IUSTITIA OMNIBUS
JURNAL ILMU HUKUM
eISSN 2716-277X
pISSN 2716-1455

Iustitia Omnibus: Jurnal Ilmu Hukum
Volume 6, Number 2, 2025 pp. 60-68
P-ISSN: 2716-1455 E-ISSN: 2716-277X
Open Access: http://jurnal-pasca.unla.ac.id/index.php/iustitiaomnibus/index

Kajian Terhadap Kejahatan Carding Sebagai Bentuk Cybercrime Di Indonesia

Alamsyah[1*], Edy Santoso[2], Nugraha Pranadita[3]
[1,2,3]Pascasarjana, Universitas Langlangbuana, Bandung, Indonesia
e-mail: *alawfirm.webs@gmail.com

ARTICLE INFO

Article history:
Received July, 2025
Revised July, 2025
Accepted July, 2025
Available online July, 2025

Kata Kunci:
Cybercrime, Kejahatan Carding, Teknologi Digital, Penegakan Hukum

Keywords:
Cybercrime, Carding Crime, Digital Technology, Law Enforcement

ABSTRAK

Keamanan digital dan perlindungan terhadap kejahatan siber, khususnya carding, menjadi isu penting di era transformasi teknologi informasi saat ini. Penelitian ini bertujuan menelaah efektivitas kerangka hukum Indonesia dalam menangani kejahatan carding sebagai bentuk cybercrime. Metode yang digunakan adalah yuridis normatif, dengan studi kepustakaan terhadap norma hukum positif, peraturan perundang-undangan, jurnal, dan dokumen relevan. Data dianalisis secara kualitatif dengan pendekatan deskriptif analitis, menelaah aspek regulasi, implementasi, dan hambatan penegakan hukum. Hasil penelitian menunjukkan bahwa efektivitas penegakan hukum Indonesia masih rendah karena absennya regulasi khusus terhadap carding, sehingga banyak kasus sulit diusut dan diproses secara maksimal. Ketidakcukupan kapasitas aparat dalam teknologi digital forensik dan kerjasama internasional yang belum optimal memperkuat tantangan tersebut. Oleh karena itu, direkomendasikan reformasi hukum berbasis teknologi, peningkatan kapasitas penegak hukum, dan kerja sama internasional yang lebih intensif. Penguatan regulasi, edukasi masyarakat, dan penggunaan teknologi canggih dianggap kunci untuk menciptakan sistem transaksi digital yang aman, adil, dan mampu menanggulangi kejahatan carding secara efektif di Indonesia.

ABSTRACT

Digital security and protection against cybercrime, particularly carding, have become critical issues in the era of information technology transformation. This study aims to examine the effectiveness of Indonesia's legal framework in addressing carding as a form of cybercrime. The method used is normative juridical research, employing literature studies on positive legal norms, laws and regulations, academic journals, and relevant documents. The data were analysed qualitatively using a descriptive-analytical approach, focusing on regulatory aspects, implementation, and enforcement challenges. The findings indicate that the effectiveness of law enforcement in Indonesia remains low due to the absence of specific regulations on carding, making many cases difficult to investigate and prosecute effectively. The lack of digital forensic capabilities among law enforcement and suboptimal international cooperation further exacerbates these challenges. Therefore, the study recommends legal reforms based on technological advancements, capacity building for law enforcement officers, and more intensive international collaboration. Strengthening regulations, public education, and the use of advanced technologies are considered key to creating a secure, fair, and effective digital transaction system capable of combating carding crimes in Indonesia.

PENDAHULUAN

Negara Indonesia merupakan negara hukum sebagaimana tercantum dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 hasil amandemen ketiga, dan diperkuat melalui Pasal 27 ayat (1) UUD 1945, yang menegaskan bahwa semua warga negara memiliki kedudukan yang sama di hadapan hukum dan pemerintahan tanpa kecuali. Konsep negara hukum yang dianut Indonesia merupakan cerminan dari negara hukum modern (*modern rechtsstaat*), yang tidak hanya menjamin ketertiban dan keamanan hukum, tetapi juga memberikan perlindungan terhadap hak asasi dan kesejahteraan masyarakat. Dalam konteks ini, hukum tidak hanya berfungsi sebagai instrumen normatif, tetapi juga sebagai sistem yang dinamis dan adaptif terhadap perkembangan sosial, termasuk perubahan akibat kemajuan teknologi informasi dan komunikasi.

Seiring dengan laju perkembangan teknologi digital, bentuk-bentuk kejahatan mengalami transformasi yang signifikan. Fenomena ini melahirkan kategori baru dalam studi hukum pidana, yaitu kejahatan dunia maya (cybercrime), yang melibatkan sistem komputer, jaringan, atau perangkat digital lainnya. Salah satu bentuk cybercrime yang semakin marak adalah carding, yakni pencurian data kartu kredit milik orang lain yang digunakan untuk transaksi daring. Kejahatan ini tidak hanya bersifat lokal, tetapi juga telah berkembang dalam skala transnasional, melibatkan jaringan terorganisir dan penggunaan perangkat lunak canggih untuk menghindari deteksi. Ginara., et al, dijelaskan bahwa kejahatan carding umumnya dilakukan dengan membobol sistem keamanan situs e-commerce, mencuri data kartu kredit secara ilegal, lalu memanfaatkannya untuk transaksi tanpa seizin pemilik kartu, dan tindakan ini telah menjadi pola kejahatan siber yang terstruktur di Indonesia.[1] Nursalam., et al yang mengungkap bahwa praktik carding di Makassar memperlihatkan adanya keterlibatan pelaku lintas negara, penggunaan identitas palsu, hingga transaksi menggunakan metode virtual private network (VPN) dan situs dark web, yang menyulitkan penegakan hukum berbasis yurisdiksi nasional.[2] Dengan demikian, kompleksitas kejahatan ini menuntut adanya pembaruan dalam strategi penanggulangan hukum pidana siber, baik dari sisi regulasi, kapasitas aparat penegak hukum, hingga kerja sama internasional lintas batas negara.

Fenomena *carding* di Indonesia berkembang pesat seiring dengan maraknya transaksi digital dan e-commerce. Saat ini, praktik *carding* telah bertransformasi dari kejahatan konvensional menjadi kejahatan terorganisir berteknologi tinggi, yang memanfaatkan infrastruktur siber canggih. Pelaku atau *carder* sering menggunakan berbagai teknik seperti rekayasa sosial, phishing, hingga infiltrasi malware di situs e-commerce dan *dark web* untuk mencuri data kartu kredit. Studi terbaru mengenai ekosistem *Malware as a Service* (MaaS) menegaskan bahwa pelaku *carding* kini rutin menggunakan botnet dan malware berbasis keyloggers atau information stealers

---

1 I Gede Krisna Ginara, I Made Minggu Widyantara, and Ni Komang Arini Styawati, "Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia," *Jurnal Preferensi Hukum* 3, no. 1 (2022): 138–42, https://doi.org/10.22225/jph.3.1.4673.138-142.

2 Muh. Fandi Nursalam, Ashar Sinilele, and Istiqamah, "Carding Crime in Makassar City: Juridical Review As an Issues of Cybercrime," *Alauddin Law Development Journal* 6, no. 1 (2024): 172–79, https://doi.org/10.24252/aldev.v6i1.22387.

untuk otomatisasi pencurian dan validasi data kartu kredit.[3] Selain itu, database hasil *carding* diperjualbelikan di forum bawah tanah, di mana pelaku membeli "credit card credentials" atau "Fullz" dengan harga bervariasi sesuai kualitas data.[4] Infrastruktur seperti ini memungkinkan *carding* modern menghasilkan kerugian besar bagi individu dan lembaga keuangan. Melihat kondisi tersebut, diperlukan penegakan hukum siber yang dilengkapi dengan teknologi digital forensik, regulasi spesifik untuk *carding*, serta kerja sama lintas yurisdiksi guna menanggulangi kejahatan ini secara efektif.

Dalam kerangka hukum Indonesia, penanggulangan kejahatan *carding* masih menghadapi berbagai tantangan signifikan. Secara normatif, tindak *carding* dapat dikategorikan sebagai pencurian dan penipuan sesuai Pasal 362, 363, dan 378 KUHP. Namun karena kejahatan ini memanfaatkan sarana elektronik, aparat penegak hukum lebih sering menerapkan UU ITE, khususnya Pasal 30 dan Pasal 46 UU No. 11 Tahun 2008 beserta perubahan melalui UU No. 19 Tahun 2016 untuk menjerat akses ilegal ke sistem elektronik. Meskipun demikian, efektivitas yurisdiksi dalam penegakan kasus *cybercrime* di Indonesia masih lemah, karena prosedur hukum eksternal seperti ekstradisi dan mutual legal assistance belum optimal dan sering tidak berjalan sesuai standar internasional.[5] Ketidaksinkronan norma internasional dengan hukum nasional menghambat penanganan pelaku *cybercrime* lintas negara, sehingga banyak kasus *carding* tidak bisa diproses saat pelaku berada di luar negeri.[6] Kendala seperti ini mencerminkan permasalahan mendasar dalam pembuktian digital, yurisdiksi, dan kerjasama internasional faktor yang dibutuhkan untuk menjawab kompleksitas kejahatan *carding* dalam era digital.

Dalam konteks akademik, penelitian mengenai carding di Indonesia sebagian besar masih berfokus pada aspek yuridis formal dan belum banyak mengeksplorasi pendekatan multidisipliner yang mengaitkan antara hukum pidana, keamanan siber, serta kebijakan digital nasional. Ini menciptakan research gap yang penting untuk diisi. Sebagian besar regulasi yang digunakan masih bersifat reaktif dan belum menyentuh aspek pencegahan secara strategis melalui penguatan sistem digital nasional dan edukasi publik mengenai keamanan transaksi elektronik. Oleh karena itu, diperlukan upaya untuk mengintegrasikan pendekatan hukum siber yang lebih progresif dengan perlindungan korban dan penguatan lembaga penegak hukum agar mampu menyesuaikan diri dengan perkembangan teknologi yang sangat dinamis.

Urgensi penelitian ini semakin mengemuka jika melihat tingginya kerugian yang ditimbulkan oleh kejahatan carding dan lemahnya sistem pengawasan transaksi digital di Indonesia. World Economic Forum melaporkan bahwa kejahatan siber,

---

[3] Constantinos Patsakis, David Arroyo, and Fran Casino, "The Malware as a Service Ecosystem," 2025, 371–94, https://doi.org/10.1007/978-3-031-66245-4_16.

[4] Roderic Broadhurst et al., "Malware Trends on 'Darknet' Crypto-Markets: Research Review," *SSRN Electronic Journal*, 2018, https://doi.org/10.2139/ssrn.3226758.

[5] Amanda Fitria Najwa, Aqila Husna, and Aqila Husna, "Efektifitas Yurisdiksi Cybercrime Di Tengah Perkembangan Teknologi Informasi," *Jurnal Hukum Dan Sosial Politik* 2, no. 3 (2024): 126–35, https://doi.org/10.59581/jhsp-widyakarya.v2i3.3426.

[6] Desia Rakhma Banjarani and Muhammad Apriliansyah Rahmadhani, "Cybercrime as Transnational Crime: Law Enforcement and Countermeasure Problems in the Perspective of International Criminal Law," *Yustisia Tirtayasa : Jurnal Tugas Akhir* 4, no. 4 (2024), https://doi.org/10.51825/yta.v4i4.29046.

termasuk carding, diproyeksikan menyebabkan kerugian global hingga USD 10,5 triliun per tahun pada 2025 jika tidak ditanggulangi secara sistemik.[7] Di Indonesia, data dari BSSN dan OJK menunjukkan bahwa serangan siber dengan motif finansial terus meningkat, terutama dalam bentuk pencurian data kartu kredit. Berdasarkan hal tersebut, penelitian ini menjadi penting sebagai upaya untuk mengkaji efektivitas kerangka hukum Indonesia dalam merespons kejahatan carding, serta menyusun strategi hukum yang lebih responsif terhadap tantangan era digital.

Dengan demikian, penelitian ini memiliki kebaharuan dalam mengangkat persoalan carding secara spesifik sebagai objek kajian hukum pidana yang berbasis pada pendekatan teknologi, sekaligus menyoroti kebutuhan akan pembaruan hukum yang lebih adaptif terhadap perkembangan kejahatan digital. Fokus penelitian ini tidak hanya pada tataran normatif, tetapi juga pada praktik implementasi hukum di lapangan, serta kontribusi terhadap penguatan sistem perlindungan hukum di Indonesia terhadap ancaman *cybercrime* yang semakin kompleks.

METODE

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian yang berfokus pada studi terhadap norma hukum positif yang berlaku, khususnya dalam menelaah relevansi aturan dan urgensi penegakan hukum terhadap kejahatan carding sebagai bentuk kejahatan siber, ditinjau dari efektivitas dan pemidanaannya. Spesifikasi penelitian bersifat deskriptif analitis, yakni menggambarkan dan menganalisis ketentuan hukum, teori-teori, serta praktik pelaksanaan hukum yang terkait. Data dikumpulkan melalui studi kepustakaan, mencakup buku, peraturan perundang-undangan, jurnal, dan dokumen hukum lain yang relevan. Analisis dilakukan secara normatif kualitatif, yaitu dengan menguraikan data secara sistematis berdasarkan norma hukum, asas, dan doktrin yang ada. Pendekatan ini dilakukan dengan menjabarkan data berdasarkan norma-norma hukum dan teori yang relevan terhadap pokok persoalan yang diteliti.[8]

HASIL DAN PEMBAHASAN

Kejahatan *carding* di Indonesia mengalami peningkatan signifikan dalam satu dekade terakhir, seiring dengan pertumbuhan ekonomi digital dan penggunaan transaksi non-tunai berbasis kartu kredit atau debit. *Carding* umumnya didefinisikan sebagai tindakan memperoleh dan menggunakan data kartu kredit orang lain secara ilegal, biasanya untuk transaksi online tanpa izin pemilik sah. Modus operandi utama, seperti phishing, malware, social engineering, dan pembelian data melalui marketplace gelap (*dark web*), telah berkembang dari aksi individu menjadi kejahatan terorganisir lintas negara. Marazqah et al, yang menyebutkan bahwa "credit card cyber fraud is a major security risk worldwide… market is predicted to…

---

[7] World Economic Forum, *Global Cybersecurity Outlook 2023* (Geneva: WEF, 2023), https://www.weforum.org/publications/global-cybersecurity-outlook-2023/.

[8] Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat* (Jakarta: Raja Grafindo Persada, 2010).

exceed USD 10.5 trillion annually by 2025".[9] Studi ini menyoroti bahwa bank dan penyedia layanan keuangan perlu mengadopsi teknik deteksi yang canggih karena semakin meningkatnya otomasi serangan dan kerugian global yang besar. Kerugian akibat kejahatan siber termasuk *carding* diperkirakan menimbulkan kerugian tahunan lebih dari USD 10.5 triliun secara global, dengan peningkatan hingga 82% sejak tahun 2021.[10] Temuan ini menggarisbawahi bahwa *carding* kini menjadi kejahatan strategis yang membutuhkan respons hukum dan teknologi yang terintegrasi.

Dalam konteks hukum pidana Indonesia, carding belum memiliki pengaturan yang eksplisit sebagai tindak pidana khusus. Saat ini, kejahatan tersebut dikualifikasikan melalui ketentuan umum seperti Pasal 362 KUHP (pencurian), Pasal 378 KUHP (penipuan), dan Pasal 30 juncto Pasal 46 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016. Dalam praktiknya, penegak hukum lebih banyak menggunakan UU ITE karena kejahatan ini dilakukan melalui akses tidak sah ke sistem elektronik. Namun, rumusan norma dalam UU ITE masih bersifat umum dan tidak secara spesifik menyasar perbuatan pencurian data keuangan atau financial identity theft. Akibatnya, banyak kasus carding yang sulit untuk dijerat secara maksimal karena hambatan dalam pembuktian dan kekaburan dalam unsur delik yang diterapkan.

Dari sudut pandang teori hukum pidana, pendekatan yang digunakan dalam pembahasan ini merujuk pada teori sistem pemidanaan yang dikemukakan oleh Barda Nawawi Arief. Teori ini memandang bahwa sistem pemidanaan merupakan suatu rangkaian yang utuh dan terdiri dari tiga tahap utama, yaitu tahap formulasi (*legislative policy*), aplikasi (*judicial policy*), dan eksekusi (*executive policy*), yang harus berjalan secara terpadu untuk mencapai tujuan pemidanaan yang efektif.[11] Dalam konteks kejahatan carding, ketiga tahap tersebut di Indonesia belum berjalan secara optimal. Pada tahap formulasi, Indonesia masih menghadapi kekosongan hukum yang spesifik dan komprehensif terkait kejahatan carding. UU ITE dan KUHP belum secara eksplisit menyebut carding sebagai bentuk tindak pidana tersendiri, sehingga aparat penegak hukum sering kali menghadapi kendala dalam menentukan pasal yang tepat. Kesenjangan ini diperparah oleh perkembangan teknologi dan modus operandi pelaku carding yang sangat dinamis dan transnasional. Kejahatan siber berkembang lebih cepat daripada kemampuan legislator untuk mengaturnya, menciptakan apa yang disebut sebagai *regulatory lag* dalam sistem hukum pidana.[12] Sistem hukum nasional sering kali tidak mampu merespons kompleksitas kejahatan

---

[9] Eyad Abdel Latif Marazqah Btoush et al., "A Systematic Review of Literature on Credit Card Cyber Fraud Detection Using Machine and Deep Learning," *PeerJ Computer Science* 9 (2023), https://doi.org/10.7717/PEERJ-CS.1278.

[10] Monica Nila Sari, "Cybercrime in Association of Southeast Asian Nations," *Journal of Information Policy* 14 (2024): 568–98, https://doi.org/10.5325/jinfopoli.14.2024.0016.

[11] Barda Nawawi Arief, *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan* (Jakarta: Kencana, 2018).

[12] Anthony Quinn, Louise Cooke, and Mark Monaghan, "An Exploration of the Progress of Open Crime Data: How Do Ongoing Limitations with the Police.Uk Website Restrict a Comprehensive Understanding of Recorded Crime?," *Policing and Society* 29, no. 4 (2019): 455–70, https://doi.org/10.1080/10439463.2017.1397149.

digital secara efektif tanpa kerangka hukum yang adaptif dan berbasis risiko.[13] Oleh karena itu, untuk menghadapi kejahatan seperti carding, diperlukan reformulasi kebijakan kriminal yang bersifat progresif dan antisipatif terhadap perkembangan teknologi.

Negara-negara yang berhasil menanggulangi kejahatan carding umumnya memiliki regulasi khusus yang mengatur tentang pencurian data keuangan atau identitas, serta sistem pemidanaan yang didesain untuk menghadapi kejahatan digital.[14] Hal ini dapat dijumpai pada sistem hukum di Amerika Serikat dengan Identity Theft and Assumption Deterrence Act, atau di Jerman melalui Undang-Undang Perlindungan Data dan Keamanan Informasi. Indonesia, hingga kini, masih menempatkan carding sebagai subkategori dari kejahatan akses ilegal, bukan sebagai tindak pidana tersendiri. Implikasinya adalah pada kelemahan penegakan hukum dalam menyesuaikan norma dengan kompleksitas kejahatan yang terjadi.

Pada tahap aplikasi, efektivitas penegakan hukum juga masih rendah. Aparat penegak hukum seperti penyidik, jaksa, dan hakim masih memiliki keterbatasan dalam pemahaman teknis mengenai kejahatan berbasis digital. Minimnya pelatihan dan kurangnya infrastruktur digital forensik menjadi kendala utama. Sebagian besar penegakan hukum di negara berkembang mengalami kendala dalam pengumpulan dan verifikasi bukti digital, terutama ketika pelaku menggunakan teknik penyamaran seperti VPN, proxy, atau deep web untuk menyembunyikan identitas dan lokasi.[15] Dalam beberapa kasus di Indonesia, pelaku carding sulit dilacak karena berada di luar negeri atau menggunakan identitas palsu yang tidak terdaftar dalam sistem kependudukan nasional.

Lebih lanjut, proses pembuktian dalam tindak pidana carding kerap terhambat karena ketergantungan pada pihak ketiga seperti penyedia layanan hosting luar negeri, platform e-commerce, atau perbankan internasional. Indonesia belum memiliki sistem kerja sama internasional yang kuat dalam pertukaran data digital lintas negara atau *mutual legal assistance (MLA)* yang efisien. Akibatnya, proses hukum berjalan lambat dan sering kali gagal menghasilkan putusan yang memberikan efek jera[16]. Di samping itu, kerangka penegakan hukum siber di Indonesia masih menghadapi berbagai kendala teknis dan koordinatif. Salah satu hambatan utama adalah belum tersedianya standar prosedur penanganan bukti digital (*digital evidence*), sehingga investigasi sering terhambat oleh fragmentasi mekanisme pengumpulan dan pengelolaan bukti.[2] Selain itu, regulasi di bidang perlindungan data pelanggan

---

[13] Bert-Jaap Koops, "Should ICT Regulation Be Technology-Neutral?," 2006, https://doi.org/10.1007/978-90-6704-665-7_4.

[14] Radina Stoykova, "The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations," *Computer Law & Security Review* 49 (2023): 105801, https://doi.org/10.1016/j.clsr.2023.105801.

[15] P. S. Sanjan et al., "Enhancement of Power Quality in Domestic Loads Using Harmonic Filters," *IEEE Access* 8 (2020): 197730–44, https://doi.org/10.1109/ACCESS.2020.3034734.

[16] Muhammad Taufik Rusydi, "Cyber Law Policy Development: Indonesia's Response to International Cybercrime Threats," *Journal of Progressive Law and Legal Studies* 3, no. 01 (2025): 69–85, https://doi.org/10.59653/jplls.v3i01.1365.

perbankan digital dinilai belum memberikan kepastian hukum terhadap tanggung jawab institusi keuangan dalam penanganan data dan kerugian nasabah.[17]

Pada tahap eksekusi, yaitu pelaksanaan pidana, pengadilan cenderung menjatuhkan sanksi yang ringan terhadap pelaku carding, berupa pidana denda atau penjara singkat tidak sebanding dengan dampak ekonomi signifikan yang ditimbulkan bagi korban individu maupun lembaga keuangan. Dalam perspektif **penal policy,** hal ini menunjukkan bahwa pemidanaan sebagai alat perlindungan masyarakat dan pencegahan kejahatan belum berjalan optimal. regulasi pemidanaan di era digital memerlukan strategi berbasis manajemen risiko (*risk-based sanctions*), yang tidak hanya fokus pada pemerosesan represif tetapi juga memperkuat fungsi preventif melalui pengawasan teknologi, pembatasan akses digital, dan sistem peringatan dini terutama pada sistem pembayaran elektronik.[18]

Dari sisi korban, perlindungan hukum terhadap individu yang mengalami kerugian akibat carding juga belum maksimal. UU ITE memang menyebutkan perlindungan terhadap transaksi elektronik dan data pribadi, namun dalam praktiknya korban sering kali tidak mendapatkan restitusi atau kompensasi yang sebanding. Sebagian besar pelaku tidak dapat dijerat atau tidak memiliki kemampuan finansial untuk mengganti kerugian korban. Berdasarkan laporan Interpol Cybercrime Directorate pada tahun 2022, di Asia Tenggara hanya sekitar 15% korban kejahatan finansial digital yang mendapatkan pengembalian dana atau bentuk perlindungan hukum formal. Dalam konteks ini, posisi korban seringkali terpinggirkan, baik dalam proses hukum maupun dalam kebijakan keamanan siber nasional.

Selain itu, perlu dicermati bahwa carding bukan hanya permasalahan hukum pidana, tetapi juga merupakan isu sistemik yang menyangkut keamanan siber nasional. Sistem keamanan transaksi elektronik, enkripsi data, regulasi perbankan digital, hingga kebijakan perlindungan data pribadi, semuanya memiliki peran penting dalam pencegahan carding. Negara-negara seperti Singapura dan Estonia telah menunjukkan bahwa pendekatan holistik antara regulasi, teknologi, dan edukasi publik dapat menurunkan tingkat kejahatan siber secara signifikan. Strategi keamanan siber nasional yang efektif harus mengintegrasikan aspek teknologi perlindungan infrastruktur kritis, desain sistem digital yang aman, serta konektivitas dengan sistem hukum yang tangguh.[19] Pendekatan semacam ini mampu membentuk arsitektur sistem keuangan digital yang tidak hanya efisien, tetapi juga tahan terhadap kejahatan finansial berbasis digital seperti carding.

Dari hasil pembahasan tersebut, jelas bahwa kejahatan carding membutuhkan respons hukum yang lebih dari sekadar penerapan pasal-pasal pidana umum. Diperlukan regulasi khusus yang mengatur tindak pidana pencurian data keuangan secara elektronik, serta sistem pembuktian yang disesuaikan dengan karakteristik

---

[17] Sriono et al., "LEGAL PROTECTION FOR DIGITAL BANK CUSTOMERS IN INDONESIA: ANALYSIS OF DATA CONFIDENTIALITY REGULATIONS AND BANK RESPONSIBILITY," *LITIGASI* 25, no. 2 (January 2024): 301–30, https://doi.org/10.23969/litigasi.v25i2.18538.

[18] Williams Haruna, Toyin Ajiboro Aremu, and Yetunde Ajao Modupe, "Defending against Cybersecurity Threats to the Payments and Banking System," 2022.

[19] Adejoke T. Odebade and Elhadj Benkhelifa, "A Comparative Study of National Cyber Security Strategies of Ten Nations," 2023.

digital evidence. Selain itu, strategi penanggulangan harus melibatkan kerja sama lintas sektor, termasuk lembaga keuangan, penyedia layanan teknologi, regulator, dan aparat penegak hukum. Pendidikan publik tentang keamanan digital juga harus ditingkatkan untuk meminimalkan potensi korban.

Dengan demikian, dapat disimpulkan bahwa efektivitas penegakan hukum terhadap kejahatan carding di Indonesia masih menghadapi tantangan serius baik dari sisi regulasi, implementasi, hingga eksekusi. Ketidaksesuaian antara hukum yang berlaku dengan sifat kejahatan digital yang terus berkembang menunjukkan perlunya reformasi hukum pidana siber yang lebih progresif, berbasis teknologi, dan berorientasi pada perlindungan masyarakat secara menyeluruh.

KESIMPULAN

Penegakan hukum terhadap kejahatan carding di Indonesia masih menghadapi berbagai tantangan, seperti kelemahan legislasi, rendahnya pemahaman teknis aparat penegak hukum, serta kurangnya kerjasama internasional yang efektif. Selain itu, proses identifikasi dan pembuktian kasus juga terkendala oleh keterbatasan infrastruktur digital forensik dan banyaknya pelaku yang beroperasi secara lintas negara dengan metode yang semakin canggih. Di sisi lain, perkembangan teknologi telah memberikan peluang besar untuk mempermudah pelaku dalam melakukan kejahatan digital, namun juga menawarkan solusi dalam penanggulangannya, seperti penggunaan teknologi untuk meningkatkan efektivitas pelacakan dan penanganan kejahatan siber. Oleh karena itu, disarankan agar Indonesia mengembangkan regulasi khusus yang mengatur kejahatan carding secara lebih spesifik dan komprehensif, serta meningkatkan kapasitas aparat penegak hukum melalui pelatihan teknologi informasi dan digital forensik. Selain itu, perlu dilakukan kerja sama internasional yang lebih erat dalam pertukaran data dan penegakan hukum lintas negara agar kejahatan ini dapat ditanggulangi secara lebih efektif dan preventif. Penguatan sistem perlindungan hukum, edukasi masyarakat, serta pengembangan teknologi keamanan siber juga sangat penting untuk mengatasi tantangan tersebut dan menciptakan ekosistem transaksi digital yang lebih aman dan terpercaya.

DAFTAR PUSTAKA

Amanda Fitria Najwa, Aqila Husna, and Aqila Husna. "Efektifitas Yurisdiksi Cybercrime Di Tengah Perkembangan Teknologi Informasi." *Jurnal Hukum Dan Sosial Politik* 2, no. 3 (2024): 126–35. https://doi.org/10.59581/jhsp-widyakarya.v2i3.3426.

Arief, Barda Nawawi. *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*. Jakarta: Kencana, 2018.

Banjarani, Desia Rakhma, and Muhammad Apriliansyah Rahmadhani. "Cybercrime as Transnational Crime: Law Enforcement and Countermeasure Problems in the Perspective of International Criminal Law." *Yustisia Tirtayasa : Jurnal Tugas Akhir* 4, no. 4 (2024). https://doi.org/10.51825/yta.v4i4.29046.

Broadhurst, Roderic, David Lord, Donald Maxim, Hannah Woodford-Smith, Corey Johnston, Ho Woon Chung, Samara Carroll, Harshit Trivedi, and Bianca Sabol.

"Malware Trends on 'Darknet' Crypto-Markets: Research Review." *SSRN Electronic Journal*, 2018. https://doi.org/10.2139/ssrn.3226758.

Btoush, Eyad Abdel Latif Marazqah, Xujuan Zhou, Raj Gururajan, Ka Ching Chan, Rohan Genrich, and Prema Sankaran. "A Systematic Review of Literature on Credit Card Cyber Fraud Detection Using Machine and Deep Learning." *PeerJ Computer Science* 9 (2023). https://doi.org/10.7717/PEERJ-CS.1278.

Ginara, I Gede Krisna, I Made Minggu Widyantara, and Ni Komang Arini Styawati. "Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia." *Jurnal Preferensi Hukum* 3, no. 1 (2022): 138–42. https://doi.org/10.22225/jph.3.1.4673.138-142.

Haruna, Williams, Toyin Ajiboro Aremu, and Yetunde Ajao Modupe. "Defending against Cybersecurity Threats to the Payments and Banking System," 2022.

Koops, Bert-Jaap. "Should ICT Regulation Be Technology-Neutral?," 2006. https://doi.org/10.1007/978-90-6704-665-7_4.

Muh. Fandi Nursalam, Ashar Sinilele, and Istiqamah. "Carding Crime in Makassar City: Juridical Review As an Issues of Cybercrime." *Alauddin Law Development Journal* 6, no. 1 (2024): 172–79. https://doi.org/10.24252/aldev.v6i1.22387.

Odebade, Adejoke T., and Elhadj Benkhelifa. "A Comparative Study of National Cyber Security Strategies of Ten Nations," 2023.

Patsakis, Constantinos, David Arroyo, and Fran Casino. "The Malware as a Service Ecosystem," 371–94, 2025. https://doi.org/10.1007/978-3-031-66245-4_16.

Quinn, Anthony, Louise Cooke, and Mark Monaghan. "An Exploration of the Progress of Open Crime Data: How Do Ongoing Limitations with the Police.Uk Website Restrict a Comprehensive Understanding of Recorded Crime?" *Policing and Society* 29, no. 4 (2019): 455–70. https://doi.org/10.1080/10439463.2017.1397149.

Rusydi, Muhammad Taufik. "Cyber Law Policy Development: Indonesia's Response to International Cybercrime Threats." *Journal of Progressive Law and Legal Studies* 3, no. 01 (2025): 69–85. https://doi.org/10.59653/jplls.v3i01.1365.

Sanjan, P. S., N. Gowtham, Mahajan Sagar Bhaskar, Umashankar Subramaniam, Dhafer J. Almakhles, Sanjeevikumar Padmanaban, and N. G. Yamini. "Enhancement of Power Quality in Domestic Loads Using Harmonic Filters." *IEEE Access* 8 (2020): 197730–44. https://doi.org/10.1109/ACCESS.2020.3034734.

Sari, Monica Nila. "Cybercrime in Association of Southeast Asian Nations." *Journal of Information Policy* 14 (2024): 568–98. https://doi.org/10.5325/jinfopoli.14.2024.0016.

Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada, 2010.

Sriono, Risdalina, Kusno, Indra Kumalasari M, and Hengki Syahyunan. "LEGAL PROTECTION FOR DIGITAL BANK CUSTOMERS IN INDONESIA: ANALYSIS OF DATA CONFIDENTIALITY REGULATIONS AND BANK RESPONSIBILITY." *LITIGASI* 25, no. 2 (January 2024): 301–30. https://doi.org/10.23969/litigasi.v25i2.18538.

Stoykova, Radina. "The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations." *Computer Law & Security Review* 49 (2023): 105801. https://doi.org/10.1016/j.clsr.2023.105801.

World Economic Forum. *Global Cybersecurity Outlook 2023*. Geneva: WEF, 2023. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/.