SIMPUL: Jurnal Ilmu Politik dan Hukum
Vol. 1, No. 4, Desember 2025, pp. 121-128
eISSN 3090-0867 | https://ejournal.gemacendekia.org/index.php/simpul

Paradigma Baru Hukum Pidana Dalam Menangani Kejahatan Digital Lintas Batas Negara

Andrean Nurhakim [a,1,*], Ahmad Fauzan [a,2], Milkan Sibawaeh [a,3]

[a] Program Studi Ilmu Hukum, Universitas Dr Soetomo, Indonesia
[1] andreannur42@gmail.com *; [2] ahmadfauzan735@gmail.com; [3] milkansibawaeh79@gmail.com
* Corresponding Author

ABSTRACT

The development of information technology has given rise to transnational forms of digital crime and poses serious challenges to national criminal law systems. Digital crime is no longer bound by a specific time and place, thus weakening the effectiveness of the conventional criminal law paradigm based on the principle of territoriality. This study aims to analyze the need for a renewed criminal law paradigm in addressing transnational digital crime and to formulate a criminal law policy direction that is more adaptive to global and digital realities. This study uses normative legal research methods with conceptual, statutory, and comparative approaches. The analysis examines criminal law doctrine, jurisdictional principles, and regulatory developments and law enforcement practices related to transnational cybercrime. Data were obtained through a literature review sourced from scientific literature, international journals, and relevant legal documents related to digital crime and transnational legal cooperation. The results of the study indicate that the national and territorial criminal law paradigm is no longer adequate to address the complexity of transnational digital crime. A new, transnational criminal law approach is needed, emphasizing legal harmonization, strengthening proportional extraterritorial jurisdiction, and effective international cooperation. This study confirms that updating the criminal law paradigm is a primary prerequisite for ensuring legal certainty, effective law enforcement, and protection of human rights in the global digital era.

Article History
Received 2025-10-17
Revised 2025-11-13
Accepted 2025-12-31

Keywords
Criminal Law, Digital Crime, Cross-Border, Jurisdiction, International Cooperation.

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mengubah secara fundamental pola interaksi sosial, ekonomi, dan hukum di tingkat global. Digitalisasi tidak hanya menciptakan efisiensi dan percepatan aktivitas lintas negara, tetapi juga melahirkan bentuk-bentuk kejahatan baru yang melampaui batas teritorial negara. Kejahatan digital lintas batas negara muncul sebagai fenomena hukum yang kompleks karena dilakukan melalui ruang siber yang tidak mengenal batas geografis, menggunakan infrastruktur global, serta melibatkan pelaku, korban, dan dampak yang tersebar di berbagai yurisdiksi. Kondisi ini menantang fondasi klasik hukum pidana yang sejak awal dibangun atas asumsi ruang fisik dan kedaulatan teritorial.

Kejahatan ekonomi digital transnasional menjadi salah satu manifestasi paling nyata dari perubahan tersebut. Modus operandi seperti pencucian uang berbasis teknologi, penipuan elektronik, carding, business email compromise, dan penipuan telekomunikasi menunjukkan tingkat adaptasi pelaku kejahatan yang sangat tinggi terhadap perkembangan teknologi (Djunarjanto et al., 2025; Kamilah, 2024; Qiu, 2024). Kejahatan-kejahatan ini tidak lagi bergantung pada kehadiran fisik pelaku di wilayah negara tertentu. Aktivitas kriminal dapat dilakukan dari satu negara, menggunakan server di negara lain, dan menimbulkan kerugian di berbagai yurisdiksi sekaligus. Akibatnya, mekanisme hukum pidana nasional sering kali kehilangan daya jangkau dan efektivitasnya.

Dari perspektif kriminologi, teknologi informasi berperan sebagai faktor kriminogenik yang memperluas peluang kejahatan sekaligus menurunkan risiko tertangkapnya pelaku. Infrastruktur digital menyediakan anonimitas, kecepatan, dan skala yang tidak pernah ada

How to cite: Nurhakim, A., Fauzan, A., Sibawaeh, M. (2025). Paradigma Baru Hukum Pidana dalam Menangani Kejahatan Digital Lintas Batas Negara. *SIMPUL: Jurnal Ilmu Politik dan Hukum, 1*(4), 121-128. https://doi.org/10.71094/simpul.v1i4.319

sebelumnya, sehingga memperbesar proliferasi kejahatan siber lintas negara (Maldonado Ruiz, 2025). Dalam konteks ini, kejahatan digital tidak dapat lagi dipandang sebagai penyimpangan individual semata, tetapi sebagai fenomena struktural yang terkait erat dengan globalisasi ekonomi dan integrasi teknologi global. Hukum pidana dituntut untuk merespons fenomena tersebut secara lebih adaptif dan progresif.

Namun demikian, paradigma hukum pidana konvensional masih sangat bergantung pada prinsip teritorialitas. Prinsip ini mengaitkan kewenangan negara untuk mengadili kejahatan dengan lokasi terjadinya tindak pidana. Dalam konteks kejahatan digital, prinsip tersebut sering kali menjadi sumber ketidakpastian hukum. Penentuan locus delicti dan tempus delicti menjadi problematis karena perbuatan, alat, dan akibat kejahatan terjadi secara simultan di ruang digital yang tersebar (Marsudianto & Israhadi, 2025). Ketidakpastian ini berdampak langsung pada kesulitan penegakan hukum, mulai dari penyelidikan, penuntutan, hingga pembuktian di pengadilan.

Keterbatasan paradigma konvensional ini telah lama disoroti dalam literatur hukum siber. Brenner (2004) menegaskan bahwa model penegakan hukum tradisional yang berbasis wilayah fisik tidak lagi memadai untuk menghadapi kejahatan di ruang siber. Ia mengusulkan perlunya model hukum pidana baru yang secara khusus dirancang untuk cyberspace, dengan menekankan kolaborasi lintas sektor dan lintas negara. Pandangan ini diperkuat oleh Jones dan Choo (2014a; 2014b) yang mempertanyakan kecukupan hukum pidana yang ada dan mengusulkan pembentukan badan hukum baru bagi ruang siber. Argumen tersebut menegaskan bahwa kejahatan digital lintas batas negara bukan sekadar variasi dari kejahatan konvensional, melainkan fenomena hukum yang memerlukan pendekatan paradigmatik baru.

Masalah yurisdiksi menjadi isu sentral dalam penanganan kejahatan digital lintas batas. Sistem hukum nasional cenderung memiliki batas kewenangan yang jelas, sementara kejahatan digital beroperasi secara transnasional. Ketegangan antara yurisdiksi nasional dan karakter global kejahatan siber menimbulkan fragmentasi penegakan hukum dan berpotensi menciptakan ruang impunitas bagi pelaku (Dragojlović, 2023). Tantangan ini semakin kompleks ketika dikaitkan dengan prinsip due process dan perlindungan hak asasi manusia. Upaya penegakan hukum lintas negara sering kali dihadapkan pada perbedaan standar pembuktian, perlindungan data pribadi, dan prosedur peradilan pidana (AllahRakha, 2025; Erikha & Saptomo, 2024).

Dalam praktiknya, kerja sama internasional menjadi instrumen utama untuk mengatasi keterbatasan yurisdiksi nasional. Namun, mekanisme kerja sama seperti mutual legal assistance sering kali berjalan lambat dan tidak sebanding dengan kecepatan kejahatan digital (Flora et al., 2024). Kesenjangan waktu ini berdampak pada hilangnya bukti elektronik dan melemahnya peluang penegakan hukum yang efektif. Kondisi tersebut menunjukkan bahwa persoalan kejahatan digital lintas batas tidak dapat diselesaikan hanya dengan penyesuaian prosedural, tetapi membutuhkan pembaruan paradigma hukum pidana secara menyeluruh.

Perkembangan terbaru di tingkat regional dan global menunjukkan adanya upaya untuk merespons tantangan tersebut. Di Uni Eropa, misalnya, terjadi pergeseran paradigma kerja sama yudisial melalui regulasi akses lintas batas terhadap bukti elektronik yang melibatkan penyedia layanan digital secara langsung (Sachoulidou, 2024). Model ini menandai perubahan signifikan dari pendekatan tradisional yang sepenuhnya bergantung pada kerja sama antarnegara. Meski demikian, model tersebut juga menimbulkan pertanyaan baru terkait privatisasi fungsi penegakan hukum dan perlindungan hak fundamental.

Secara teoretis, kejahatan digital lintas batas dapat dipahami sebagai bagian dari kejahatan transnasional modern yang lahir dari globalisasi. Sornarajah (2006) memandang kejahatan transnasional sebagai cabang baru dalam hukum pidana yang didorong oleh kepentingan global, bukan semata-mata kepentingan moral atau keamanan negara tertentu. Perspektif ini relevan untuk memahami bahwa respons hukum terhadap kejahatan digital tidak dapat bersifat unilateral. Diperlukan kerangka normatif yang lebih harmonis dan terkoordinasi di tingkat internasional.

Sejalan dengan itu, kajian tentang transformasi yurisdiksi pidana menunjukkan adanya pergeseran konseptual dari pendekatan teritorial menuju pendekatan yang lebih fleksibel dan fungsional. Hernández et al. (2020) menekankan bahwa perubahan sifat kejahatan menuntut rekonstruksi konsep yurisdiksi pidana, termasuk batasan kewenangan negara dan mekanisme

pengawasan terhadap penggunaan kewenangan tersebut. Tanpa rekonstruksi konseptual, hukum pidana berisiko tertinggal jauh dari realitas kejahatan digital.

Di tingkat global, perdebatan mengenai kebutuhan akan kerangka hukum cybercrime yang terharmonisasi terus berlangsung. Watney (2012) dan Nduka dan Basdeo (2022) menyoroti urgensi pembentukan regulasi global atau setidaknya harmonisasi hukum nasional untuk mencegah fragmentasi dan konflik yurisdiksi. Tanpa kerangka bersama, penegakan hukum siber akan terus menghadapi hambatan struktural yang melemahkan efektivitasnya. Krishna (2024) menambahkan bahwa strategi regulasi yang inovatif diperlukan untuk menyeimbangkan kepentingan keamanan, hak asasi manusia, dan perkembangan teknologi.

Dalam konteks tersebut, penelitian ini berangkat dari kesadaran bahwa persoalan utama kejahatan digital lintas batas negara terletak pada ketidaksesuaian antara karakter kejahatan dan paradigma hukum pidana yang digunakan untuk menanganinya. Rumusan masalah penelitian ini adalah bagaimana keterbatasan paradigma hukum pidana konvensional dalam menangani kejahatan digital lintas batas negara, bagaimana tantangan yurisdiksi dan pembuktian yang dihadapi, serta bagaimana konsep paradigma baru hukum pidana yang relevan dan adaptif terhadap karakter kejahatan digital transnasional.

Tujuan penelitian ini adalah untuk menganalisis secara kritis paradigma hukum pidana yang berlaku saat ini dan merumuskan kerangka konseptual paradigma baru yang mampu menjawab tantangan kejahatan digital lintas batas negara. Kebaruan penelitian ini terletak pada integrasi analisis hukum pidana, hukum internasional, dan perkembangan teknologi forensik digital dalam satu kerangka normatif yang utuh. Penelitian ini tidak hanya menyoroti kebutuhan reformasi normatif, tetapi juga menekankan rekonstruksi paradigma hukum pidana sebagai fondasi penanganan kejahatan digital di era global.

2. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif yang bertujuan untuk mengkaji dan menganalisis norma hukum, prinsip, dan konsep yang relevan dengan penanganan kejahatan digital lintas batas negara. Pendekatan normatif dipilih karena fokus penelitian terletak pada evaluasi paradigma hukum pidana, konstruksi konseptual, serta perumusan kerangka normatif yang adaptif terhadap perkembangan kejahatan digital transnasional. Penelitian ini tidak berorientasi pada pengumpulan data empiris lapangan, melainkan pada analisis mendalam terhadap bahan hukum dan literatur ilmiah yang relevan.

Pendekatan pertama yang digunakan adalah pendekatan perundang-undangan. Pendekatan ini dilakukan dengan mengkaji berbagai regulasi hukum pidana nasional dan internasional yang berkaitan dengan cybercrime, yurisdiksi pidana, dan kerja sama lintas negara. Analisis difokuskan pada bagaimana hukum positif mengatur kewenangan negara dalam menangani kejahatan digital serta sejauh mana aturan tersebut mampu menjawab tantangan karakter kejahatan lintas batas. Pendekatan ini penting untuk mengidentifikasi kesenjangan normatif dan disharmoni regulasi yang sering menjadi hambatan penegakan hukum (Flora et al., 2024; Erikha & Saptomo, 2024).

Pendekatan kedua adalah pendekatan konseptual. Pendekatan ini digunakan untuk mengkaji teori dan konsep hukum pidana, hukum siber, dan hukum pidana transnasional yang berkembang dalam literatur akademik. Konsep-konsep seperti hukum pidana cyberspace, kejahatan transnasional, dan transformasi yurisdiksi pidana dianalisis secara kritis untuk memahami landasan teoretis paradigma baru hukum pidana (Brenner, 2004; Sornarajah, 2006; Hernández et al., 2020). Pendekatan konseptual memungkinkan penelitian ini untuk tidak terjebak pada deskripsi normatif semata, tetapi mampu menawarkan konstruksi pemikiran yang bersifat preskriptif.

Pendekatan ketiga adalah pendekatan komparatif. Pendekatan ini dilakukan dengan membandingkan model penanganan kejahatan digital lintas batas di berbagai konteks hukum, baik nasional maupun regional. Perbandingan dilakukan terhadap kebijakan kerja sama internasional, mekanisme akses bukti elektronik, dan penerapan yurisdiksi ekstrateritorial (Sachoulidou, 2024; Ba'abud & Heriyanto, 2024). Melalui pendekatan komparatif, penelitian ini berupaya mengidentifikasi praktik terbaik yang dapat menjadi rujukan dalam merumuskan paradigma hukum pidana yang lebih efektif.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi prinsip-prinsip dasar hukum pidana dan hukum internasional yang relevan dengan yurisdiksi dan penegakan hukum siber. Bahan hukum sekunder mencakup buku, artikel jurnal, dan prosiding ilmiah yang membahas kejahatan digital, hukum pidana transnasional, dan reformasi hukum siber (Djunarjanto et al., 2025; AllahRakha, 2025; Krishna, 2024). Bahan hukum tersier digunakan secara terbatas untuk memperjelas terminologi dan konsep yang digunakan dalam analisis.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan secara sistematis. Literatur dipilih berdasarkan relevansi dengan topik penelitian, reputasi publikasi, dan kontribusi teoretisnya terhadap diskursus hukum pidana dan kejahatan digital. Setiap sumber dianalisis secara kritis untuk mengidentifikasi argumen utama, pendekatan metodologis, dan implikasi normatifnya. Proses ini bertujuan untuk memastikan bahwa analisis yang dihasilkan bersifat komprehensif dan berimbang.

Analisis bahan hukum dilakukan dengan metode kualitatif melalui penafsiran hukum dan argumentasi yuridis. Penafsiran dilakukan terhadap norma dan konsep hukum untuk memahami makna dan implikasinya dalam konteks kejahatan digital lintas batas. Argumentasi yuridis digunakan untuk mengaitkan temuan-temuan literatur dengan tujuan penelitian, serta untuk menyusun rekomendasi konseptual mengenai paradigma baru hukum pidana. Analisis ini juga melibatkan sintesis berbagai pandangan akademik guna membangun kerangka normatif yang koheren.

Tahap akhir analisis diarahkan pada konstruksi paradigma baru hukum pidana dalam menangani kejahatan digital lintas batas negara. Konstruksi ini didasarkan pada hasil evaluasi terhadap keterbatasan paradigma konvensional dan praktik penegakan hukum yang ada. Dengan mengintegrasikan perspektif hukum pidana, hukum internasional, dan perkembangan teknologi forensik digital, penelitian ini berupaya menawarkan kerangka pemikiran yang adaptif, realistis, dan relevan dengan tantangan kejahatan digital di era global.

3. Hasil dan Pembahasan

Hasil penelitian ini menunjukkan bahwa kejahatan digital lintas batas negara tidak lagi dapat dipahami dalam kerangka hukum pidana konvensional yang berorientasi pada ruang fisik dan kedaulatan teritorial. Analisis terhadap bahan hukum dan literatur yang dikaji mengonfirmasi adanya ketimpangan mendasar antara karakteristik kejahatan digital dan paradigma hukum pidana yang selama ini digunakan untuk menanganinya. Ketimpangan ini tercermin dalam tiga aspek utama, yaitu sifat transnasional kejahatan digital, keterbatasan konsep yurisdiksi pidana, dan ketidakcukupan mekanisme pembuktian serta kerja sama internasional.

Kejahatan digital lintas batas negara berkembang seiring dengan intensifikasi penggunaan teknologi informasi dalam aktivitas ekonomi dan sosial global. Penelitian Djunarjanto et al. (2025) menunjukkan bahwa kejahatan ekonomi digital transnasional mengalami transformasi signifikan baik dari segi modus operandi maupun kompleksitas teknisnya. Pelaku memanfaatkan celah regulasi, perbedaan sistem hukum, dan keterbatasan kapasitas penegak hukum untuk menghindari pertanggungjawaban pidana. Temuan ini sejalan dengan analisis Maldonado Ruiz (2025) yang menegaskan bahwa teknologi informasi berfungsi sebagai faktor kriminogenik yang memperluas peluang kejahatan sekaligus memperkecil risiko deteksi.

Hasil kajian terhadap literatur juga menunjukkan bahwa kejahatan digital lintas batas tidak berdiri sebagai fenomena tunggal, melainkan sebagai spektrum kejahatan yang saling berkaitan. Carding, penipuan telekomunikasi, pencurian data pribadi, dan pencucian uang digital merupakan bagian dari ekosistem kejahatan siber transnasional yang terorganisasi (Kamilah, 2024; Qiu, 2024). Karakter lintas batas dari kejahatan-kejahatan tersebut memperlihatkan bahwa hukum pidana nasional yang bersifat parsial dan terfragmentasi tidak mampu merespons ancaman secara komprehensif.

Dari perspektif yurisdiksi pidana, hasil penelitian ini menguatkan temuan Marsudianto dan Israhadi (2025) mengenai ketidakpastian locus delicti dan tempus delicti dalam kejahatan siber. Analisis normatif menunjukkan bahwa penentuan tempat dan waktu terjadinya tindak pidana menjadi kabur ketika perbuatan dilakukan melalui jaringan global yang melibatkan

banyak negara. Ketidakpastian ini berdampak langsung pada penentuan kewenangan penegakan hukum dan forum peradilan yang berhak mengadili perkara. Dalam praktiknya, kondisi ini sering kali dimanfaatkan oleh pelaku kejahatan untuk menciptakan konflik yurisdiksi atau bahkan menghindari proses hukum sama sekali.

Temuan ini memperkuat argumen Brenner (2004) yang menyatakan bahwa hukum pidana konvensional dirancang untuk dunia fisik dan tidak mampu beradaptasi secara optimal dengan realitas ruang siber. Hukum pidana tradisional mengasumsikan keterkaitan langsung antara perbuatan pidana dan wilayah negara tertentu. Dalam kejahatan digital lintas batas, asumsi tersebut tidak lagi relevan. Jones dan Choo (2014a; 2014b) bahkan menilai bahwa kondisi ini menuntut pembentukan kerangka hukum baru bagi ruang siber, karena pendekatan konvensional hanya menghasilkan respons yang reaktif dan tidak sistemik.

Hasil analisis juga menunjukkan bahwa pendekatan yurisdiksi nasional yang terfragmentasi menciptakan kesenjangan penegakan hukum di tingkat global. Dragojlović (2023) menegaskan bahwa meskipun beberapa negara telah menerapkan prinsip yurisdiksi ekstrateritorial, penerapannya masih bersifat terbatas dan tidak konsisten. Penelitian ini menemukan bahwa yurisdiksi ekstrateritorial sering kali terhambat oleh perbedaan standar hukum, kepentingan politik, dan ketiadaan mekanisme koordinasi yang efektif. Kondisi ini menguatkan temuan AllahRakha (2025) bahwa fragmentasi yurisdiksi berpotensi melemahkan due process dan merugikan korban kejahatan digital.

Dalam konteks kerja sama internasional, hasil penelitian menunjukkan bahwa mekanisme yang ada belum mampu mengimbangi dinamika kejahatan digital. Mutual legal assistance yang menjadi instrumen utama kerja sama lintas negara sering kali berjalan lambat dan birokratis (Flora et al., 2024). Prosedur formal yang panjang menyebabkan keterlambatan dalam pengumpulan bukti elektronik yang bersifat volatil. Bukti digital dapat dengan mudah dihapus, dimodifikasi, atau dipindahkan ke yurisdiksi lain sebelum permintaan bantuan hukum diproses. Hal ini mengonfirmasi bahwa tantangan kejahatan digital lintas batas bukan hanya bersifat normatif, tetapi juga operasional.

Hasil kajian terhadap perkembangan regulasi di tingkat regional menunjukkan adanya upaya untuk menjawab tantangan tersebut melalui pendekatan yang lebih adaptif. Sachoulidou (2024) mengungkapkan bahwa Uni Eropa telah mengadopsi model kerja sama baru dalam akses bukti elektronik lintas batas yang melibatkan penyedia layanan digital secara langsung. Model ini merepresentasikan pergeseran paradigma dari kerja sama antarnegara menuju kerja sama yang lebih fungsional dan berbasis kebutuhan penegakan hukum. Penelitian ini menilai bahwa pendekatan tersebut memiliki potensi untuk meningkatkan efektivitas penegakan hukum, meskipun tetap menimbulkan persoalan baru terkait perlindungan hak privasi dan akuntabilitas aktor non-negara.

Dari perspektif teori hukum pidana, hasil penelitian menunjukkan bahwa kejahatan digital lintas batas negara sejalan dengan konsep kejahatan transnasional modern. Sornarajah (2006) menyatakan bahwa kejahatan transnasional merupakan cabang baru hukum pidana yang lahir dari globalisasi dan menuntut respons hukum yang bersifat kolektif. Analisis ini menemukan bahwa kejahatan digital lintas batas tidak dapat diatasi melalui pendekatan nasional yang terisolasi. Diperlukan kerangka normatif yang mengakui kepentingan global dan mendorong harmonisasi hukum pidana antarnegara.

Kajian terhadap literatur mengenai transformasi yurisdiksi pidana memperlihatkan bahwa paradigma hukum pidana sedang berada dalam fase transisi. Hernández et al. (2020) menekankan bahwa perubahan sifat kejahatan menuntut rekonstruksi konsep yurisdiksi, termasuk redefinisi batas kewenangan negara dan mekanisme pengawasan. Hasil penelitian ini mendukung pandangan tersebut dengan menunjukkan bahwa tanpa rekonstruksi konseptual, upaya reformasi hukum pidana akan bersifat tambal sulam dan tidak menyentuh akar permasalahan.

Di tingkat global, hasil penelitian juga menegaskan urgensi harmonisasi hukum cybercrime. Watney (2012) dan Nduka dan Basdeo (2022) mengemukakan bahwa absennya kerangka hukum global yang seragam menciptakan fragmentasi regulasi dan konflik yurisdiksi. Penelitian ini menemukan bahwa perbedaan definisi cybercrime, standar pembuktian, dan prosedur penegakan hukum antarnegara memperbesar peluang impunitas

bagi pelaku. Harmonisasi hukum pidana global dipandang sebagai prasyarat penting untuk membangun respons yang efektif terhadap kejahatan digital lintas batas.

Hasil penelitian juga menyoroti pentingnya keseimbangan antara penegakan hukum dan perlindungan hak asasi manusia. Erikha dan Saptomo (2024) menekankan bahwa kebijakan hukum siber harus mampu menyeimbangkan kebutuhan akses data bagi penegak hukum dengan perlindungan privasi individu. Analisis penelitian ini menunjukkan bahwa paradigma baru hukum pidana tidak boleh hanya berorientasi pada efektivitas penegakan hukum, tetapi juga harus menjamin legitimasi dan akuntabilitas. Tanpa perlindungan hak asasi manusia, upaya penegakan hukum berisiko menimbulkan pelanggaran yang merusak kepercayaan publik.

Dalam konteks kejahatan ekonomi digital, hasil penelitian menunjukkan bahwa integrasi hukum pidana dengan teknologi forensik siber merupakan kebutuhan yang tidak terelakkan. Djunarjanto et al. (2025) menegaskan bahwa pembuktian kejahatan digital membutuhkan kompetensi teknis dan pendekatan multidisipliner. Penelitian ini menemukan bahwa paradigma hukum pidana yang baru harus mengakomodasi perkembangan teknologi forensik sebagai bagian integral dari sistem pembuktian. Tanpa integrasi tersebut, hukum pidana akan terus tertinggal dari inovasi kejahatan digital.

Hasil penelitian juga mengonfirmasi bahwa pendekatan yurisdiksi ekstrateritorial memiliki potensi signifikan dalam menangani kejahatan digital lintas batas, khususnya dalam kasus pelanggaran data pribadi. Ba'abud dan Heriyanto (2024) menunjukkan bahwa penerapan yurisdiksi ekstrateritorial dapat memperluas jangkauan hukum pidana nasional. Namun, penelitian ini menekankan bahwa penerapan tersebut harus didukung oleh kerja sama internasional yang kuat dan standar normatif yang jelas untuk menghindari konflik yurisdiksi dan pelanggaran kedaulatan.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa kejahatan digital lintas batas negara menuntut perubahan paradigma hukum pidana yang bersifat mendasar. Paradigma baru tersebut harus melampaui pendekatan teritorial sempit dan mengadopsi perspektif transnasional yang lebih fleksibel. Brenner (2004) dan Jones dan Choo (2014b) menegaskan bahwa hukum pidana cyberspace harus dirancang untuk mencegah kejahatan secara proaktif, bukan sekadar merespons setelah kejahatan terjadi. Penelitian ini mendukung pandangan tersebut dengan menunjukkan bahwa pencegahan dan kerja sama internasional merupakan elemen kunci dalam paradigma baru hukum pidana.

Pembahasan ini juga menunjukkan bahwa paradigma baru hukum pidana tidak dapat berdiri sendiri tanpa dukungan regulasi global dan regional yang harmonis. Krishna (2024) menekankan bahwa strategi regulasi inovatif diperlukan untuk menghadapi tantangan kejahatan digital yang terus berkembang. Penelitian ini menyimpulkan bahwa inovasi regulasi harus disertai dengan reformasi institusional dan peningkatan kapasitas penegak hukum. Tanpa pendekatan holistik, paradigma baru hukum pidana berisiko menjadi konsep normatif tanpa implementasi efektif.

Dengan demikian, hasil dan pembahasan penelitian ini menegaskan bahwa kejahatan digital lintas batas negara merupakan ujian serius bagi hukum pidana modern. Keterbatasan paradigma konvensional, fragmentasi yurisdiksi, dan lemahnya kerja sama internasional menunjukkan perlunya rekonstruksi paradigma hukum pidana yang lebih adaptif, transnasional, dan berorientasi pada perlindungan kepentingan global. Paradigma baru hukum pidana yang diusulkan dalam penelitian ini bertumpu pada integrasi hukum pidana nasional dan internasional, harmonisasi regulasi, penguatan teknologi forensik digital, serta keseimbangan antara efektivitas penegakan hukum dan perlindungan hak asasi manusia.

4. Kesimpulan

Penelitian ini menyimpulkan bahwa kejahatan digital lintas batas negara merupakan tantangan fundamental bagi keberlakuan dan efektivitas hukum pidana modern. Karakter kejahatan yang bersifat transnasional, berbasis teknologi, dan tidak terikat ruang fisik telah menimbulkan ketimpangan serius antara realitas empiris kejahatan digital dan paradigma hukum pidana konvensional yang masih berorientasi teritorial. Ketimpangan tersebut tercermin dalam ketidakpastian yurisdiksi, lemahnya mekanisme penegakan hukum lintas

negara, serta keterbatasan sistem pembuktian dalam menghadapi bukti elektronik yang dinamis dan mudah berubah.

Hasil penelitian menunjukkan bahwa pendekatan hukum pidana nasional yang parsial dan terfragmentasi tidak lagi memadai untuk merespons kompleksitas kejahatan digital lintas batas. Penegakan hukum yang bergantung pada batas wilayah negara menghadapi hambatan struktural ketika kejahatan dilakukan melalui jaringan global yang melibatkan banyak yurisdiksi. Kondisi ini membuka ruang impunitas bagi pelaku dan melemahkan perlindungan hukum bagi korban. Oleh karena itu, dibutuhkan rekonstruksi paradigma hukum pidana yang mampu melampaui batas teritorial tanpa mengabaikan prinsip kedaulatan dan perlindungan hak asasi manusia.

Penelitian ini menegaskan bahwa paradigma baru hukum pidana harus bersifat transnasional, adaptif, dan berbasis kerja sama internasional yang efektif. Harmonisasi regulasi, penguatan yurisdiksi ekstrateritorial yang terukur, serta integrasi teknologi forensik digital menjadi elemen kunci dalam membangun sistem penegakan hukum yang responsif terhadap kejahatan digital lintas batas. Selain itu, keseimbangan antara efektivitas penegakan hukum dan perlindungan hak privasi harus menjadi prinsip utama agar legitimasi hukum tetap terjaga.

Dengan demikian, kejahatan digital lintas batas negara bukan sekadar persoalan teknis penegakan hukum, tetapi merupakan isu struktural yang menuntut perubahan paradigma hukum pidana secara menyeluruh. Tanpa reformasi konseptual dan institusional yang berkelanjutan, hukum pidana akan terus tertinggal dari perkembangan kejahatan digital dan kehilangan daya gunanya dalam melindungi kepentingan hukum masyarakat global.

Daftar Pustaka

Al-Abdali, M., Al-Nasrawi, H., Muslim, H., et al. (2025). Al-mas'ūliyyah 'an al-jarā'im al-ilikturūniyyah al-'ābirah lil-ḥudūd wafqan li-qawā'id al-qānūn al-duwalī. Ādāb al-Kūfaẗ, 1(65). https://doi.org/10.36317/kja/2025/v1.i65.20035

AllahRakha, N. (2025). Cross-border e-crimes: Jurisdiction and due process challenges. Adliya: Jurnal Hukum dan Kemanusiaan, 18(2), 201–220. https://doi.org/10.15575/adliya.v18i2.38633

Ba'abud, M. F. R., & Heriyanto, D. S. N. (2024). Application of the principles of extraterritorial jurisdiction towards personal data breach committed cross-country borders. Uti Possidetis, 5(1), 1–14. https://doi.org/10.22437/up.v5i1.28300

Brenner, S. W. (2004). Toward a criminal law for cyberspace: A new model of law enforcement? Rutgers Computer and Technology Law Journal, 30(1), 1–47.

Djunarjanto, A. A., Purwati, A. A., & Marina, L. (2025). Transformasi modus kejahatan ekonomi transnasional di era digital: Analisis hukum pidana dan teknik forensik siber. Sentri, 4(8). https://doi.org/10.55681/sentri.v4i8.4448

Dragojlović, J. (2023). Jurisdiction for criminal offenses of cybercrime: International and national standards. Pravo, 57(1), 23–39. https://doi.org/10.5937/ptp2300063d

Erikha, A., & Saptomo, A. (2024). Dilemma of legal policy to address cybercrime in the digital era. Asian Journal of Social and Humanities, 3(3), 301–318. https://doi.org/10.59888/ajosh.v3i3.452

Flora, H. S., Maharjan, K., Mark, E., et al. (2024). Reform of criminal procedure law in dealing with transnational cyber crime. Rechtsnormen, 2(3), 145–162. https://doi.org/10.70177/rjl.v2i3.1293

Hernández, G., et al. (2020). Transformations in criminal jurisdiction. Bloomsbury Publishing. https://doi.org/10.5040/9781509954254

Jones, D., & Choo, K.-K. R. (2014). Should there be a new body of law for cyber space. In Proceedings of the International Conference on Cybercrime (pp. 1–10).

Jones, D., & Choo, K.-K. R. (2014). Should there be a new body of law for cyber space. Social Science Research Network. https://ssrn.com/abstract=2437445

Kamilah, A. (2024). Carding sebagai cyber crime dan penegakan hukumnya melalui tort dalam perspektif hukum perdata internasional. Jurnal Hukum Mimbar Justitia, 10(2), 215–230. https://doi.org/10.35194/jhmj.v10i2.4841

Krishna, L. S. (2024). Navigating legal frontiers: Contemporary challenges and regulatory strategies in combating cybercrime. International Journal for Research Publication and Seminar, 15(1), 166–182. https://doi.org/10.36676/jrps.v15.i1.1667

Maldonado Ruiz, L. M. (2025). Elementos criminógenos de las tecnologías de la información y proliferación de la delincuencia informática. Investigación Tecnología e Innovación, 17(23), 55–70. https://doi.org/10.53591/iti.v17i23.1945

Marsudianto, D. N., & Israhadi, E. (2025). Uncertainty of locus delicti and tempus delicti as an obstacle to law enforcement against cybercrime. Global Indonesian Journal of Law and Social Sciences, 3(2), 98–113. https://doi.org/10.38035/gijlss.v3i2.404

Nduka, R., & Basdeo, V. (2022). The need for harmonised and specialised global legislation to address the growing spectre of cybercrime. Southern African Public Law, 37(1), 45–63. https://doi.org/10.25159/2522-6800/8112

Qiu, M. (2024). Research on the criminal law response to telecom fraud in the digital society. Economics, Law and Policy, 7(3), 33–49. https://doi.org/10.22158/elp.v7n3p33

Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of judicial cooperation. New Journal of European Criminal Law, 15(2), 180–197. https://doi.org/10.1177/20322844241258649

Sornarajah, M. (2006). Transnational crimes: The third limb of the criminal law. Social Science Research Network. https://ssrn.com/abstract=955099

Watney, M. (2012). Cybercrime regulation at a cross-road: State and transnational laws versus global laws. In Proceedings of the International Cyberlaw Conference (pp. 1–12).