asas nasional pasif, Indonesia dapat mengklaim yurisdiksi demi melindungi warga negaranya.

Namun, penerapan asas ini menghadapi tantangan berupa konflik yurisdiksi dengan negara tempat pelaku berada. Oleh sebab itu, asas nasional pasif menuntut adanya koordinasi internasional yang kuat agar perlindungan korban tidak berhenti pada batas negara.

4. Asas Protektif dalam Menjaga Kepentingan Vital Negara

Asas protektif (protective principle) memberikan kewenangan kepada negara untuk menindak tindak pidana yang dilakukan di luar wilayahnya apabila perbuatan tersebut mengancam kepentingan fundamental negara, seperti keamanan nasional, stabilitas ekonomi, atau kedaulatan negara.¹⁴

Dalam konteks cyber crime modern, asas protektif menjadi semakin penting karena serangan siber sering kali menargetkan infrastruktur strategis negara, termasuk sistem pemerintahan, lembaga keuangan, dan jaringan telekomunikasi.

¹³ Rika Ratna Permata, "Perlindungan Hukum terhadap Korban Kejahatan Siber," *Jurnal Ilmu Hukum* 15, no. 1 (2022): 98.

¹⁴ Dewa Gede Sudika Mangku, "Kebijakan Hukum Pidana dalam Menanggulangi Cyber Crime," *Jurnal Komunikasi Hukum* 8, no. 2 (2022): 214.

Serangan terhadap data pemerintah atau sistem pertahanan dapat dikualifikasikan sebagai ancaman terhadap kepentingan nasional Indonesia.

Asas ini menunjukkan bahwa cyber crime tidak hanya merupakan kejahatan individu, tetapi juga dapat berkembang menjadi ancaman terhadap keamanan nasional dan stabilitas negara.

5. Signifikansi Keempat Asas dalam Menutup Kesenjangan Penegakan Hukum Siber Indonesia

Keempat asas yurisdiksi tersebut membentuk kerangka penting dalam memperluas jangkauan hukum pidana Indonesia terhadap cyber crime lintas negara. Asas teritorial memberikan dasar utama, asas nasional aktif menjangkau WNI pelaku di luar negeri, asas nasional pasif melindungi WNI korban, dan asas protektif menjaga kepentingan strategis negara.

Namun demikian, tantangan penegakan hukum tetap besar karena keterbatasan yurisdiksi, lemahnya ekstradisi, kesulitan pembuktian digital lintas negara, serta perbedaan sistem hukum antarnegara. Kondisi ini menyebabkan nilai kepastian hukum sebagaimana ditegaskan Radbruch menjadi problematik dalam konteks cyber crime transnasional.

Oleh karena itu, penguatan penegakan hukum cyber crime lintas negara tidak hanya membutuhkan instrumen hukum nasional, tetapi juga harmonisasi hukum internasional, penguatan kerja sama regional dan global, serta reformasi mekanisme yurisdiksi pidana agar mampu menjawab perkembangan kejahatan digital yang semakin kompleks.

B. Keterbatasan Yurisdiksi Hukum Pidana Internasional Indonesia Dalam Menangani Kejahatan Siber Lintas Negara Dan Posisi Indonesia Di Luar *Budapest Convention On Cybercrime*

Kejahatan siber lintas negara merupakan manifestasi nyata dari perubahan lanskap kriminalitas global yang dipicu oleh kemajuan teknologi informasi dan komunikasi. Perkembangan ruang digital yang semakin terintegrasi secara internasional telah melahirkan bentuk-bentuk kejahatan baru yang tidak lagi terikat pada batas-batas geografis tradisional. Cyber crime, dalam konteks ini, tidak hanya sekadar menjadi persoalan kriminalitas berbasis teknologi, melainkan telah berkembang menjadi

fenomena transnasional yang kompleks, sistematis, serta melibatkan jaringan lintas yurisdiksi negara.

Karakteristik utama cyber crime yang bersifat borderless, anonim, serta bergantung pada infrastruktur digital global menjadikannya sebagai salah satu bentuk tindak pidana yang paling menantang dalam penegakan hukum pidana modern.¹⁵ Kejahatan ini memungkinkan pelaku beroperasi dari suatu negara, memanfaatkan server di negara lain, serta menimbulkan dampak hukum terhadap korban yang berada di yurisdiksi berbeda. Konsekuensinya, cyber crime lintas negara secara simultan menimbulkan persoalan hukum yang tidak dapat diselesaikan hanya melalui pendekatan hukum pidana nasional yang bersifat teritorial.¹⁶

Indonesia sebagai bagian dari komunitas internasional tidak terlepas dari ancaman cyber crime transnasional. Penipuan daring, pencurian identitas digital, peretasan sistem elektronik, hingga operasi scam online terorganisir yang melibatkan WNI sebagai pelaku maupun korban menunjukkan bahwa cyber crime telah menjadi ancaman multidimensional. Bahkan, kasus-kasus nyata seperti keterlibatan ribuan WNI dalam jaringan scam internasional di kawasan Asia Tenggara memperlihatkan bahwa cyber crime tidak berdiri sendiri, melainkan beririsan erat dengan tindak pidana perdagangan orang, eksploitasi tenaga kerja, serta kejahatan terorganisir lintas negara.

Meskipun Indonesia telah memiliki perangkat hukum nasional seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta KUHP Nasional terbaru, penegakan hukum terhadap cyber crime lintas batas masih menghadapi keterbatasan yurisdiksi pidana internasional yang substansial. Hambatan tersebut terutama berkaitan dengan lemahnya mekanisme kerja sama internasional, kesulitan pembuktian digital lintas negara, serta posisi Indonesia yang hingga kini belum menjadi pihak dalam *Budapest Convention on Cybercrime*, yang secara luas dipandang sebagai rezim internasional utama dalam penanggulangan kejahatan siber global.

¹⁵ Khoirunnisa dan Jubaidi, "Indonesia's Digital Security Strategy: Countering Cybercrime," *Politeia Journal* 2, no. 2 (2024): 62.

¹⁶ Adinda Lola Sariani Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia," *Al-Dalil* (2024): 70.

Dengan demikian, keterbatasan yurisdiksi Indonesia dalam menangani cyber crime transnasional tidak hanya bersifat normatif, tetapi juga mencerminkan persoalan struktural dan institusional dalam hubungan antarnegara di era digital.

1. Problem Yurisdiksi Ekstrateritorial Ketegangan antara Kedaulatan Negara dan Realitas Kejahatan Digital Tanpa Batas

Salah satu keterbatasan mendasar dalam penegakan hukum cyber crime lintas negara adalah problem yurisdiksi ekstrateritorial. Secara konseptual, hukum pidana internasional mengenal beberapa asas yurisdiksi seperti asas nasional aktif, nasional pasif, maupun asas protektif yang memungkinkan negara memperluas kewenangannya terhadap tindak pidana di luar wilayah teritorialnya.

Namun, dalam praktiknya, penerapan yurisdiksi ekstrateritorial tersebut sering kali terbentur pada prinsip kedaulatan negara yang tetap menjadi fondasi utama dalam sistem internasional.¹⁷ Indonesia, misalnya, tidak dapat secara unilateral melakukan tindakan penegakan hukum koersif seperti penangkapan, penggeledahan, ataupun penyitaan terhadap pelaku dan alat bukti yang berada di wilayah negara lain tanpa adanya persetujuan atau kerja sama resmi dari negara terkait.

Hal ini menciptakan keterbatasan faktual dalam penegakan hukum, sebab yurisdiksi ekstrateritorial yang secara teoritis dimungkinkan sering kali tidak dapat diwujudkan secara efektif di lapangan. Dalam kasus scam online yang melibatkan WNI di Kamboja atau Myanmar, misalnya, Indonesia dapat mengklaim kewenangan berdasarkan asas nasional aktif, tetapi tetap tidak dapat memproses pelaku apabila negara tempat pelaku berada tidak memberikan dukungan hukum atau kerja sama yang memadai.

Dengan kata lain, cyber crime menegaskan paradoks besar dalam hukum pidana internasional: kejahatan berkembang melampaui batas negara, sementara penegakan hukum masih terikat pada batas-batas kedaulatan teritorial.¹⁸

2. Kompleksitas Pembuktian Digital Lintas Negara Tantangan *Mutual Legal Assistance* dan Kerentanan *Digital Evidence*

¹⁷ Manayra Aisha Putri Indradjaja et al., "Implementasi Penyidikan Siber," (2024): 165.

¹⁸ Rafi Septia Budianto Pansariadi dan Noenik Soekorini, "Tindak Pidana Cyber Crime," (2023): 290.

Kendala lain yang sangat krusial adalah kesulitan dalam memperoleh, mengamankan, serta memverifikasi alat bukti elektronik lintas negara. Cyber crime pada hakikatnya merupakan kejahatan yang meninggalkan jejak digital, seperti log aktivitas server, metadata komunikasi, transaksi elektronik, alamat IP, hingga rekaman digital lainnya.

Namun, alat bukti tersebut sering kali berada di luar yurisdiksi Indonesia, tersimpan pada perusahaan penyedia layanan digital global, atau terletak pada server yang berlokasi di negara lain. Dalam situasi demikian, aparat penegak hukum Indonesia tidak memiliki kewenangan langsung untuk mengakses atau menyita bukti tersebut tanpa melalui mekanisme bantuan hukum timbal balik (mutual legal assistance).

Permasalahan utama dari MLA adalah sifatnya yang prosedural, birokratis, dan cenderung memakan waktu lama. Padahal, bukti digital memiliki karakteristik yang sangat rentan: mudah dihapus, dimodifikasi, atau dipindahkan dalam hitungan detik.¹⁹ Akibatnya, proses permintaan bantuan hukum yang lambat sering kali tidak sejalan dengan kebutuhan investigasi cyber crime yang menuntut respons cepat dan presisi tinggi.

Kondisi ini memperlihatkan bahwa keterbatasan yurisdiksi Indonesia tidak hanya terkait aspek normatif, tetapi juga terkait kemampuan institusional dalam mengamankan bukti digital lintas negara secara efektif.

3. Hambatan Ekstradisi dan Ruang Impunitas bagi Pelaku Cyber Crime

Dalam banyak kasus cyber crime lintas negara, pelaku berada di luar wilayah Indonesia. Oleh karena itu, mekanisme ekstradisi menjadi instrumen penting agar pelaku dapat dibawa ke yurisdiksi Indonesia untuk diproses secara pidana.

Namun, sistem ekstradisi Indonesia masih menghadapi sejumlah keterbatasan, antara lain:

- 1) tidak adanya perjanjian ekstradisi dengan seluruh negara,
- 2) cyber crime belum selalu diprioritaskan sebagai extraditable offence,

¹⁹ Siti Aliza Nuraini Wahdini dan Fiqri Fitrah Banu Irfansyah, "Analisis Yurisdiksi Cyber Crime," (2024): 8.

3) prinsip double criminality yang mensyaratkan kesamaan delik di kedua negara,

4) pertimbangan politik dan diplomatik dalam penyerahan pelaku.

Dalam konteks kasus scam WNI di Kamboja, misalnya, negara tempat tindak pidana dilakukan dapat memilih untuk mengadili pelaku sendiri atau bahkan tidak menindaklanjuti proses hukum secara maksimal. Hal ini menciptakan ruang impunitas, yakni kondisi di mana pelaku dapat lolos dari jerat hukum karena celah yurisdiksi antarnegara.

4. Konflik Yurisdiksi dan Minimnya Harmonisasi Regulasi Cyber Crime Global

Cyber crime lintas negara hampir selalu melibatkan tumpang tindih yurisdiksi. Negara pelaku, negara korban, negara tempat server berada, hingga negara tempat akibat dirasakan dapat secara bersamaan mengklaim kewenangan hukum.

Namun, koordinasi antarnegara sering kali sulit dilakukan karena perbedaan sistem hukum, perbedaan definisi cyber crime, serta variasi standar prosedural dalam pembuktian elektronik. Tidak semua negara memiliki regulasi yang sama mengenai phishing, hacking, atau scam online. Bahkan, beberapa yurisdiksi mungkin masih belum memiliki instrumen cyber law yang memadai.

Dengan demikian, cyber crime menegaskan urgensi harmonisasi hukum internasional. Namun, hingga kini, harmonisasi tersebut masih bersifat parsial dan belum mampu menjawab sepenuhnya tantangan kriminalitas digital global.

5. Posisi Indonesia di Luar Budapest Convention: Konsekuensi terhadap Kerja Sama Penegakan Hukum Global

Salah satu faktor yang memperkuat keterbatasan yurisdiksi Indonesia adalah kenyataan bahwa Indonesia belum menjadi pihak dalam Budapest Convention on Cybercrime. Konvensi ini merupakan instrumen internasional utama yang menyediakan kerangka kerja komprehensif dalam penanggulangan cyber crime, termasuk harmonisasi tindak pidana siber, prosedur pembuktian digital, serta mekanisme kerja sama internasional cepat melalui jaringan kontak 24/7.²⁰

²⁰ Khoirunnisa dan Jubaidi, "Digital Security Strategy," (2024): 70.

Ketidakterlibatan Indonesia dalam konvensi ini memiliki beberapa konsekuensi strategis. Pertama, Indonesia tidak memiliki akses penuh terhadap mekanisme kerja sama cepat yang dimiliki negara-negara anggota, sehingga permintaan bantuan bukti digital harus dilakukan melalui jalur bilateral yang lebih lambat dan terbatas. Kedua, absennya Indonesia dari Budapest Convention menyebabkan kesenjangan standar hukum dengan negara-negara anggota, sehingga koordinasi penegakan hukum cyber crime menjadi kurang efektif. Ketiga, dalam konteks diplomasi hukum internasional, posisi Indonesia menjadi relatif lebih lemah karena berada di luar rezim utama cyber crime enforcement global.

6. Dimensi Politik dan Kedaulatan Digital dalam Keputusan Indonesia

Perlu dipahami bahwa ketidakikutsertaan Indonesia dalam Budapest Convention tidak semata-mata disebabkan oleh faktor teknis, melainkan juga berkaitan dengan dimensi politik internasional dan isu kedaulatan digital.

Sebagian negara berkembang memandang Budapest Convention sebagai instrumen yang disusun dengan dominasi negara-negara Eropa tanpa partisipasi luas negara Global South. Kekhawatiran utama meliputi potensi akses lintas negara terhadap data domestik yang dapat mengganggu kedaulatan informasi, serta ketidakseimbangan dalam mekanisme cross-border data sharing.

Oleh karena itu, Indonesia cenderung mendukung inisiatif alternatif melalui PBB, seperti perumusan UN Cybercrime Treaty, yang dianggap lebih inklusif dan representatif bagi kepentingan negara berkembang.

7. Implikasi terhadap Kepastian Hukum dan Perlindungan Warga Negara Indonesia

Keterbatasan yurisdiksi pidana internasional tersebut berdampak langsung terhadap kepastian hukum bagi masyarakat Indonesia. Ketika pelaku berada di luar negeri dan sulit dijangkau, korban kehilangan akses terhadap keadilan, sementara negara mengalami kesulitan memberikan perlindungan optimal.

Dalam perspektif Gustav Radbruch, nilai kepastian hukum menjadi problematik karena hukum nasional tidak sepenuhnya mampu menjangkau realitas cyber crime transnasional. Hal ini menegaskan perlunya reformasi kebijakan hukum pidana internasional Indonesia agar lebih adaptif, responsif, serta mampu menjawab perkembangan kejahatan digital global.

8. Urgensi Reformasi Kerja Sama Internasional dan Penguatan Yurisdiksi Indonesia

Menghadapi keterbatasan tersebut, Indonesia perlu mengembangkan strategi komprehensif melalui:

- 1) penguatan MLA dan ekstradisi regional di ASEAN,
- 2) pembentukan mekanisme cepat pertukaran bukti elektronik,
- 3) harmonisasi regulasi cyber crime lintas negara,
- 4) mempertimbangkan akses Budapest Convention atau setidaknya mengadopsi standar substansinya,
- 5) memperkuat posisi Indonesia dalam UN Cybercrime Treaty.

Dengan demikian, penegakan hukum cyber crime lintas negara dapat berjalan lebih efektif, memberikan kepastian hukum, serta menjamin perlindungan nyata bagi kepentingan nasional Indonesia.

Secara keseluruhan, keterbatasan yurisdiksi hukum pidana internasional Indonesia dalam menangani cyber crime lintas negara terutama terletak pada kesulitan pembuktian digital lintas batas, lemahnya mekanisme ekstradisi, konflik yurisdiksi antarnegara, serta posisi Indonesia yang belum menjadi pihak dalam Budapest Convention. Kondisi ini memperlihatkan adanya kesenjangan antara perkembangan modus kejahatan siber yang semakin global dengan kemampuan penegakan hukum nasional, sehingga reformasi kerja sama internasional menjadi kebutuhan mendesak demi menjamin keadilan, kemanfaatan, dan kepastian hukum.

KESIMPULAN DAN SARAN

Berdasarkan pembahasan yang telah diuraikan, dapat disimpulkan bahwa penegakan hukum terhadap kejahatan siber lintas negara menuntut penerapan asas-asas yurisdiksi dalam hukum pidana internasional, yaitu asas teritorial, asas nasional aktif, asas nasional pasif, dan asas protektif. Keempat asas tersebut memberikan dasar kewenangan bagi Indonesia untuk menindak kejahatan siber yang melibatkan pelaku, korban, maupun dampak hukum yang berkaitan dengan kepentingan nasional. Namun demikian, penerapan asas-asas tersebut dalam praktik masih menghadapi berbagai keterbatasan, seperti kesulitan pembuktian digital lintas negara, keterbatasan mekanisme ekstradisi, perbedaan sistem hukum antarnegara, serta terbatasnya akses kerja sama

internasional karena Indonesia belum menjadi pihak dalam rezim global seperti Budapest Convention on Cybercrime.

Oleh karena itu, diperlukan penguatan kerangka kerja sama internasional, optimalisasi mekanisme bantuan hukum timbal balik dan ekstradisi, serta harmonisasi regulasi nasional yang lebih adaptif terhadap perkembangan kejahatan siber. Selain itu, pemerintah perlu mempertimbangkan secara strategis keterlibatan Indonesia dalam instrumen hukum internasional terkait cyber crime serta meningkatkan kapasitas aparat penegak hukum dalam bidang investigasi dan forensik digital, sehingga penegakan hukum terhadap kejahatan siber lintas negara dapat berjalan lebih efektif dan mampu memberikan kepastian hukum serta perlindungan yang optimal bagi kepentingan hukum Indonesia.

DAFTAR PUSTAKA

- Peter Mahmud Marzuki. Penelitian Hukum. Jakarta: Kencana, 2017.
- Soerjono Soekanto dan Sri Mamudji. Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: RajaGrafindo Persada, 2001.
- Adinda Lola Sariani Dinda, “Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia,” *Al-Dalil* (2024): 70.
- Bernard L. Tanya et al., *Teori Hukum: Strategi Tertib Manusia Lintas Ruang dan Generasi* (Yogyakarta: Genta Publishing, 2010), 130.
- Budi Suhariyanto, “Kebijakan Hukum dalam Penanggulangan Cyber Crime,” *Jurnal Rechts Vinding* 2, no. 2 (2013): 201.
- Dewa Gede Sudika Mangku, “Kebijakan Hukum Pidana dalam Menanggulangi Cyber Crime,” *Jurnal Komunikasi Hukum* 8, no. 2 (2022): 214.
- Eddy O.S. Hiariej, *Prinsip-Prinsip Hukum Pidana* (Yogyakarta: Cahaya Atma Pustaka, 2016), 115.
- Khoirunnisa dan Jubaidi, “Digital Security Strategy,” (2024):
- Khoirunnisa dan Jubaidi, “Indonesia’s Digital Security Strategy: Countering Cybercrime,” *Politeia Journal* 2, no. 2 (2024): 62.
- Manayra Aisha Putri Indradjaja et al., “Implementasi Penyidikan Siber,” (2024): 165.
- Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Jakarta: Kencana, 2013), 4.

- Rafi Septia Budianto Pansariadi dan Noenik Soekorini, “Tindak Pidana Cyber Crime,” (2023): 290.
- Rika Ratna Permata, “Perlindungan Hukum terhadap Korban Kejahatan Siber,” *Jurnal Ilmu Hukum* 15, no. 1 (2022): 98.
- S. J. Lesmana, I. Sofia, dan F. Felina, “Law Enforcement in Efforts to Combat Cyber Crime in Indonesia,” *International Journal of Law Review* 1, no. 3 (2023): 120.
- Satjipto Rahardjo, *Ilmu Hukum* (Bandung: Citra Aditya Bakti, 2006), 53.
- Sigid Suseno, “Yurisdiksi dalam Kejahatan Siber,” *Jurnal Hukum Ius Quia Iustum* 17, no. 3 (2010): 345.
- Siti Aliza Nuraini Wahdini dan Fiqri Fitrah Banu Irfansyah, “Analisis Yurisdiksi Cyber Crime,” (2024): 8.
- Yoga Dwi Cahya Sejati dan Muhammad Awal Satrio Nugroho, “Upaya Peningkatan Kompetensi Penyidik Cyber Crime,” *Jurnal Riset Manajemen Akuntansi Indonesia* 1, no. 2 (2023): 380.
- ANTARA News. “Kemlu catat 6.800 WN Indonesia terlibat kasus penipuan online.” Diakses 11 April 2026. <https://www.antaranews.com/>.