Kajian Normatif terhadap Tantangan Penegakan Hukum atas Tindak Pidana Scam Lintas Negara di Era Globalisasi

Budi Himawan[1*]

[1]Universitas Terbuka, Jalan Pondok Cabe Raya, Kec. Ciputat, Tangerang Selatan, Indonesia

*Alamat email penulis koresponden: 055514916@ecampus.ut.ac.id

Abstrak

Fenomena tindak pidana scam lintas negara telah meningkat secara signifikan seiring dengan kemajuan teknologi informasi dan globalisasi. Kejahatan ini bersifat transnasional, melibatkan pelaku, korban, dan sarana kejahatan dari berbagai yurisdiksi, sehingga menimbulkan tantangan besar bagi penegakan hukum nasional. Artikel ini bertujuan untuk menganalisis tantangan dan solusi penegakan hukum terhadap tindak pidana scam lintas negara di Indonesia melalui pendekatan normatif. Metode penelitian yang digunakan adalah penelitian hukum yuridis normatif, dengan pendekatan perundang-undangan**,** konseptual**,** dan komparatif. Hasil penelitian menunjukkan bahwa tindak pidana *scam* lintas negara di Indonesia masih menghadapi berbagai kendala, baik dari aspek normatif maupun structural. Efektivitas penegakan hukum masih terhambat oleh keterbatasan asas teritorialitas, perbedaan sistem hukum antarnegara, dan lambatnya mekanisme kerja sama internasional. Untuk itu, diperlukan penguatan regulasi nasional, pengembangan instrumen kerja sama hukum internasional seperti Mutual Legal Assistance dan ekstradisi, serta peningkatan kapasitas aparat penegak hukum melalui teknologi forensik digital dan pemahaman hukum internasional. Pendekatan normatif ini diharapkan dapat memperkuat kerangka hukum dan mekanisme penegakan hukum Indonesia dalam menghadapi tindak pidana scam lintas negara.

Kata Kunci Scam; Penegakan hukum; Cybercrime; Pendekatan normatif; Globalisasi

Abstract

The phenomenon of cross-border scam crimes has increased significantly in line with advances in information technology and globalization. This crime is transnational in nature, involving perpetrators, victims, and criminal instruments from multiple jurisdictions, thereby creating major challenges for national law enforcement. This article aims to analyze the challenges and solutions of law enforcement against cross-border scam crimes in Indonesia through a normative approach. The research method employed is normative juridical legal research, using statutory, conceptual, and comparative approaches. The results indicate that cross-border scam crimes in Indonesia still face various obstacles, both normatively and structurally. The effectiveness of law enforcement remains hindered by the limitations of the territoriality principle, differences in legal systems among countries, and the slow pace of international cooperation mechanisms. Therefore, it is necessary to strengthen national regulations, develop international legal cooperation instruments such as Mutual Legal Assistance and extradition, and enhance the capacity of law enforcement officials through digital forensic technology and understanding of international law. This normative approach is expected to strengthen Indonesia's legal framework and law enforcement mechanisms in addressing cross-border scam crimes.

Keywords: *Scam; Law enforcement; Cybercrime; Normative approach; Globalization*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era globalisasi telah mengubah secara fundamental pola interaksi sosial, ekonomi, dan hukum masyarakat dunia. Aktivitas transaksi lintas negara yang sebelumnya membutuhkan kehadiran fisik kini dapat dilakukan secara instan melalui media digital. Transformasi ini, meskipun membawa kemudahan dan efisiensi, juga membuka ruang baru bagi munculnya berbagai bentuk kejahatan siber (*cybercrime*), salah satunya ialah tindak pidana scam atau penipuan daring lintas negara. Fenomena ini bukan hanya menjadi masalah hukum nasional, tetapi juga masalah hukum transnasional yang kompleks, karena pelaku, korban, dan instrumen kejahatannya kerap berada di yurisdiksi negara yang berbeda. Kondisi tersebut menimbulkan tantangan serius bagi sistem penegakan hukum, terutama terkait keterbatasan hukum positif Indonesia dalam menjangkau dan menindak pelaku kejahatan scam yang beroperasi secara global (Djunarjanto, A. A., et al., 2024).

Dalam konteks hukum positif di Indonesia, tindak pidana scam pada dasarnya dapat dikualifikasikan sebagai tindak pidana penipuan sebagaimana diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP), serta dapat dikaitkan dengan ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Namun, ketentuan-ketentuan tersebut belum secara eksplisit mengatur dimensi lintas negara dari kejahatan scam. Dalam praktiknya, pelaku seringkali berdomisili di luar negeri, menggunakan jaringan server asing, serta beroperasi dengan pola kejahatan terorganisir lintas batas. Hal ini menimbulkan kesulitan dalam hal pembuktian, pelacakan, serta ekstradisi pelaku, karena keterbatasan yurisdiksi nasional serta belum optimalnya kerja sama hukum internasional antara Indonesia dan negara lain. Di sinilah terlihat adanya kesenjangan antara perkembangan modus kejahatan global dengan pengaturan dan kapasitas penegakan hukum nasional.

Sejumlah penelitian terdahulu telah membahas isu penegakan hukum terhadap kejahatan siber di Indonesia. Misalnya, penelitian oleh Riyanto (2020) yang menyoroti lemahnya koordinasi antar lembaga penegak hukum dalam menghadapi kejahatan digital di dalam negeri, serta Sari (2021) yang membahas efektivitas UU ITE terhadap penipuan daring domestik. Penelitian lain oleh Nasution (2022) juga menekankan pentingnya peningkatan kapasitas digital forensics dalam pembuktian perkara kejahatan siber. Namun, sebagian besar penelitian tersebut masih berfokus pada konteks kejahatan scam di ranah nasional dan belum mengkaji secara mendalam aspek lintas negara serta hambatan kerja sama hukum internasional yang menjadi faktor kunci dalam penegakan hukum di era globalisasi. Dengan demikian, kajian yang menelaah secara normatif tantangan penegakan hukum terhadap tindak pidana scam lintas negara menjadi penting untuk mengisi kekosongan akademik tersebut.

Dari perspektif teori hukum dan penegakan hukum, globalisasi telah menantang prinsip kedaulatan hukum negara. Menurut teori transnational criminal law, yurisdiksi nasional tidak lagi memadai untuk menjangkau kejahatan yang bersifat lintas batas karena sistem hukum setiap negara memiliki aturan dan mekanisme yang berbeda. Dalam konteks Indonesia, keterlibatan negara dalam berbagai instrumen hukum internasional seperti *Mutual Legal*

Assistance in Criminal Matters (MLA), konvensi ekstradisi, maupun perjanjian kerja sama digital belum sepenuhnya dimanfaatkan secara optimal. Hal ini menunjukkan adanya kebutuhan untuk melakukan pembaruan dan harmonisasi hukum nasional dengan standar internasional agar penegakan hukum dapat berjalan efektif terhadap tindak pidana scam lintas negara (Sari, D.M., 2021).

Urgensi penelitian ini terletak pada meningkatnya eskalasi kejahatan scam lintas negara yang berdampak langsung terhadap masyarakat Indonesia. Peningkatan signifikan kasus penipuan daring internasional yang melibatkan warga negara Indonesia, baik sebagai korban maupun sebagai pelaku yang direkrut oleh jaringan kriminal global. Dampak sosial yang ditimbulkan tidak hanya berupa kerugian ekonomi masyarakat, tetapi juga hilangnya kepercayaan terhadap sistem hukum dan keamanan digital nasional (Tobing, C. I., et al., 2023). Oleh karena itu, diperlukan suatu kajian normatif yang mendalam untuk menelaah sejauh mana hukum nasional telah mampu mengantisipasi dan menanggulangi fenomena ini serta bagaimana strategi penegakan hukumnya dapat disinergikan dengan kerja sama internasional di bidang hukum pidana. Penelitian ini berupaya menunjukkan bahwa efektivitas penegakan hukum terhadap tindak pidana scam lintas negara tidak dapat hanya bergantung pada hukum nasional, melainkan membutuhkan integrasi norma hukum internasional, mekanisme kerja sama antarnegara, dan adaptasi terhadap perkembangan teknologi informasi global. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan kontribusi teoritis bagi pengembangan hukum pidana transnasional di Indonesia serta menawarkan rekomendasi kebijakan normatif untuk memperkuat sistem penegakan hukum terhadap kejahatan scam lintas negara di era globalisasi.

2. METODE

Penelitian ini menggunakan metode penelitian hukum normatif yuridis (*normative juridical research*), yaitu pendekatan yang menelaah hukum dari sisi normatif dengan menitikberatkan pada bahan hukum tertulis. Metode ini dipilih karena penelitian berfokus pada efektivitas dan kesesuaian norma hukum dalam menghadapi kejahatan lintas negara, khususnya tindak pidana *scam* akibat globalisasi dan kemajuan teknologi informasi. Pendekatan yang digunakan meliputi pendekatan perundang-undangan**,** konseptual**,** dan komparatif. Pendekatan perundang-undangan digunakan untuk mengkaji regulasi nasional seperti KUHP, Undang-Undang Nomor 1 tahun 2024 tentang perubahan kedua Undang-Undang Nomor 11 Tahun 2008 tentang ITE dan Undang-Undang Nomor 1 Tahun 2023 tentang KUHP baru guna menilai sejauh mana hukum positif Indonesia menjangkau tindak pidana *scam* lintas negara. Pendekatan konseptual mengkaji teori dan doktrin hukum terkait *transnational crime*, yurisdiksi, dan tanggung jawab pidana lintas negara. Sedangkan pendekatan komparatif digunakan untuk menelaah pengaturan dan penegakan hukum di negara lain yang telah meratifikasi *Budapest Convention on Cybercrime*, agar dapat diidentifikasi praktik terbaik (*best practices*) bagi sistem hukum Indonesia (Soekanto, S., et al., 2015; Marzuki, P.M., 2017).

Sumber data terdiri atas bahan hukum primer**,** sekunder**,** dan tersier. Bahan primer mencakup peraturan nasional dan internasional seperti *Budapest Convention* dan *Mutual Legal Assistance (MLA)*. Bahan sekunder diperoleh dari buku, jurnal, dan publikasi lembaga resmi seperti Kominfo dan Kepolisian RI, sedangkan bahan tersier meliputi kamus hukum dan ensiklopedia. Data dikumpulkan melalui studi kepustakaan (*library research*) dan dianalisis secara kualitatif dengan penalaran deduktif, yakni dari prinsip umum dan teori hukum menuju analisis terhadap norma positif dan praktik penegakan hukum terhadap tindak pidana *scam* lintas negara (Marzuki, P.M., 2017).

3. HASIL DAN PEMBAHASAN

3.1. Pengaturan Hukum Positif di Indonesia mengenai Tindak Pidana *Scam* Lintas Negara

Pengaturan hukum positif di Indonesia mengenai tindak pidana *scam*, khususnya yang bersifat lintas negara (*cross-border crime*), pada dasarnya masih tersebar dalam berbagai instrumen hukum, baik yang bersifat umum maupun khusus. Sebagai tindak kejahatan yang memanfaatkan teknologi informasi dan komunikasi, *scam* pada dasarnya termasuk dalam kategori kejahatan siber (*cybercrime*), namun dengan karakteristik khusus karena melibatkan unsur penipuan yang dilakukan melalui jaringan elektronik dan sering kali melampaui batas yurisdiksi nasional. Oleh karena itu, pengaturan hukum yang relevan tidak hanya mencakup ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP), tetapi juga dalam Undang-Undang Nomor 1 tahun 2024 tentang perubahan kedua Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta beberapa peraturan internasional yang menjadi acuan dalam kerja sama penegakan hukum lintas negara.

Secara historis, ketentuan mengenai *scam* dapat ditemukan dalam Pasal 378 KUHP yang mengatur tindak pidana penipuan. Pasal tersebut menyebutkan bahwa setiap orang yang dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, atau rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan sesuatu barang kepadanya, dapat dipidana karena penipuan. Meskipun pasal ini bersifat umum dan belum mengakomodasi aspek digital, substansi penipuannya relevan untuk *scam* karena sama-sama mengandung unsur penyesatan dan pengelabuan terhadap korban. Namun demikian, penerapan Pasal 378 KUHP sering kali menghadapi kendala dalam konteks kejahatan siber lintas negara, karena unsur "perbuatan" dan "akibat" yang terjadi di wilayah yurisdiksi berbeda, sehingga menimbulkan kesulitan pembuktian dan penegakan hokum (Simbolon, N. Y. 2023; Sinaga, M.I.J., 2024).

Untuk menjawab kekosongan tersebut, lahir Undang-Undang Nomor 1 tahun 2024 tentang perubahan kedua Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE memberikan dasar hukum yang lebih spesifik terhadap tindak pidana *scam* berbasis elektronik. Pasal 28 ayat (1) UU ITE secara tegas melarang setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang merugikan konsumen dalam transaksi elektronik. Ketentuan ini dapat digunakan untuk menjerat pelaku *online scam* yang melakukan penipuan melalui media digital seperti situs web, media sosial,

atau aplikasi pesan. Selain itu, Pasal 35 UU ITE juga mengatur perbuatan manipulasi data elektronik dengan tujuan memperoleh keuntungan bagi diri sendiri atau orang lain secara melawan hukum, yang substansinya sejalan dengan modus *phishing*, *investment scam*, dan bentuk penipuan digital lainnya.

Meskipun UU ITE telah memberikan landasan hukum yang lebih modern, penerapannya terhadap kejahatan lintas negara masih menghadapi tantangan yurisdiksi. Hal ini disebabkan karena prinsip dasar hukum pidana Indonesia, sebagaimana diatur dalam Pasal 2 KUHP, menganut asas teritorialitas, yang berarti hukum pidana Indonesia hanya berlaku terhadap perbuatan yang dilakukan di wilayah Indonesia. Sementara itu, dalam kasus *scam* lintas negara, pelaku dapat berada di luar negeri sedangkan korban berada di Indonesia, atau sebaliknya. Kondisi ini menimbulkan kesulitan dalam menentukan yurisdiksi hukum mana yang berwenang memproses perkara tersebut. Meskipun KUHP dalam Pasal 4 sampai dengan Pasal 9 memberikan pengecualian dengan menerapkan asas ekstrateritorial terbatas (misalnya terhadap kejahatan yang merugikan kepentingan nasional), penerapannya terhadap *cyber scam* masih belum optimal karena membutuhkan mekanisme kerja sama internasional yang lebih efektif (Lokapala, Y. H et al., 2024).

Perkembangan terbaru dalam hukum nasional, yakni dengan disahkannya Undang-Undang Nomor 1 Tahun 2023 tentang KUHP baru, memberikan peluang pembaruan terhadap sistem hukum pidana dalam konteks globalisasi. UU ini memperluas jangkauan yurisdiksi hukum pidana Indonesia dengan memperkenalkan asas kejahatan lintas batas (*transnational crimes*) yang mengakui pentingnya kerja sama internasional dalam penegakan hukum. Meskipun belum secara eksplisit menyebut istilah *scam*, ketentuan ini dapat dijadikan dasar normatif untuk memperkuat pengaturan dan penegakan hukum terhadap tindak pidana yang melibatkan unsur lintas negara melalui media digital (Hasri, H., et al, 2024).

Dalam konteks internasional, pengaturan terhadap *scam* lintas negara idealnya selaras dengan instrumen hukum global, salah satunya Budapest Convention on Cybercrime (2001), yang merupakan konvensi internasional pertama dan paling komprehensif dalam penanggulangan kejahatan siber. Konvensi ini mengatur kerja sama lintas negara dalam penyelidikan, pengumpulan bukti elektronik, dan ekstradisi pelaku kejahatan siber. Indonesia hingga saat ini belum meratifikasi konvensi tersebut, sehingga mekanisme kerja sama internasional masih terbatas pada perjanjian bilateral atau regional, seperti *Mutual Legal Assistance in Criminal Matters (MLA)* dalam kerangka ASEAN. Keterbatasan ini menyebabkan penegakan hukum terhadap *scam* lintas negara sering kali tidak efektif, karena dibutuhkan koordinasi antarotoritas yang kompleks serta perbedaan sistem hukum antarnegara yang menghambat proses pembuktian dan pemidanaan (Widiastuti, A., et al, 2025). Selain dari aspek normatif, tantangan lain yang dihadapi adalah rendahnya kapasitas lembaga penegak hukum dalam memahami modus kejahatan siber modern. Penegakan hukum terhadap *scam* lintas negara membutuhkan pemahaman teknis mendalam tentang teknologi informasi, kemampuan digital forensik, serta kerja sama lintas yurisdiksi yang cepat dan efisien (Masyhar, A., et al., 2023). Oleh karena itu, penguatan regulasi perlu diiringi dengan peningkatan kapasitas kelembagaan dan penyesuaian terhadap standar hukum internasional.

Dengan demikian, dapat disimpulkan bahwa pengaturan hukum positif di Indonesia terhadap tindak pidana *scam* lintas negara masih bersifat parsial dan belum sepenuhnya komprehensif. KUHP dan UU ITE memang menyediakan dasar hukum untuk menjerat pelaku, namun belum cukup menjawab kompleksitas *scam* lintas batas yang melibatkan yurisdiksi asing. Ketiadaan ratifikasi terhadap konvensi internasional seperti *Budapest Convention* juga memperlemah posisi Indonesia dalam kerja sama global. Oleh karena itu, diperlukan langkah normatif berupa pembaruan regulasi yang secara eksplisit mengatur kejahatan siber lintas negara serta penguatan mekanisme kerja sama internasional agar penegakan hukum terhadap tindak pidana *scam* di era globalisasi dapat berjalan efektif, terkoordinasi, dan sejalan dengan prinsip keadilan universal.

3.2. Tantangan Yuridis dalam Penegakan Hukum terhadap Tindak Pidana *Scam* Lintas Negara di Era Globalisasi

Penegakan hukum terhadap tindak pidana *scam* lintas negara di era globalisasi menghadapi berbagai tantangan yuridis yang kompleks, terutama karena sifat kejahatan ini yang tidak mengenal batas teritorial negara dan dilakukan melalui jaringan teknologi informasi yang bersifat global. Karakteristik tersebut menimbulkan persoalan mendasar dalam hal yurisdiksi, pembuktian, kerja sama internasional, hingga disparitas hukum antarnegara. Dari perspektif hukum positif Indonesia, berbagai ketentuan telah tersedia melalui KUHP, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta peraturan lain yang terkait, namun implementasinya dihadapkan pada sejumlah kendala normatif dan struktural yang membatasi efektivitas penegakan hukum.

Tantangan yuridis pertama yang dihadapi aparat penegak hukum adalah masalah yurisdiksi dan batasan kedaulatan hukum**.** Dalam konteks kejahatan *scam* lintas negara, pelaku, korban, dan sarana kejahatan sering kali berada di wilayah hukum yang berbeda. Sebagai contoh, pelaku dapat beroperasi dari luar negeri, sementara korban dan akibat hukum terjadi di Indonesia. Menurut prinsip dasar hukum pidana Indonesia sebagaimana diatur dalam Pasal 2 KUHP, hukum pidana Indonesia hanya berlaku terhadap perbuatan yang dilakukan di wilayah Indonesia (asas teritorialitas). Sementara asas-asas lain seperti nasional aktif**,** nasional pasif**,** dan perlindungan universal hanya berlaku dalam kondisi tertentu dan sangat terbatas penerapannya terhadap kejahatan siber. Ketiadaan pengaturan eksplisit mengenai yurisdiksi dalam kejahatan siber lintas negara membuat aparat penegak hukum sering kali kesulitan menentukan dasar kewenangan untuk memproses pelaku yang berada di luar negeri. Kondisi ini semakin rumit ketika negara tempat pelaku berada tidak memiliki perjanjian ekstradisi atau kerja sama hukum dengan Indonesia, sehingga proses penegakan hukum menjadi terhambat atau bahkan tidak dapat dilakukan sama sekali (Sitanggang, A. S., et al., 2024 ; Widyastuti, A., et al., 2025).

Tantangan kedua adalah keterbatasan instrumen hukum nasional yang belum sepenuhnya mengakomodasi sifat transnasional kejahatan *scam*. UU ITE sebagai payung hukum utama untuk menjerat pelaku kejahatan siber memang telah mengatur perbuatan penipuan digital, manipulasi data, serta penyebaran informasi menyesatkan. Namun, undang-undang ini tidak

secara tegas mengatur mekanisme penanganan lintas batas negara, termasuk prosedur pengumpulan alat bukti elektronik dari luar negeri atau pelaksanaan penegakan hukum terhadap warga negara asing. Sementara itu, KUHP masih berlandaskan konsep klasik yang menitikberatkan pada ruang dan waktu terjadinya tindak pidana, yang kurang relevan untuk menjerat kejahatan siber yang bersifat virtual dan lintas yurisdiksi. Akibatnya, terdapat kesenjangan normatif antara substansi hukum nasional dengan realitas perkembangan teknologi dan modus kejahatan di era digital (Isa, S.N., et al., 2023; Tobing, C.I., et al., 2023).

Tantangan ketiga berkaitan dengan kesulitan pembuktian dan validitas alat bukti elektronik. Dalam kasus *scam* lintas negara, alat bukti yang relevan sering kali tersebar di berbagai negara dan tersimpan dalam server milik penyedia layanan digital internasional. Hal ini menimbulkan hambatan dalam memperoleh bukti elektronik yang sah menurut hukum acara pidana Indonesia. Meskipun UU ITE dan Peraturan Mahkamah Agung Nomor 1 Tahun 2019 telah mengakui validitas alat bukti elektronik, proses memperoleh dan mengesahkannya dalam konteks internasional tetap memerlukan mekanisme bantuan hukum timbal balik (*Mutual Legal Assistance* atau MLA). Namun, pelaksanaannya sering kali lambat dan tidak efektif karena perbedaan sistem hukum, birokrasi antarnegara, serta faktor kerahasiaan data pribadi yang diatur ketat oleh hukum negara lain. Akibatnya, proses pembuktian menjadi terhambat dan berdampak pada sulitnya menjerat pelaku secara hokum (Masyhar, A., et al., 2023; Widyastuti, A., et al., 2025).

Selain itu, tantangan yuridis juga muncul dalam aspek harmonisasi hukum internasional dan keterlibatan Indonesia dalam instrumen global. Hingga saat ini, Indonesia belum meratifikasi *Budapest Convention on Cybercrime (2001)*, padahal konvensi tersebut merupakan standar internasional utama yang mengatur tentang kerja sama, ekstradisi, serta pertukaran data lintas negara dalam penanganan kejahatan siber. Ketidakterlibatan Indonesia menyebabkan keterbatasan akses terhadap mekanisme kerja sama formal dengan negara-negara anggota konvensi, sehingga upaya penegakan hukum terhadap *scam* lintas negara sering kali harus dilakukan melalui jalur diplomatik atau perjanjian bilateral yang lebih lambat dan tidak terstandar. Kondisi ini memperlemah posisi Indonesia dalam upaya global melawan kejahatan siber dan mengurangi efektivitas penegakan hukum nasional terhadap pelaku kejahatan lintas negara (Sitanggang, A. S., et al., 2024).

Tantangan berikutnya adalah keterbatasan sumber daya aparat penegak hukum dan infrastruktur penegakan hukum siber. Kejahatan *scam* lintas negara sering menggunakan teknik dan perangkat digital yang sangat kompleks, seperti *phishing*, *malware injection*, *social engineering*, hingga penggunaan jaringan anonim (*dark web*). Kondisi ini menuntut kemampuan teknis dan investigatif yang tinggi dari aparat penegak hukum, terutama dalam bidang digital forensik dan analisis data lintas negara. Namun, dalam praktiknya, kemampuan teknis dan fasilitas pendukung di lembaga penegak hukum Indonesia masih belum merata. Penanganan kasus kejahatan siber sering kali bergantung pada unit khusus seperti Direktorat Tindak Pidana Siber Bareskrim Polri, sementara koordinasi antarinstansi seperti Kominfo, Kejaksaan, dan lembaga peradilan belum sepenuhnya terintegrasi. Keterbatasan ini berimplikasi pada lambatnya proses penyelidikan, kurangnya pemahaman teknis aparat

terhadap modus kejahatan digital, serta kesulitan menyesuaikan proses pembuktian dengan standar hukum internasional (Isa, S.N., et al.,2023; Tobing, C.I., et al.,2023).

Dari sudut pandang yuridis-formal, tantangan lain juga muncul dalam aspek perlindungan korban dan restitusi lintas negara. Hukum nasional Indonesia belum memiliki mekanisme yang jelas untuk memberikan perlindungan hukum dan pemulihan bagi korban *scam* lintas negara. Ketika korban berada di Indonesia tetapi pelaku di luar negeri, proses pengembalian kerugian finansial menjadi hampir tidak mungkin dilakukan karena keterbatasan yurisdiksi dan ketiadaan mekanisme pengakuan putusan antarnegara (*judgment recognition*) (Lokapala, Y. H., et al., 2024). Dalam konteks ini, korban sering kali tidak hanya mengalami kerugian ekonomi, tetapi juga kehilangan akses keadilan karena sistem hukum belum mampu menjangkau pelaku yang berada di luar negeri.

Secara konseptual, berbagai tantangan yuridis tersebut menunjukkan bahwa sistem hukum nasional Indonesia masih berorientasi pada paradigma hukum pidana tradisional yang berbasis teritorial, sementara kejahatan *scam* lintas negara menuntut pendekatan yang lebih adaptif dan kolaboratif secara internasional. Oleh karena itu, diperlukan langkah pembaruan hukum berupa integrasi antara hukum nasional dan hukum internasional, khususnya dengan memperkuat dasar yurisdiksi ekstateritorial, mempercepat ratifikasi konvensi internasional seperti *Budapest Convention*, serta memperluas perjanjian kerja sama hukum bilateral dan multilateral. Di samping itu, penguatan kapasitas aparat penegak hukum, peningkatan infrastruktur digital forensik, dan pembentukan mekanisme perlindungan korban lintas negara menjadi prasyarat penting bagi efektivitas penegakan hukum di era globalisasi (Hasri, H., et al., 2024).

Dengan demikian, tantangan yuridis dalam penegakan hukum terhadap tindak pidana *scam* lintas negara di Indonesia bukan hanya terletak pada kekurangan norma hukum, tetapi juga pada keterbatasan koordinasi internasional dan kesiapan institusional dalam menghadapi bentuk-bentuk kejahatan baru yang bersifat lintas batas. Upaya mengatasi tantangan ini memerlukan sinergi antara pembaruan hukum nasional, harmonisasi dengan standar internasional, dan peningkatan kapasitas penegak hukum agar sistem peradilan pidana Indonesia mampu beradaptasi dengan dinamika global dan memberikan perlindungan hukum yang efektif bagi masyarakat di era digital.

3.3. Upaya dan Mekanisme Kerja Sama Hukum Internasional dalam Mengatasi Hambatan Penegakan Hukum terhadap Tindak Pidana *Scam* Lintas Negara

Dalam konteks globalisasi dan kemajuan teknologi informasi, tindak pidana *scam* telah berkembang menjadi fenomena kejahatan lintas negara (*transnational cybercrime*) yang sulit ditangani secara unilateral oleh suatu negara. Sifatnya yang lintas yurisdiksi, melibatkan pelaku, korban, dan sarana kejahatan dari berbagai negara, menuntut adanya kerja sama hukum internasional yang efektif dan terkoordinasi. Penegakan hukum terhadap *scam* lintas negara tidak dapat hanya bergantung pada hukum nasional seperti KUHP dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), karena keterbatasan asas teritorialitas dan kedaulatan negara sering kali menghambat penyelidikan, penuntutan, maupun pelaksanaan putusan. Oleh karena itu, mekanisme kerja sama hukum internasional menjadi instrumen

penting dalam menjembatani keterbatasan tersebut dan memperkuat efektivitas penegakan hukum lintas batas (Tobing, C.I., 2023; Djunarjanto, A. A., et al., 2024).

Kerja sama hukum internasional dalam konteks tindak pidana *scam* dapat dilakukan melalui berbagai mekanisme formal, baik bilateral, regional, maupun multilateral. Salah satu bentuk utama adalah *Mutual Legal Assistance in Criminal Matters* (MLA), yaitu mekanisme bantuan timbal balik antarnegara dalam pengumpulan alat bukti, pemeriksaan saksi, penyitaan aset, serta pelaksanaan proses hukum lain yang diperlukan dalam perkara pidana lintas negara. Indonesia telah memiliki landasan hukum untuk pelaksanaan kerja sama ini melalui Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana. Melalui instrumen tersebut, Indonesia dapat meminta atau memberikan bantuan hukum kepada negara lain dalam penyelidikan kasus *scam* lintas negara. Misalnya, ketika pelaku *scam* berada di luar negeri namun korbannya di Indonesia, aparat penegak hukum Indonesia dapat mengajukan permintaan resmi kepada negara tempat pelaku berada untuk memperoleh bukti elektronik, memeriksa rekening, atau melakukan penangkapan. Walaupun demikian, efektivitas MLA masih sangat bergantung pada adanya perjanjian bilateral antara Indonesia dan negara tujuan serta kesediaan negara lain untuk bekerja sama (Anggraeni, K., et al., 2024; Sinaga, M. I. J., 2024).

Selain melalui MLA, kerja sama internasional juga dapat dilakukan melalui perjanjian ekstradisi, yaitu mekanisme penyerahan pelaku kejahatan dari satu negara ke negara lain untuk diadili atau menjalani hukuman. Ekstradisi menjadi penting dalam penanganan *scam* lintas negara karena sering kali pelaku melarikan diri atau beroperasi dari negara yang berbeda dengan tempat terjadinya kerugian. Indonesia telah memiliki dasar hukum ekstradisi melalui Undang-Undang Nomor 1 Tahun 1979 tentang Ekstradisi, serta sejumlah perjanjian bilateral dengan negara seperti Malaysia, Thailand, Australia, dan Singapura. Namun, masih banyak negara lain yang belum memiliki perjanjian ekstradisi dengan Indonesia, sehingga penegakan hukum terhadap pelaku *scam* internasional sering kali terhambat oleh perbedaan sistem hukum dan prinsip non-ekstradisi bagi warga negara tertentu (Sinaga, M.I.J., 2024; Bhuy, L. S., et al., 2024).

Dalam konteks multilateral, Budapest Convention on Cybercrime (2001) merupakan instrumen internasional paling penting dalam penanggulangan kejahatan siber, termasuk tindak pidana *scam*. Konvensi ini mengatur kerja sama internasional dalam penyelidikan, pengumpulan bukti elektronik, dan ekstradisi pelaku kejahatan siber. Negara-negara yang menjadi pihak konvensi memiliki kewajiban untuk membantu satu sama lain dalam penyidikan kejahatan siber secara cepat dan efisien melalui mekanisme komunikasi langsung antarotoritas. Meskipun Indonesia belum meratifikasi konvensi tersebut, substansi Budapest Convention dapat dijadikan acuan dalam memperkuat kerangka hukum nasional dan membangun standar kerja sama internasional. Ratifikasi terhadap konvensi ini akan memberikan manfaat strategis, antara lain mempercepat pertukaran informasi lintas negara, memperluas jaringan kerja sama investigatif, dan memberikan legitimasi bagi aparat penegak hukum Indonesia untuk mengakses data lintas yurisdiksi sesuai prosedur hukum internasional.

Selain instrumen formal tersebut, kerja sama internasional dalam penanggulangan *scam* lintas negara juga dapat dilakukan melalui mekanisme regional dan kelembagaan multinasional. Di kawasan Asia Tenggara, kerja sama hukum diatur dalam kerangka *ASEAN Mutual Legal Assistance Treaty (ASEAN MLAT)* yang ditandatangani pada tahun 2004. Perjanjian ini menjadi landasan koordinasi antarnegara ASEAN dalam penyelidikan kejahatan lintas batas, termasuk kejahatan siber. Dalam praktiknya, *ASEAN MLAT* berperan penting dalam memperkuat jaringan komunikasi antarpenegak hukum melalui forum seperti *ASEAN Ministerial Meeting on Transnational Crime (AMMTC)* dan *ASEANAPOL* (ASEAN Chiefs of National Police). Melalui mekanisme ini, negara-negara ASEAN dapat saling bertukar data intelijen, modus operandi, dan pola kejahatan *scam* yang semakin kompleks (Masyhar, A., et al., 2024).

Kerja sama internasional tidak hanya dilakukan antarnegara, tetapi juga melibatkan organisasi internasional dan lembaga penegakan hukum global, seperti *Interpol*, *Europol*, dan *United Nations Office on Drugs and Crime (UNODC)*. *Interpol* misalnya, memiliki sistem *I-24/7 Global Police Communication System* yang memungkinkan pertukaran data kriminal dan identitas pelaku secara real time antarnegara. Indonesia sebagai anggota aktif *Interpol* dapat memanfaatkan sistem ini untuk melacak pelaku *scam* lintas negara, mengidentifikasi jaringan kejahatan terorganisasi, serta memantau pergerakan dana hasil kejahatan melalui sistem perbankan global. Sementara itu, *UNODC* memberikan dukungan teknis dan pelatihan kepada aparat penegak hukum dalam penguatan kapasitas digital forensik dan tata kelola keamanan siber (Bhuy, S.L., wt al., 2024 ; Hasri, H., et al., 2024).

Namun demikian, penerapan mekanisme kerja sama hukum internasional dalam praktiknya masih menghadapi sejumlah hambatan. Hambatan tersebut meliputi perbedaan sistem hukum antarnegara, lamanya proses birokrasi dalam permintaan bantuan hukum, keterbatasan sumber daya manusia dan teknologi, serta isu kedaulatan dan perlindungan data pribadi. Oleh karena itu, efektivitas kerja sama hukum internasional bergantung pada sejauh mana negara-negara bersedia mengharmonisasikan hukum nasionalnya dengan standar internasional dan membangun kepercayaan (mutual trust) antarotoritas penegak hukum. Dalam konteks Indonesia, langkah strategis yang dapat ditempuh adalah memperkuat instrumen nasional seperti UU ITE dan UU MLA dengan menambahkan ketentuan khusus mengenai kejahatan siber lintas negara, mempercepat proses ratifikasi *Budapest Convention*, serta memperluas perjanjian bilateral yang mencakup pertukaran data digital, pembekuan aset, dan ekstradisi pelaku *scam* (Djunarjanto, A. A., et al., 2024).

Selain pembaruan regulasi, kerja sama hukum internasional juga harus diiringi dengan penguatan kapasitas kelembagaan dan peningkatan teknologi hukum (*legal technology*). Aparat penegak hukum perlu dibekali kemampuan digital forensik, investigasi siber, serta pemahaman hukum internasional agar mampu berperan aktif dalam jaringan kerja sama global. Integrasi antara kepolisian, kejaksaan, Kementerian Komunikasi dan Digital, serta lembaga peradilan juga penting untuk memastikan bahwa setiap permintaan bantuan hukum atau ekstradisi dapat diproses secara cepat dan terkoordinasi (Widiastuti, A., et al., 2025).

Dengan demikian, mekanisme kerja sama hukum internasional menjadi elemen kunci dalam mengatasi hambatan penegakan hukum terhadap tindak pidana *scam* lintas negara. Upaya melalui MLA, ekstradisi, ratifikasi konvensi internasional, dan partisipasi dalam forum regional maupun global merupakan langkah strategis untuk memperkuat posisi Indonesia dalam menghadapi kejahatan lintas batas di era globalisasi. Penerapan kerja sama tersebut tidak hanya memperluas jangkauan yurisdiksi hukum nasional, tetapi juga menciptakan sistem penegakan hukum yang responsif, adaptif, dan terintegrasi dengan tata hukum internasional. Dengan dukungan politik hukum yang kuat serta komitmen antarnegara, kejahatan *scam* lintas negara dapat ditangani secara lebih efektif, memberikan perlindungan hukum bagi masyarakat, dan memperkuat reputasi Indonesia sebagai negara yang aktif berperan dalam menjaga keamanan siber global.

3.4. Pendekatan Normatif yang dapat digunakan untuk Memperkuat Efektivitas Penegakan Hukum terhadap Tindak Pidana Scam Lintas Negara

Dalam menghadapi tantangan penegakan hukum terhadap tindak pidana *scam* lintas negara, pendekatan normatif menjadi strategi utama untuk memperkuat landasan hukum nasional sekaligus mengharmonisasikannya dengan instrumen hukum internasional. Pendekatan normatif dalam konteks hukum pidana berorientasi pada analisis terhadap norma-norma hukum positif yang berlaku, baik tertulis maupun tidak tertulis, serta menelaah bagaimana norma tersebut dapat diadaptasikan untuk menjawab perkembangan kejahatan yang bersifat dinamis dan transnasional. Pendekatan ini tidak hanya menekankan pada tataran tekstual peraturan perundang-undangan, tetapi juga memandang penting keterpaduan antara prinsip-prinsip hukum, asas yurisdiksi, dan kebijakan kriminal (penal policy) yang sejalan dengan nilai keadilan dan efektivitas penegakan hukum di era globalisasi digital.

Secara konseptual, pendekatan normatif terhadap kejahatan *scam* lintas negara berangkat dari pandangan bahwa hukum pidana harus adaptif terhadap perubahan teknologi dan globalisasi. Kejahatan *scam* tidak lagi terjadi dalam batas-batas geografis tradisional, melainkan menggunakan ruang siber (*cyberspace*) yang bersifat virtual dan melintasi yurisdiksi banyak negara. Kondisi ini menimbulkan tantangan serius bagi sistem hukum nasional yang masih menganut asas teritorialitas sebagaimana diatur dalam Pasal 2 Kitab Undang-Undang Hukum Pidana (KUHP). Oleh karena itu, melalui pendekatan normatif, perlu dilakukan reinterpretasi dan revitalisasi terhadap asas-asas hukum pidana klasik agar lebih sesuai dengan kebutuhan hukum modern. Salah satunya dengan memperluas cakupan yurisdiksi melalui penerapan asas ekstrateritorial atau *universal jurisdiction*, yang memungkinkan Indonesia menindak pelaku kejahatan siber yang berdampak di wilayah hukum Indonesia meskipun pelaku berada di luar negeri. Langkah ini telah mulai diakomodasi dalam Undang-Undang Nomor 1 Tahun 2023 tentang KUHP baru yang memperkenalkan konsep kejahatan lintas batas (*transnational crimes*) dan memperkuat dasar hukum untuk kerja sama penegakan hukum internasional (Simbolon, N. Y., 2023; Hasri, H., et al., 2024).

Pendekatan normatif juga harus mencakup pembaruan terhadap regulasi khusus di bidang kejahatan siber. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Undang-

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah memberikan landasan hukum yang cukup kuat untuk menjerat pelaku penipuan digital. Namun, dalam konteks *scam* lintas negara, masih diperlukan penguatan norma terkait yurisdiksi internasional, mekanisme pembuktian lintas batas, serta pengakuan terhadap bukti elektronik dari luar negeri. Pendekatan normatif dalam hal ini dapat diarahkan pada pembentukan norma hukum baru atau amandemen terhadap UU ITE, dengan menambahkan ketentuan mengenai kerja sama internasional dalam penyelidikan dan pembuktian tindak pidana siber (Widiastuti, A., et al., 2025). Pengaturan ini juga harus selaras dengan prinsip-prinsip yang diatur dalam *Budapest Convention on Cybercrime (2001)* agar sistem hukum nasional Indonesia dapat beroperasi dalam kerangka kerja sama global yang terstandar.

Lebih jauh, pendekatan normatif dalam memperkuat efektivitas penegakan hukum terhadap tindak pidana *scam* lintas negara juga harus mempertimbangkan harmonisasi antara hukum nasional dan hukum internasional. Dalam sistem hukum pidana modern, tidak mungkin lagi suatu negara berdiri sendiri tanpa interkoneksi dengan sistem hukum negara lain. Oleh karena itu, Indonesia perlu menegaskan posisinya melalui ratifikasi instrumen hukum internasional yang relevan, seperti *Budapest Convention on Cybercrime* dan *United Nations Convention against Transnational Organized Crime (UNTOC)*. Ratifikasi ini bukan semata tindakan politik hukum internasional, melainkan langkah normatif strategis untuk memberikan legitimasi dan dasar hukum bagi aparat penegak hukum Indonesia dalam melakukan koordinasi lintas yurisdiksi, pertukaran data digital, serta pelacakan aset hasil kejahatan lintas negara. Pendekatan normatif yang berorientasi pada harmonisasi hukum ini akan memperkuat kedudukan Indonesia dalam sistem hukum global dan meningkatkan efektivitas penegakan hukum nasional terhadap pelaku kejahatan digital lintas batas (Masyhar, A., et al., 2024; Widiastuti, A., et al., 2025).

Di samping itu, dalam perspektif *law in action*, pendekatan normatif tidak dapat dilepaskan dari aspek kebijakan kriminal (*criminal policy*). Norma hukum yang baik harus diikuti dengan kebijakan implementatif yang realistis dan dapat diterapkan oleh aparat penegak hukum. Dalam konteks kejahatan *scam* lintas negara, pendekatan normatif perlu diarahkan untuk mengintegrasikan hukum pidana materiel, hukum pidana formil, dan hukum pelaksanaan pidana. Hukum pidana materiel (KUHP dan UU ITE) harus mengatur secara tegas unsur tindak pidana dan yurisdiksinya; hukum pidana formil (KUHAP) perlu disesuaikan agar mengakomodasi bukti elektronik lintas negara dan mekanisme bantuan hukum timbal balik (*Mutual Legal Assistance*); sementara hukum pelaksanaan pidana perlu diadaptasi agar memungkinkan eksekusi terhadap pelaku asing melalui mekanisme perjanjian ekstradisi atau kerja sama internasional. Pendekatan normatif semacam ini memastikan bahwa sistem hukum pidana Indonesia tidak hanya kuat di atas kertas, tetapi juga efektif dalam praktik penegakan hukum global (Isa, S. N., et al., 2023; Simbolon, N.Y., 2023).

Selanjutnya, pendekatan normatif yang digunakan juga harus mengakomodasi prinsip-prinsip keadilan universal (*universal justice*) dan perlindungan terhadap korban lintas negara. Hukum positif Indonesia masih lemah dalam memberikan mekanisme restitusi dan kompensasi bagi korban *scam* yang dirugikan oleh pelaku yang berada di luar negeri. Oleh karena itu,

secara normatif perlu dirumuskan ketentuan baru yang mengatur pengakuan dan pelaksanaan putusan pengadilan asing (*foreign judgment recognition*), sehingga korban dapat memperoleh hak ganti rugi lintas negara. Pengaturan semacam ini telah diterapkan di beberapa negara melalui prinsip *reciprocal enforcement of judgments*, dan dapat menjadi acuan bagi Indonesia dalam merancang kerangka hukum baru yang lebih responsif terhadap kepentingan korban kejahatan digital global (Lokapala, Y. H., et al., 2024).

Selain pembaruan norma dan prinsip, pendekatan normatif juga harus diarahkan pada penguatan *institusional framework* dalam sistem hukum nasional. Penegakan hukum terhadap tindak pidana *scam* lintas negara tidak hanya bergantung pada norma hukum, tetapi juga pada kejelasan otoritas dan koordinasi antarlembaga. Oleh karena itu, pendekatan normatif dapat mendorong pembentukan lembaga atau mekanisme nasional khusus, seperti *National Cybercrime Coordination Center* yang bertugas mengintegrasikan Polri, Kejaksaan, Komdigi, PPATK, dan BSSN dalam menangani kasus kejahatan siber lintas negara. Pembentukan lembaga ini harus didasarkan pada payung hukum yang kuat, misalnya melalui peraturan pemerintah atau undang-undang tersendiri tentang penegakan hukum siber, sehingga koordinasi lintas sektor dapat berjalan secara efektif, cepat, dan sesuai standar internasional (Riyanto, A., 2020).

Pendekatan normatif juga berperan dalam membangun kerangka hukum yang selaras dengan prinsip-prinsip hukum internasional publik. Dalam konteks ini, norma hukum nasional harus menjamin adanya mekanisme *legal reciprocity* dan *mutual trust* antarnegara, yang menjadi syarat utama bagi keberhasilan kerja sama hukum internasional. Prinsip ini dapat diwujudkan dengan menyesuaikan peraturan nasional mengenai ekstradisi dan bantuan hukum timbal balik agar sesuai dengan standar internasional. Revisi terhadap Undang-Undang Nomor 1 Tahun 1979 tentang Ekstradisi dan Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana perlu dilakukan dengan memasukkan ketentuan khusus mengenai kejahatan siber dan alat bukti elektronik lintas negara (Hariyono, A. G et al., 2024. Hasri, H., et al., 2024) Dengan demikian, hukum nasional Indonesia akan memiliki legitimasi dan kompatibilitas untuk digunakan dalam forum hukum internasional, baik bilateral maupun multilateral.

Akhirnya, pendekatan normatif yang ideal untuk memperkuat efektivitas penegakan hukum terhadap tindak pidana *scam* lintas negara adalah pendekatan yang bersifat integratif, yaitu menggabungkan pembaruan hukum nasional dengan harmonisasi terhadap standar hukum internasional, penguatan kelembagaan, serta orientasi pada perlindungan hak asasi dan keadilan bagi korban. Pendekatan ini tidak hanya memandang hukum sebagai sistem aturan, tetapi juga sebagai instrumen sosial yang dinamis untuk menegakkan keadilan dalam konteks global. Dalam kerangka ini, pembaruan hukum harus diarahkan pada pembentukan sistem hukum pidana siber nasional yang komprehensif, memiliki dimensi internasional, dan mampu beradaptasi dengan tantangan globalisasi teknologi. Dengan penerapan pendekatan normatif secara konsisten, Indonesia dapat membangun sistem penegakan hukum yang lebih efektif, berdaya saing global, dan mampu memberikan perlindungan hukum yang adil terhadap masyarakat dari ancaman kejahatan *scam* lintas negara di era digital.

4. KESIMPULAN

Penegakan hukum terhadap tindak pidana *scam* lintas negara di Indonesia masih menghadapi berbagai kendala, baik dari aspek normatif maupun struktural. Instrumen hukum nasional seperti KUHP dan UU ITE memang telah memberikan dasar hukum terhadap kejahatan siber, namun belum sepenuhnya mampu menjawab kompleksitas kejahatan lintas batas yang melibatkan yurisdiksi dan sistem hukum berbeda. Keterbatasan asas teritorialitas, kesulitan pembuktian elektronik lintas negara, serta lemahnya koordinasi internasional menjadi faktor utama rendahnya efektivitas penegakan hukum. Pendekatan normatif yang diperlukan untuk memperkuat efektivitas penegakan hukum harus diarahkan pada pembaruan dan harmonisasi hukum nasional dengan standar hukum internasional. Langkah ini mencakup perluasan asas yurisdiksi pidana dalam KUHP baru, penyempurnaan UU ITE agar lebih adaptif terhadap kejahatan digital, serta dorongan bagi Indonesia untuk meratifikasi *Budapest Convention on Cybercrime* dan memperluas kerja sama *Mutual Legal Assistance* serta ekstradisi. Selain pembaruan regulasi, peningkatan kapasitas aparat penegak hukum, penguatan forensik digital, dan koordinasi lintas lembaga juga menjadi faktor penting dalam implementasi hukum yang efektif.

DAFTAR PUSTAKA

Anggraeni, K., Rahmatiar, Y., & Abas, M. (2024). *Perlindungan konsumen terhadap scam di era digital: Studi komparatif efektivitas Indonesia Anti Scam Centre dan regulasi Singapura. Jurnal Ilmu Hukum, Humaniora dan Politik, 5*(6). https://doi.org/10.38035/jihhp.v5i6.5684

Bhuy, L. S., & Cartin-Pecson, R. (2024). *Dynamics of the Electronic Transaction Information Law in tackling cybercrime in Indonesia. Hermeneutika: Jurnal Ilmu Hukum, 8*(2). https://doi.org/10.33603/hermeneutika.v8i2.9594

Budapest Convention on Cybercrime. (2001). *Convention on Cybercrime, ETS No. 185.* Council of Europe. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Djunarjanto, A. A., Purwati, A., & Marina, L. (2024). *Transformasi modus kejahatan ekonomi transnasional di era digital: Analisis hukum pidana dan teknik forensik siber. SENTRI: Jurnal Riset Ilmiah, 4*(8). https://doi.org/10.55681/sentri.v4i8.4448

Hariyono, A. G., & Simangunsong, F. (2024). *Perlindungan hukum korban pencurian data pribadi (phishing cybercrime) dalam perspektif kriminologi. Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, 3*(1). https://doi.org/10.53363/bureau.v3i1.191

Hasri, H., Mashendra, M., Hayun, H., & Nurul Nisa, F. (2024). *Kejahatan cybercrime dan penanggulangannya dalam kerangka sistem hukum nasional. Indonesian Journal of Legality of Law, 7*(2). https://doi.org/10.35965/ijlf.v7i2.6240

Isa, S. N., Rahmayanti, R., Purba, P., & Manurung, K. (2023). *Criminal law policy in dealing with the development of transnational cyber crime. International Journal of Sociology and Law, 2*(2). https://doi.org/10.62951/ijsl.v2i2.652

Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). *Aspek yuridis kejahatan phishing dalam ketentuan hukum di Indonesia. Indonesian Journal of Criminal Law and Criminology, 5*(1). https://doi.org/10.18196/ijclc.v5i1.19853

Marzuki, P. M. (2017). *Penelitian hukum* (Edisi revisi). Jakarta: Kencana Prenada Media Grup.

Masyhar, A., Utari, I. S., Usman, U., & Sabri, A. Z. S. A. (2023). *Legal challenges of combating international cyberterrorism: the NCB Interpol Indonesia and global cooperation. Legality: Jurnal Ilmiah Hukum, 31*(2), 344–366. https://doi.org/10.22219/ljih.v31i2.29668

Nasution, R. (2022). *Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia: Analisis terhadap kapasitas digital forensik. Jurnal Hukum & Teknologi, 5*(2), 112–128.

Riyanto, A. (2020). *Koordinasi antar lembaga penegak hukum dalam menghadapi kejahatan siber di Indonesia. Jurnal Hukum dan Pembangunan, 50*(3), 389–406.

Sari, D. M. (2021). *Efektivitas Undang-Undang Informasi dan Transaksi Elektronik terhadap tindak pidana penipuan online di Indonesia. Jurnal Penegakan Hukum Indonesia, 9*(1), 55–70.

Simbolon, N. Y. (2023). *Ancaman cybercrime di Indonesia: Tinjauan sistematis dan peran cybersecurity pada e-commerce dalam hukum pidana. Jurnal Sosial Humaniora dan Pendidikan, 4*(2). https://doi.org/10.55606/inovasi.v4i2.4425

Sinaga, M. I. J. (2024). *Penetapan tersangka dalam penyidikan tindak pidana transnational cybercrime menurut sistem hukum di Indonesia. Syntax Literate: Jurnal Ilmiah Indonesia, 7*(3). https://doi.org/10.36418/syntax-literate.v7i3.6430

Sitanggang, A. S., Darmawan, F., & Saputra, D. (2024). *Hukum siber dan penegakan hukum di Indonesia: Tantangan dan solusi memerangi kejahatan siber. Jurnal Pendidikan dan Teknologi Indonesia, 4*(3), 79–83. https://doi.org/10.52436/1.jpti.409

Soekanto, S., & Mamudji, S. (2015). *Penelitian hukum normatif* (Edisi 1, cetakan revisi). Jakarta: Rajawali Pers.

Tobing, C. I., Surya, T. M., Selvias, L. R., Girsang, S. R., Azzahra, P. B., Yolanda, L., & Rusmana, N. (2023). *Globalisasi digital dan cybercrime: Tantangan hukum dalam*

menghadapi kejahatan siber lintas batas. Jurnal Hukum Sasana, 10(2). https://doi.org/10.31599/sasana.v10i2.3170

Undang-Undang Nomor 11 Tahun 2008 tentang *Informasi dan Transaksi Elektronik* (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58).

Undang-Undang Nomor 19 Tahun 2016 tentang *Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251).

Undang-Undang Nomor 1 Tahun 2023 tentang *Kitab Undang-Undang Hukum Pidana* (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 6841).

Undang-Undang Nomor 1 Tahun 2024 tentang *Perubahan Kedua Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 6905).

Widiastuti, A., & Mandasari Saragih, Y. (2025). *Transnational cyber crime: Challenges of international cooperation in combating cybercrime. International Journal of Contemporary Sciences, 3*(7). https://doi.org/10.55927/ijcs.v3i7.132