MILTHREE LAW JOURNAL

Volume 1 Nomor 1 Maret 2025

Ratifikasi *Convention on Cybercrime* Oleh Indonesia Sebagai Bentuk Pencegahan *Carding* Dalam Perspektif Hukum Internasional

Yogi Wirandicha[1], Zulfikar Jayakusuma[2], Ledy Diana[3]

[1] Universitas Riau, Indonesia
[2] Universitas Riau, Indonesia
[3] Universitas Riau, Indonesia

Email Korespondensi:
yogi.wirandicha3035@student.unri.ac.id

ABSTRAK

Penggunaan fasilitas komputer dan melakukan kejahatan pada sistem atau jaringan komputer dianggap sebagai kejahatan siber. Pada tahun 2021, Indonesia mencatat sekitar 1,6 miliar serangan siber. Pemerintah Indonesia memiliki perlu untuk meratifikasi *Convention on Cybercrime* dan perlu mengembangkan kolaborasi internasional dalam penegakan hukum khususnya pada kejahatan *carding*. Tujuan dari penelitian ini adalah untuk mengetahui bentuk pencegahan yang dilakukan Indonesia dalam mengambil langkah-langkah proaktif untuk memerangi dan mencegah kejahatan *carding*. Penelitian ini menggunakan metode penelitian hukum normatif, atau sering disebut juga sebagai penelitian hukum doktrinal, yang mengacu pada sumber-sumber hukum primer, sekunder, dan tersier sebagai sumber data sekunder. Penelitian yuridis normatif ini melihat

MILTHREE LAW JOURNAL
Volume 1 Nomor 1 Maret 2025

bagaimana hukum di Indonesia tentang kejahatan siber, khususnya yang berkaitan dengan kejahatan *carding*, selaras dengan konvensi kejahatan siber.

Hasil penelitian menunjukkan langkah yang dilakukan Indonesia adalah dengan ratifikasi *Convention on Cybercrime* untuk memperkuat kerangka hukum internasional dalam menangani kejahatan siber lintas negara dan pembaruan undang-undang, khususnya terkait *cybercrime.* Sehingga dengan adanya regulasi yang lebih komprehensif tersebut, penegakan hukum di Indonesia akan lebih efektif dalam mengatasi kasus *carding* dan mencegah kerugian finansial serta kerusakan reputasi yang dapat ditimbulkan dari kejahatan siber.

Kata Kunci: kejahatan siber, *carding*, ratifikasi, *convention on cybercrime*

ABSTRACT

Using computer facilities and committing crimes on computer systems or networks is considered a cyber crime. In 2021, Indonesia recorded around 1.6 billion cyber attacks. The Indonesian government has the need to ratify the Convention on Cybercrime and needs to develop international collaboration in law enforcement, especially on carding crimes. The purpose of this study is to determine the form of prevention taken by Indonesia in taking proactive measures to combat and prevent carding crimes. This research uses normative legal research methods, or often referred to as doctrinal legal research, which refers to primary, secondary, and tertiary legal sources as secondary data sources. This normative juridical research looks at how Indonesian laws on cybercrime, especially those relating to carding crimes, are in line with the cybercrime convention. The results of the research show that the steps taken by Indonesia are the ratification of the Convention on Cybercrime to strengthen the international legal framework in dealing with cross-border cybercrime and the renewal of laws, especially those related to cybercrime. So that with these more comprehensive regulations, law enforcement in Indonesia will be more effective in overcoming carding cases and preventing financial losses and reputational damage that can be caused by cybercrime.

MILTHREE LAW JOURNAL
Volume 1 Nomor 1 Maret 2025

Keywords: *cybercrime, carding, ratification, convention on cybercrime*

ABSTRACT

Waqf land is an immovable object that also has economic value, and must be managed properly by the nazhir (waqf recipient) in accordance with applicable laws and regulations. The aim of this research is to find out how unlawful acts are in disputes over control of waqf land, the consequences of unlawful acts over control of waqf land in the Civil Code, and how judges consider in resolving cases of unlawful acts caused by control of waqf land in decisions. Number 04/Pdt.G/2018/PN Ktn. The method used is a descriptive method in the form of normative juridical, the data used is primary data and secondary data and the data collection used is a literature study in the decision of the Kutacane District Court in decision Number: 04/Pdt.G/2018/PN-Ktn using the method data analysis approach to law. Analysis of the Judge's Decision regarding control of waqf land, which is based on legal facts concluded in the judge's consideration that it is clearly proven that land Certificate No. 02 is waqf land from wakif Sehaddin to Nazhir. The local community headed by Rasimin has also been proven that the Plaintiff is the Substitute Nazhir in the aquo case, therefore the object of the dispute which is currently controlled by Defendant I and Defendant II must be handed over to the Plaintiff as Substitute Nazhir so that the Court sentenced Defendant I and Defendant II who control Certificate Number 02 of the waqf land to hand it over to the Plaintiff after the decision in the aquo case becomes legally binding.

Keywords: Unlawful Acts, Waqf, Without Rights.

1. Pendahuluan

Beberapa dekade terakhir telah terjadi perkembangan teknologi informasi dan komunikasi yang pesat dan mendorong transformasi signifikan dalam kehidupan manusia di berbagai aspek. Kehadiran internet menjadi manifestasi dari adanya perkembangan tersebut yang telah membuat perubahan pada dunia pada era yang serba mudah dalam terhubung dan berkomunikasi satu sama lain

tanpa khawatir jarak serta waktu[1]. Namun, selain kemudahan yang ditawarkan dari adanya kemajuan tersebut, namun juga kondisi yang turut melahirkan bentuk-bentuk kejahatan baru atau kriminal yang berbasis internet atau yang dikenal dengan kejahatan dunia maya (*cybercrime)*[2].

Cybercrime didefiniskan sebagai kejahatan terhadap sistem komputer, yang dalam artian luasnya mencakup pada kejahatan yang menggunakan sarana komputer untuk melakukan tindak pidana terhadap sistem atau jaringan komputer[3]. Batas teritorial tidak menjadi batasan dalam *cybercrime* karena sifat dari internet yang tidak mengenal adanya batasan (borderless). Sehingga pelaku kejahatan yang berada pada wilayah teritorial tidak dapat diadili di negara yang menjadi korban dikarenakan alasan yuridiksi dari suatu negara[4].

Konvensi Perserikatan Bangsa-Bangsa Menentang Kejahatan Organisasi Transnasional *(United Nation Convention Transnational Organized Crime)* (*Palermo Convention*) pada November 2000 menetapkan *cybercrime* sebagai salah satu jenis kejahatan transnasional. UNCITRAL *Model Law*, yang disahkan oleh Majelis Umum PBB dengan Resolusi 51/162 tanggal 16 Desember 1996, menetapkan bahwa negara tidak terikat oleh aturan-aturan yang terkandung dalam *Model Law*, yang menjadikan negara bebas untuk mengikuti atau menolak *Model Law* tersebut secara keseluruhan atau sebagian. Adolf menyebutkan bahwa menggalakkan

---

[1] Abdul Wahid and Labib Mohammad, *Kejahatan mayantara (cyber crime)* (Bandung: Refika Aditama, 2005).

[2] V. Selvie Sinaga, *Hukum Perjanjian Internasional: Diskursus Tentang Konvensi wina 1969* (Penerbit Unika Atma Jaya Jakarta, 2019).

[3] S Sumarwani, "TINJAUAN YURIDIS PEMIDANAAN *CYBERCRIME* DALAM PERPEKTIF HUKUM PIDANA POSITIF," *Jurnal Pembaharuan Hukum*, no. 3 (2014).

[4] Yuliana Surya Galih, "YURISDIKSI HUKUM PIDANA DALAM DUNIA MAYA," *Jurnal Ilmiah Galuh Justisi* 7, no. 1 (June 20, 2019): 59–74, https://doi.org/10.25157/jigj.v7i1.2138.

aturan-aturan hukum terkait penggunaan jaringan komputer dalam transaksi-transaksi komersial merupakan tujuan dari *Model Law*[5].

Berbagai macam *cybercrime* yang ada di dunia saat ini mulai dari Ddos, ramsomware, hingga kejahatan dunia maya lain yang marak terjadi yaitu *carding*. *Carding* sendiri merupakan tindakan kejahatan dunia maya berupa penggunaan kartu kredit secara ilegal atau tidak sah untuk memsan ataupun membeli barang secara online dengan mencantumkan nomor kartu kredit orang lain untuk pembayaran barang yang dibeli[6]. Kejahatan tersebut sangat merugikan, tidak hanya dari individu yang menjadi korban akan tetapi juga sampai pada institusi keuangan. *Carding* sendiri juga sudah menjadi *cybercrime* yang serius dan menjadi permasalahan yang masih sering memakan korban di Indonesia.

Serangan siber sendiri tercatat pada tahun 2021 sebanyak ±1,6 milyar di Indonesia. Selain kejahatan yang sudah disebutkan sebelumnya, serangan siber di Indonesia juga merambah pada terjadinya kebocoran data, namun *carding* masih menjadi tindak kejahatan dunia maya yang sering terjadi di Indonesia. Sebagai contoh kasus *carding*, pada tahun 2019 di Surabaya dilakukan penangkapan pada 18 peretas kartu kredit milik warga negara asing (WNA), dimana pelaku mengantongi keuntungan sekitar $400USD yang bulanannya mengantongi sekitar Rp. 48 juta, dan jika diakumulasikan selama satu tahun mencapai Rp. 6 milliar. Kasus lain terjadi pada tahun 2022 di Jakarta dimana banyak nasabah yang kehilangan uang akibat dari skimming, dan masih banyak lagi kasus *carding* lainnya.

Kemanan siber di Indonesia sendiri menduduk peringkat ke-6 dan ke-13 terendah di dunia dan Asia. Sebanyak 16.845 laporan tindak kejahatan siber tercatat dari tahun 2017-2020 yang masuk ke Direktorat Tindak Pidana Siber

[5] Huala Adolf, *Hukum Perdagangan Internasional* (Pt Rajagrafindo Persada, 2020).

[6] Sudaryono Sudaryono and Natangsa Subakti, *HUKUM PIDANA Dasar-Dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP* (Muhammadiyah University Press, 2022).

(Ditipidsiber) Polri, dan hampir 200.000 pengaduan terkait *carding* yang diterima Direktur Pengendalian Aplikasi Informatika Kementerian Komunikasi dan Informatika (Kemenkominfo)[7]. Tingginya angka laporan tersebut tentunya mencerminkan bahwa hukum terkait tindak kejahatan dunia maya masih belum mampu menangani banyaknya kasus *carding* di Indonesia.

Walaupun sifat kejahatannya virtual, *carding* tetap dikategorikan sebagai tindakan dan perbuatan hukum yang nyata sesuai dengan yang diatur dalam Pasal 363 ayat (5) KUHP mengenai pencurian dan pemberatan[8]. *Carding* juga merupakan kejahatan transnasional dimana melibatkan akses dan manipulasi informasi keuangan secara ilegal. Penegakan hukum terhadap *carding* memerlukan yuridiksi ekstrateritorial dimana negara wajib untuk menuntut dan mengadili pelaku kejahatan internasional, mengingat sifat *carding* yang transnasional. Dalam asas *aut dedere aut judicare,* setiap negara diharuskan tidak hanya menangkap dan menuntut pelaku, melainkan juga bekerjsama dengan negara lain dalam penegakan hukum[9].

Di Indonesia, regulasi terkait *cybercrime* mulai diterapkan dengan Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, yang menjadi landasan awal untuk pengaturan akses ilegal. Namun, baru pada Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dan perubahan terbaru Undang-Undang No. 19 Tahun 2016, pengaturan mengenai *cybercrime*, termasuk

---

[7] dob, "Ada 5.000 Kasus Perbulan, Indonesia Emergency Kejahatan Siber," CNBC Indonesia, accessed August 24, 2024, https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber.

[8] 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 (February 27, 2022): 138–42, https://doi.org/10.22225/jph.3.1.4673.138-142.

[9] Ndifon Neji Obi and Sovereign Felix Nyong, "Rethinking Civil Society Participation in the Implementation of the UN Convention Against Corruption in Nigeria," *Journal of Economics and Sustainable Development* 9, no. 16 (2018): 16.

akses ilegal dan penyadapan, diatur lebih detail. Pasal-pasal dalam UU ITE seperti Pasal 30 tentang pengaksesan ilegal, Pasal 31 tentang penyadapan ilegal, dan Pasal 34 tentang pendistribusian alat kejahatan, mengatur berbagai aspek tindakan yang terkait dengan *carding*.

Reformasi lebih lanjut dilakukan dengan pengesahan Undang-Undang No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (UU KUHP), yang mencabut dan menggantikan pasal-pasal terkait akses ilegal dari UU ITE. Pasal-pasal baru dalam UU KUHP, seperti Pasal 332 dan Pasal 258, mengakomodasi kebutuhan hukum terkait akses dan penyadapan ilegal, memberikan struktur hukum yang lebih terintegrasi dan komprehensif.

Namun, untuk menangani kejahatan *carding* secara lebih efektif, penting bagi Indonesia untuk meratifikasi *Convention on Cybercrime* yang disepakati pada 23 November 2001 di Budapest oleh *Council of Europe.* Konvensi ini menetapkan standar internasional dalam penanganan *cybercrime* dan memberikan kerangka kerja bagi negara-negara anggota untuk bekerja sama. Pasal 2 dari konvensi ini mengatur tentang akses ilegal, menetapkan bahwa setiap negara harus menjadikannya sebagai tindak pidana ketika dilakukan tanpa hak. Demikian juga, Pasal 3 mengatur tentang penyadapan ilegal, yang melibatkan teknik-teknik tertentu untuk mentransmisikan data komputer secara sembunyi-sembunyi.

Ratifikasi konvensi ini akan memberikan banyak manfaat penting bagi Indonesia. Pertama, Indonesia dapat meminta bantuan kepada anggota lain melalui kerja sama hukum internasional atau ekstradisi. Kedua, Indonesia akan berhak mendapatkan informasi dari anggota lain mengenai sistem komputer atau bukti elektronik. Ketiga, ratifikasi konvensi ini akan menjamin bahwa Indonesia tunduk pada hak dan tanggung jawab yang sama dengan negara-negara anggota

konvensi dalam hal penegakan hukum internasional, sehingga memperkuat posisi Indonesia dalam hal ekstradisi dan kerja sama internasional[10].

Dengan meratifikasi *Convention on Cybercrime,* Indonesia dapat memperkuat upayanya dalam memberantas *carding* dan kejahatan cyber lainnya. Ini akan memperluas jangkauan hukum Indonesia, meningkatkan kerjasama internasional, dan memperbaiki posisi Indonesia dalam menangani kejahatan yang melibatkan pelaku di luar negeri. Dalam penanggulangan tindak pidana carding di Indonesia terletak pada ketidakseimbangan antara karakter kejahatan yang bersifat transnasional dan borderless dengan sistem hukum pidana nasional yang masih bertumpu pada asas teritorialitas. Meskipun Indonesia telah memiliki instrumen hukum seperti UU ITE dan KUHP Nasional, efektivitas penegakan hukum terhadap carding masih menghadapi hambatan serius, khususnya dalam aspek yurisdiksi, pembuktian elektronik lintas negara, dan kerja sama internasional. Ketiadaan ratifikasi Convention on Cybercrime memperlebar celah hukum tersebut, sehingga menimbulkan legal gap yang berdampak langsung pada lemahnya perlindungan hukum bagi korban dan keterbatasan aparat penegak hukum dalam menjangkau pelaku kejahatan siber lintas batas negarag. Sebagai langkah strategis, ratifikasi konvensi ini menjadi krusial untuk melengkapi upaya domestik dan internasional dalam memerangi kejahatan cyber yang semakin kompleks.

Penelitian ini bertujuan untuk mengeksplorasi urgensi ratifikasi *Convention on Cybercrime* oleh Indonesia sebagai langkah strategis dalam pencegahan dan penanggulangan tindak pidana *carding*. Ratifikasi konvensi ini diharapkan dapat memperkuat kerjasama internasional, meningkatkan efektivitas penegakan hukum, serta melindungi masyarakat Indonesia dari ancaman kejahatan siber, khususnya *carding*. Dengan demikian, penelitian ini diharapkan dapat

[10] Amirullah Amirullah, "Arti Penting Ratifikasi European Union Convention on Cybercrime 2001 Bagi Indonesia" (Bandung, Universitas Padjajaran, 2008).

memberikan kontribusi dalam upaya penanggulangan kejahatan siber di Indonesia.

Berbagai penelitian telah dilakukan untuk memahami dan mengkaji fenomena *carding* serta upaya penanggulangannya di Indonesia. Zulfiqar Hafizh Aslam dalam penelitiannya yang berjudul "*Carding* Sebagai Bentuk Budaya Konsumerisme Modern" menyatakan bahwa *carding* sering kali digunakan untuk memenuhi kebutuhan konsumerisme masyarakat Indonesia yang cenderung kebarat-baratan. Ia menyoroti bahwa perilaku konsumtif ini tidak hanya untuk memenuhi kebutuhan, tetapi juga untuk mengonsumsi merek-merek yang memiliki citra tertentu[11].

Penelitian lain oleh Dea Alamanda Putra, dengan judul "Analisis Yuridis Pemidanaan Terhadap Pelaku Tindak Pidana *Carding* (Studi Kasus di Ditreskrimsus Polda Jateng)," menganalisis bagaimana sistem pemidanaan terhadap pelaku *carding* di Jawa Tengah. Putra menyoroti bahwa meskipun UU ITE telah mengatur tindak pidana *carding*, proses penegakannya masih memerlukan sosialisasi lebih lanjut agar lebih efektif[12].

Selanjutnya, penelitian oleh Akhdiyat Mubaraq berjudul "Tinjauan Yuridis Tindak Pidana Peretasan Kartu Kredit Melalui Internet Atau *Carding* Terhadap Warga Negara Asing (Studi Putusan Nomor 102/Pid.Sus/PN.Wns)" menemukan bahwa meskipun penerapan hukum pidana dalam kasus peretasan kartu kredit terhadap warga negara asing diatur dengan tepat oleh UU ITE, hukuman yang

[11] Zulfiqar Hafizh Aslam, "*CARDING* SEBAGAI BENTUK BUDAYA KONSUMERISME MODERN : STUDI KASUS KOMUNITAS SKATEBOARD SURABAYA" (undergraduate, UIN Sunan Ampel Surabaya, 2014), http://digilib.uinsa.ac.id/437/.

[12] Dea Alamanda Putra, "ANALISIS YURIDIS PEMIDANAAN TERHADAP PELAKU TINDAK PIDANA *CARDING* (STUDI KASUS DI DITRESKIRMSUS POLDA JATENG)" (other, Universitas Negeri Semarang, 2017), https://lib.unnes.ac.id/30219/.

dijatuhkan masih dianggap terlalu ringan jika dilihat dari dampak yang dihasilkan[13].

Penelitian-penelitian tersebut memberikan gambaran bahwa meskipun sudah ada regulasi di Indonesia yang mengatur *carding*, penerapan dan penegakan hukumnya masih menghadapi banyak tantangan, terutama karena sifatnya yang transnasional. Selain itu, penelitian-penelitian ini juga menyoroti pentingnya kerjasama internasional dalam menangani kejahatan siber.

2. Metode Penelitian

Penelitian ini mentitkberatkan pada analisis pada data sekunder atau bahan pustaka yang digunakan pada jenis penelitian hukum normatif yang menjadi metode dalam penelitian ini. Adapun pendekatan yang digunakan adalah yuridis normatif yang dilakukan dengan cara melakukan penelitian pada kajian literatur, peraturan perundang-undangan, serta bahan lainnya seperti bahan hukum yang relevan dengan topik penelitian yang diangkat[14] yaitu berkaitan pada sinkronisasi undang-undang di Indonesia berkaitan dengan *cybercrime*, utamanya pada tindak pidana *carding*, dengan ratifikasi *Convention on Cybercrime.*

Penelitian ini juga menggunakan data sekunder, dimana terdiri dari bahan hukum premier, sekunder, dan tersier[15]. Undang-Undang Dasar (UUD) Negara Republik Indonesia Tahun 1945 menjadi bahan hukum premier karena mencakup peraturan perundang-undangan terkait, selain itu undang-undang lain serta peraturan pemerintah yang relevan juga termasuk dalam bahan hukum premier.

---

[13] Akhdiyat Mubaraq, "TINJAUAN YURIDIS TINDAK PIDANA PERETASAN KARTU KREDIT MELALUI INTERNET ATAU *CARDING* TERHADAP WARGA NEGARA ASING (Studi Putusan Nomor 102/Pid.Sus/ PN. Wns)" (other, UNIVERSITAS HASANUDDIN, 2021), https://repository.unhas.ac.id/id/eprint/11544/.

[14] Soerjono Soekanto and Sri Mamudji, *Penelitian hukum normatif: suatu tinjauan singkat* (Penerbit CV. Rajawali, 1986).

[15] Soekanto and Mamudji.

Untuk bahan hukum sekunder meliputi pada publikasi terkait hukum, seperti buku teks, doktrin huku, serta jurnal hukum[16]. Sedangkan bahan hukum tersier meliputi pada kamus hukum dan sumber referensi relevan lainnya.

Data dikumpulan melalui teknik studi kepustakaan dengan cara bahan hukum premier, sekunder, dan tersier tadi ditelaah sehingga diharapkan mendapatkan pemahaman secara lebih mendalam terkait aturan hukum mengenai *cybercrime* serta perspektif literatur lainnya yang relevan yang mendukung penelitian. Teknik analisis data dilakukan melalui pendekatan kualitatif deskriptif[17], dimana data yang dikumpulkan tersebut dilakukan analisis untuk memberikan gambaran terkait kebijakan hukum yang diharapkan dapat diterapkan dalam peraturan perundang-undangan di masa mendatang. Untuk menjaga kesinambungan antara berbagai sumber data yang digunakan, proses dan pengolahan dalam analisis data dilakukan dengan cara yang bersamaan atau pada waktu yang sama.[18]

3. Pembahasan

A. Meratifikasi Convention on Cybercrime

Masifnya kejahatan cybercrime yang bersifat transnasional, maka Indonesia perlu meratifikasi *Convention on Cybercrime* untuk mengatasi berbagai ketentuan peraturan perundang-undangan yang masih belum dapat secara memadai mengatasi dan memberikan solusi terkait kasus-kasus *cybercrime*, khususnya pada kejahatan carding. Secara normatif, akses ilegal dan penyalahgunaan data elektronik secara struktural masih menyisakan persoalan mendasar, khususnya dalam penanganan kejahatan yang melibatkan pelaku, server, dan korban yang

[16] Zainuddin Ali, *Metode Penelitian Hukum* (Sinar Grafika, 2021).
[17] Sugiyono, *Metode penelitian kuantitatif, kualitatif dan R&D* (Bandung: Alfabeta, 2020).
[18] Hardani et al., *Metode Penelitian Kualitatif & Kuantitatif* (CV. Pustaka Ilmu, 2020).

berada di yurisdiksi berbeda. Dengan demikian, problem utama penegakan hukum carding di Indonesia bukan terletak pada ketiadaan norma pidana, melainkan pada keterbatasan daya jangkau hukum nasional dalam menghadapi kejahatan siber transnasional. Kondisi ini menunjukkan bahwa pembaruan hukum pidana yang bersifat nasional semata belum cukup tanpa disertai integrasi dengan rezim hukum internasional melalui ratifikasi *Convention on Cybercrime.*

Convention on Cybercrime adalah aturan luas yang mengatur jenis-jenis pelanggaran atau perilaku yang termasuk dalam kategori kejahatan siber.[19] Konvensi ini merupakan perjanjian internasional yang paling relevan dalam melawan kejahatan siber. Tingkat kerjasama antara pihak-pihak yang terlibat serta kualitas pelaksanaannya terus ditingkatkan untuk menghadapi tantangan dan isu-isu baru. *Convention on Cybercrime* juga memiliki program pembangunan kapasitas yang berfungsi sebagai mekanisme tindak lanjut yang efektif dan dilaporkan kembali ke komite yang membantu membentuk konvensi tersebut. Tujuan utama dari strategi ini adalah untuk melindungi hak setiap individu saat mereka berinteraksi atau beraktivitas menggunakan internet. Tujuan lain yang tidak kalah penting adalah untuk mendekatkan negara-negara yang menjadi partisipan atau anggota. Pertimbangan-pertimbangan tersebut menjadi dasar dari *Convention on Cybercrime*. Selain itu, juga untuk menarik perhatian pada pentingnya memperkuat hubungan dengan peserta atau anggota konvensi lainnya, dan untuk membahas kebutuhan akan perlindungan terhadap penipuan online atau kejahatan siber.[20]

Indonesia akan diuntungkan dari mekanisme kerjasama yang tertuang dalam *Convention on Cybercrime* dimana akan membantu Indonesia dalam memberantas kejahatan dunia maya terutamanya pada tindak pidana *carding*. Adapun benefit yang didapatkan tersebut dapat terlihat dari setiap negara yang

[19] Akbar Kurnia Putra, "HARMONISASI KONVENSI CYBER CRIME DALAM HUKUM NASIONAL," *Jurnal Ilmu Hukum* 5, no. 2 (2015), https://scholar.google.co.id/citations?view_op=view_citation&hl=en&user=7-B5s7EAAAAJ&citation_for_view=7-B5s7EAAAAJ:ULOm3_A8WrAC.

[20] Amirullah, "Arti Penting Ratifikasi European Union Convention on Cybercrime 2001 Bagi Indonesia."

terlibat atau termasuk dalam *Convention on Cybercrime* memberikan bantuan mereka dalam menerapkan penegakan hukum kepada pelaku kejahatan siber, selama pelaku kejahatan tersebut berada pada yuridiksi negara pihak. Sehingga, pemberatasan kejahatan siber akan lebih terlaksana dan tercipta dengan efektif. Selain benefit yang disebutkan tersebut, Indonesia juga akan memiliki hak serta kewajiban yang sama dan terikat dalam peraturan yang wajib dipatuhi dan juga berkedudukan sama dengan negara anggota lain dalam melakukan kerjasama dalam pemberantasan kejahatan siber atau cybercrime. Indonesia dalam perjalanannya nantinya tidak hanya akan dapat mampu memberantas cybercrime utamanya *carding*, namun juga memiliki hubungan yang baik dengan negara partisipan lain yang efektif serta efisien melalui mekanisme yang telah dirancang sesuai dengan *Convention on Cybercrime*. Namun, jika terjadi situasi yang melibatkan Indonesia dan negara anggota yang tidak memiliki perjanjian ekstradisi, kedua negara dapat meminta ekstradisi pelaku dengan menggunakan konvensi tersebut sebagai pembenaran. Konsep hukum perjanjian internasional *pacta sunt servanda* menyatakan bahwa para pihak dalam perjanjian internasional harus melaksanakan komitmen mereka dengan itikad baik. Akibatnya, melanggar perjanjian internasional dapat dianggap sebagai pelanggaran hukum internasional, yang mana terdapat anksi ataupun ganti rugi yang mesti dipertanggungjawabkan.

Meratifikasi *Convention on Cybercrime* oleh Indonesia dapat memperluas jenis alat bukti yang dapat digunakan dalam upaya pemberantasan kejahatan dunia maya. Konvensi ini merupakan instrumen hukum internasional untuk mengatasi kejahatan siber, sehingga jika Indonesia meratifikasinya, peraturan yang berlaku di dalam negeri akan selaras dengan standar internasional, terutama dalam menangani kejahatan siber. Selain itu, Indonesia akan memiliki lebih banyak kesempatan untuk bekerja sama dengan negara lain untuk mengatasi kejahatan siber jika meratifikasi Konvensi ini. Konvensi ini juga dapat digunakan sebagai teknik untuk mengurangi penggunaan jaringan, komputer, dan data yang tidak semestinya yang digunakan dalam kejahatan siber. Melalui sistem kerja sama internasional yang handal, Indonesia juga akan mendapatkan keuntungan dengan

meratifikasi Konvensi ini dengan memiliki kepercayaan diri dalam proses investigasi dan penuntutan baik di dalam maupun di luar negeri.

Adapun dampak yang dapat ditimbulkan jika Indonesia tidak melakukan ratifikasi terhadap *Convention on Cybercrime* adalah Indonesia akan dirugikan karena tanpa adanya mekanisme kerjasama dengan negara lain untuk memberantas kejahatan dunia maya / *cybercrime*, pemberantasan yang dilakukan oleh Indonesia sendiri tidak akan berjalan dengan efektif, apabila kejahatan tersebut melibatkan pelaku kejahatan yang berasal dari luar negeri. Penanganan kasus dengan tipologi semacam ini terkait erat dengan prinsip fundamental dalam hukum internasional, di mana kedaulatan suatu negara harus dihormati oleh negara lain. Oleh karena itu, Indonesia tidak bisa bertindak sewenang-wenang dalam menangkap dan mengadili seseorang yang berada di luar yurisdiksinya. Apalagi, Indonesia menempati peringkat kedua dalam jumlah kasus kejahatan siber terbesar di dunia, yang tentunya akan menyulitkan upaya pemberantasan kejahatan siber jika tidak meratifikasi Konvensi Kejahatan Siber tersebut.[21]

B. Merumuskan Undang-Undang yang Mengatur Tindak Pidana *Carding*

Kurangnya regulasi yang spesifik mengenai carding di Indonesia memberikan celah bagi pelaku kejahatan siber. Pemerintah bertanggung jawab untuk melindungi warganya, termasuk melindungi aset mereka dari ancaman di dunia maya. Namun, hingga kini, peraturan yang mengatur aktivitas di dunia maya belum sepenuhnya komprehensif[22]. Sebelum adanya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), penegak hukum mengandalkan undang-undang umum seperti Undang-Undang Nomor 36 Tahun 1999 tentang

[21] PDSI KOMINFO, "Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber," Website Resmi Kementerian Komunikasi dan Informatika RI, accessed August 25, 2024, http:///index.php/content/detail/4698/Indonesia-Peringkat-ke-2-Dunia-Kasus-Kejahatan-Siber/0/sorotan_media.

[22] Agus Raharjo, *Cybercrime: pemahaman dan upaya pencegahan kejahatan berteknologi* (Citra Aditya Bakti, 2002).

Telekomunikasi dan Kitab Undang-Undang Hukum Pidana (KUHP) untuk menangani kasus carding, meskipun pembuktiannya sering kali sulit[23]. KUHP menjadi dasar hukum utama untuk menjerat pelaku carding, dengan menggunakan Pasal 362 tentang pencurian dan Pasal 378 tentang penipuan. Namun, kedua pasal ini tidak secara spesifik dirancang untuk menangani kejahatan di dunia maya, sehingga penegak hukum sering kali harus menafsirkan secara ekstensif agar aturan tersebut dapat diterapkan dalam kasus kejahatan siber, khususnya carding[24].

KUHP di Indonesia juga belum mengatur secara spesifik yurisdiksi hukum untuk kejahatan yang terjadi di dunia maya. Hal ini berdampak pada perlindungan hak-hak pribadi, terutama terkait dengan data pribadi yang seringkali menjadi target dalam kejahatan di dunia maya[25]. Dengan perkembangan teknologi internet yang begitu pesat, kebutuhan untuk melindungi data pribadi dari akses tidak bertanggung jawab menjadi semakin mendesak. Untuk menangani kejahatan *carding*, diperlukan dua jenis upaya penanggulangan: penal dan non-penal. Upaya penal dilakukan secara represif dengan menegakkan hukum setelah tindak pidana terjadi, melalui mekanisme hukum yang ada. Sebaliknya, upaya non-penal bersifat preventif, bertujuan untuk

[23] Nuria Siswi Enggarani, "PENANGGULANGAN KEJAHATAN INTERNET DI INDONESIA," September 2012, http://publikasiilmiah.ums.ac.id/handle/11617/4010.

[24] Adi Setyo, "BULETIN HUKUM PERBANKAN DAN KEBANKSENTRALAN 29 Volume 4 Nomor 2, Agustus 2006 PERKEMBANGAN CYBERCRIME DAN UPAYA PENANGANANNYA DI INDONESIA OLEH POLRI Oleh : Kombes (Pol) Drs," accessed August 26, 2024, https://www.academia.edu/4941347/BULETIN_HUKUM_PERBANKAN_DAN_KEBANKSENTRALAN_29_Volume_4_Nomor_2_Agustus_2006_PERKEMBANGAN_CYBERCRIME_DAN_UPAYA_PENANGANANNYA_DI_INDONESIA_OLEH_POLRI_Oleh_Kombes_Pol_Drs.

[25] Ahmad M. Ramli, *Perencanaan pembangunan hukum nasional bidang teknologi informasi dan komunikasi* (Badan Pembinaan Hukum Nasional, Departemen Hukum dan Hak Asasi Manusia RI, 2009).

mengurangi peluang terjadinya tindak pidana carding, misalnya melalui kegiatan penyuluhan dan patroli internet[26].

Pemerintah kemudian mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai upaya untuk mengatur cybercrime. Namun, seiring dengan pesatnya perkembangan teknologi, undang-undang ini direvisi melalui Undang-Undang Nomor 19 Tahun 2016. Revisi tersebut bertujuan untuk menciptakan regulasi yang lebih harmonis dan mampu mengantisipasi perubahan di bidang teknologi informasi. Meskipun Indonesia telah memiliki UU ITE beserta revisinya sebagai hukum positif, regulasi ini masih menghadapi tantangan dalam menjerat pelaku kejahatan siber. Pembuktian dalam kasus-kasus yang melibatkan teknologi informasi sering kali sulit karena sifat kejahatannya yang kompleks dan bukti-bukti yang sulit diakses[27]. Oleh karena itu, perbaikan dan penyempurnaan regulasi tetap diperlukan agar hukum dapat berfungsi secara efektif dalam menangani kejahatan dunia maya.

Kejahatan carding di Indonesia dapat diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) melalui interpretasi ekstensif terhadap beberapa pasal, seperti Pasal 362 dan 363 tentang pencurian serta Pasal 378 tentang penipuan. Meskipun KUHP mencakup kejahatan tersebut, modus operandi carding lebih spesifik diatur dalam Undang-Undang Nomor 19 Tahun 2016, yang merupakan revisi dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai *lex spesialis*. Dalam UU ITE, Pasal 30 jo Pasal 46 mengatur pencurian data elektronik, sedangkan Pasal 35 jo Pasal 51 ayat (1) atau Pasal 32 jo Pasal 48 mengatur penipuan yang dilakukan melalui teknologi. Sanksi bagi pelaku carding juga diatur secara khusus dalam UU ITE, terutama

[26] Bambang Hartono and Recca Ayu Hapsari, "Mutual Legal Assistance Pada Pemberantasan Cyber Crime Lintas Yurisdiksi Di Indonesia," *SASI* 25, no. 1 (August 24, 2019): 59–71, https://doi.org/10.47268/sasi.v25i1.136.

[27] Gert Jan van Hardeveld, Craig Webber, and Kieron O'Hara, "Discovering Credit Card Fraud Methods in Online Tutorials," in *Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention*, OnSt '16 (New York, NY, USA: Association for Computing Machinery, 2016), 1–5, https://doi.org/10.1145/2915368.2915369.

pada Pasal 46, 47, 48, 50, dan 51, yang mencakup pidana penjara dan/atau denda. Namun, penerapan pasal-pasal ini tidak lepas dari kendala, terutama dalam investigasi yang sering kali kesulitan melacak identitas dan lokasi pelaku akibat kompleksitas jaringan internet yang digunakan[28].

Penegakan hukum terhadap kejahatan *carding* perlu memuat asas-asas hukum untuk memastikan efektivitasnya. Menurut Gustav Radbruch, hukum harus memenuhi tiga nilai utama: kepastian hukum, keadilan hukum, dan kemanfaatan hukum[29]. Asas kepastian hukum menuntut adanya aturan yang jelas dan logis dalam perundangan, yang dalam kasus *carding*, telah diatur secara jelas melalui UU ITE. Namun, meskipun sudah ada undang-undang ini, kejahatan *carding* masih marak terjadi karena adanya celah yang dimanfaatkan oleh para pelaku[30]. Dalam upaya pencegahan dan penanggulangan kejahatan *carding*, teori volgeist dari Friedrich Carl von Savigny menekankan bahwa hukum harus berkembang bersama masyarakat. Oleh karena itu, masyarakatlah yang mendorong negara untuk merumuskan hukum demi terciptanya keseimbangan dan keadilan dalam masyarakat[31]. Dengan semakin maraknya kejahatan baru akibat perkembangan teknologi, diperlukan perbaikan dalam KUHP, terutama dengan menambahkan alat bukti berbasis teknologi seperti surat elektronik dan rekaman digital untuk menangani kejahatan di dunia maya.

Kejahatan cyber seperti *carding* sering kali melibatkan jaringan telematika global yang membuat batas-batas yurisdiksi menjadi kabur. Hal ini menyulitkan dalam menentukan *locus delicti* dan menjerat pelaku yang mungkin berada di negara berbeda. Oleh karena itu, lembaga penafsiran hukum (interpretasi) sangat diperlukan untuk menyesuaikan hukum dengan situasi baru ini, agar tidak terjadi

---

[28] Ginara, Widyantara, and Styawati, "Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime dalam Hukum Pidana Indonesia."

[29] Sudikno Mertokusumo, *Mengenal hukum (suatu pengantar)* (Liberty, 1986).

[30] Khoirotun Nisa, "Urgensi Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi Dan Transaksi Elektronik Dalam Penanganan Atas Kejahatan Carding Di Bank X," *Journal of Islamic Business Law* 4, no. 3 (2020): 1–11.

[31] Hartono and Hapsari, "Mutual Legal Assistance Pada Pemberantasan Cyber Crime Lintas Yurisdiksi Di Indonesia."

kekosongan hukum yang dapat dimanfaatkan oleh pelaku kejahatan di dunia maya[32]. Pengaturan kejahatan carding lebih tepat dimasukkan dalam UU ITE sebagai *lex spesialis*, tetapi KUHP masih bisa diterapkan sebagai *lex generalis*, tergantung pada pertimbangan hakim dalam kasus tertentu. UU ITE menitikberatkan pada sanksi pidana penjara dan denda, yang tercantum dalam Pasal 45 hingga Pasal 52. Karena kejahatan carding berbeda dari kejahatan konvensional lainnya, diperlukan penafsiran hukum yang mendalam untuk memastikan peraturan dapat mengikuti perkembangan kejahatan di era digital ini[33].

Ruang siber atau cyberspace adalah dunia virtual yang memiliki dampak nyata pada kehidupan sehari-hari. Untuk mengatur aktivitas dalam ruang ini, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) digunakan selain KUHP, yang menegaskan bahwa kegiatan virtual bisa dikategorikan sebagai tindakan hukum yang nyata[34]. UU ITE telah memenuhi standar internasional sesuai dengan *Convention on Cybercrime*. Namun, beberapa ketentuan dalam UU ITE, seperti mengenai akses ilegal dan intersepsi, telah dicabut dan direformulasi melalui Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (UU KUHP).

Pasal terkait akses ilegal yang sebelumnya diatur dalam Pasal 30 jo. Pasal 46 UU ITE telah dicabut dan digantikan oleh Pasal 322 UU KUHP. Pasal 322 ini menetapkan sanksi pidana bagi tindakan mengakses komputer atau sistem elektronik orang lain secara ilegal, dengan ancaman hukuman penjara hingga 8 tahun dan/atau denda kategori V hingga VI. Reformulasi ini mengintegrasikan aturan yang lebih sistematis dan sesuai dengan perkembangan teknologi serta

---

[32] M. M. Naufal and H. Sofwan Jannah, "Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam," *Al-Mawarid: Jurnal Hukum Islam* 12, no. 1 (2012): 42565.

[33] Raden Dimas Ari Wibowo Dimas and Vivi Arfiani Siregar, "FENOMENA KEJAHATAN CARDING BERDASARKAN DALAM HUKUM PIDANA INDONESIA:," *JURNAL HUKUM DAS SOLLEN* 6, no. 2 (December 30, 2021): 99–124, https://doi.org/10.32520/das-sollen.v6i2.1833.

[34] Antonius Maria Laot Kian, "Tindak Pidana Credit/Debit Card Fraud dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia," *Hasanuddin Law Review* 1, no. 1 (May 17, 2015): 47–60, https://doi.org/10.20956/halrev.v1i1.39.

praktik kejahatan siber saat ini. Intersepsi atau penyadapan, yang sebelumnya diatur dalam Pasal 31 jo. Pasal 47 UU ITE, juga telah dicabut dan digantikan oleh Pasal 258 UU KUHP[35]. Pasal ini mengatur sanksi pidana bagi pelaku intersepsi ilegal, dengan ancaman penjara hingga 10 tahun dan/atau denda kategori VI, yang mencapai maksimal Rp 2 miliar. Undang-Undang KUHP menerapkan ancaman denda yang lebih tinggi dibandingkan dengan UU ITE, menunjukkan peningkatan perlindungan terhadap privasi dalam dunia digital.

UU KUHP baru ini juga membawa perubahan dalam cara rumusan delik dan sanksi pidana ditetapkan. Jika UU ITE memisahkan antara rumusan delik dan sanksi, UU KUHP menyatukan kedua unsur tersebut dalam satu pasal atau ayat. Hal ini memudahkan pemahaman dan penerapan hukum, serta memberikan kepastian hukum yang lebih jelas dalam menangani kasus kejahatan siber. Pada awal tahun 2024, pemerintah mengesahkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE. Undang-Undang ini menambahkan sejumlah pasal baru, seperti Pasal 13A, 16A, 16B, 18A, 27A, 27B, dan 40A, yang memperluas pengaturan terkait layanan dan kewajiban penyelenggara sertifikasi elektronik serta perlindungan anak dalam penggunaan sistem elektronik. Secara khusus, Pasal 13A UU No. 1 Tahun 2024 mengatur layanan yang bisa diberikan oleh Penyelenggara Sertifikasi Elektronik (PSE), termasuk tanda tangan elektronik, segel elektronik, dan identitas digital, menekankan pentingnya perlindungan data dan identitas digital di era digital yang semakin terhubung[36]. Tetapi demikian reformulasi delik *cybercrime* dalam UU KUHP 2023 menunjukkan kemajuan normatif, pembaruan tersebut masih berorientasi pada penguatan hukum pidana nasional semata. Tanpa dukungan mekanisme kerja sama internasional yang mengikat sebagaimana diatur dalam *Convention on Cybercrime*, efektivitas pengaturan tersebut tetap bersifat terbatas dan parsial.

---

[35] "Aturan Akses Ilegal Dan Penyadapan Dalam KUHP Baru," accessed August 26, 2024, https://nasional.kompas.com/read/2023/03/05/10105771/aturan-akses-ilegal-dan-penyadapan-dalam-kuhp-baru.

[36] "UU 1/2024: Perubahan Kedua UU No. 11 Tahun 2008 tentang ITE," accessed August 26, 2024, https://jdih.maritim.go.id/uu-12024-perubahan-kedua-uu-no-11-tahun-2008-tentang-ite.

Pasal 16A dalam undang-undang yang sama menetapkan tanggung jawab bagi Penyelenggara Sertifikasi Elektronik (PSE) untuk menyediakan perlindungan khusus bagi anak-anak yang menggunakan atau mengakses sistem elektronik. Perlindungan ini mencakup penyampaian informasi mengenai batas usia minimum, mekanisme verifikasi pengguna anak, dan prosedur pelaporan jika terjadi penyalahgunaan yang melanggar hak anak. UU No. 1 Tahun 2024 juga mengintroduksi sanksi administratif bagi PSE yang melanggar ketentuan perlindungan anak, seperti peringatan tertulis, denda administratif, penghentian sementara, atau pemutusan akses. Dengan demikian, undang-undang ini memperkuat perlindungan terhadap kelompok rentan seperti anak-anak di ruang siber. Perubahan-perubahan ini mencerminkan perkembangan regulasi di Indonesia untuk menyesuaikan dengan dinamika dunia digital. Penekanan pada penegakan hukum yang ketat terhadap kejahatan siber, dengan hukuman yang lebih berat dan denda yang lebih tinggi, mencerminkan komitmen pemerintah dalam melindungi hak digital warga negara di era digital ini.

Penanganan *cybercrime* sering kali melibatkan konflik yurisdiksi antara negara-negara yang terlibat, karena masing-masing negara memiliki pendekatan yang berbeda dalam menetapkan wewenang yurisdiksi mereka. Di Indonesia, yurisdiksi terkait *cybercrime* diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Namun, undang-undang ini belum sepenuhnya mengakomodasi semua bentuk kejahatan yang diatur dalam *Convention on Cybercrime*, terutama dalam hal penetapan yurisdiksi dan kerja sama internasional yang belum diatur secara komprehensif[37].

Pada kategori pertama, *Convention on Cybercrime* menetapkan jenis-jenis kejahatan yang harus diatur oleh negara-negara anggotanya, sedangkan kategori kedua, prosedur hukum diatur dalam konvensi ini untuk menangani kejahatan tersebut, termasuk penetapan dasar yurisdiksi. Di Indonesia, penegakan hukum terkait yurisdiksi cybercrime merujuk pada prinsip-prinsip yang diatur dalam

[37] Mubaraq, "TINJAUAN YURIDIS TINDAK PIDANA PERETASAN KARTU KREDIT MELALUI INTERNET ATAU CARDING TERHADAP WARGA NEGARA ASING (Studi Putusan Nomor 102/Pid.Sus/ PN. Wns)."

Kitab Undang-Undang Hukum Pidana (KUHP). Namun, Indonesia belum sepenuhnya mengadopsi prinsip-prinsip kerjasama internasional yang diatur oleh konvensi ini, sehingga masih terdapat kekosongan hukum yang dapat menimbulkan tantangan dalam menangani kasus cybercrime lintas negara[38].

Kejahatan *carding* adalah salah satu bentuk *cybercrime* yang dapat dikategorikan sebagai kejahatan transnasional terorganisir, sesuai dengan ketentuan dalam Article 3 Paragraph 2 dan Article 5 Paragraph 1 United Nations Convention Against Transnational Organized Crime (UNTOC). Kejahatan transnasional tidak hanya melintasi batas negara, tetapi juga mencakup kejahatan yang dilakukan di satu negara namun berdampak pada negara lain[39]. Hal ini sangat relevan dalam kasus *carding*, di mana pelaku kejahatan dapat mencuri data kartu kredit dari nasabah di negara lain dan menggunakan data tersebut untuk transaksi internasional.

Philip C. Jessup adalah orang yang pertama kali memperkenalkan istilah *transnational crime* untuk membedakannya dari *international crime.*[40] Menurut Bassiouni, kejahatan transnasional melibatkan lebih dari satu negara, baik dari segi dampak, sarana, maupun metode yang digunakan, dan melintasi batas-batas negara[41]. Dalam konteks carding, pencurian data kartu kredit sering kali melibatkan pelaku dan korban dari berbagai negara, menunjukkan sifat lintas batas yang kompleks dari kejahatan ini. UNTOC, atau *The Palermo Convention*,

---

[38] Ermanto Fahamsyah et al., "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention," *De Jure: Jurnal Hukum dan Syar'iah* 14, no. 1 (June 29, 2022): 140–59, https://doi.org/10.18860/j-fsh.v14i1.15731.

[39] Intan Soeparna, "Kejahatan Telematika Sebagai Kejahatan Transnasional," *Fakultas Hukum, Universitas Airlangga*, Agustus 2008, https://www.academia.edu/208360/Kejahatan_Telematika_sebagai_Kejahatan_Transnasional.

[40] Roni Gunawan Raja Gukguk and Nyoman Serikat Putra Jaya, "TINDAK PIDANA NARKOTIKA SEBAGAI TRANSNASIONAL ORGANIZED CRIME," *Jurnal Pembangunan Hukum Indonesia* 1, no. 3 (September 24, 2019): 337–51, https://doi.org/10.14710/jphi.v1i3.337-351.

[41] Stefanus Andika, "PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA LINTAS NEGARA MELALUI PERJANJIAN EKSTRADISI (SUATU CATATAN MENARIK UNTUK DISKUSI)," *Era Hukum - Jurnal Ilmiah Ilmu Hukum* 16 (July 3, 2019), https://doi.org/10.24912/erahukum.v16i2.4532.

berfungsi sebagai kerangka hukum internasional utama untuk mengatur kejahatan transnasional terorganisir. Pasal 3 ayat (2) konvensi ini menjelaskan karakteristik lintas batas dari kejahatan transnasional, mencakup kejahatan yang dilakukan di lebih dari satu negara atau yang perencanaannya dilakukan di satu negara tetapi berdampak pada negara lain. Ini sangat relevan dalam kasus carding, di mana aktivitas kriminal sering kali melibatkan kolaborasi internasional dan teknologi internet yang tidak mengenal batas.

Masalah yurisdiksi sangat krusial dalam menangani kejahatan carding karena sifatnya yang internasional dari kejahatan ini. Yurisdiksi merujuk pada kekuasaan hukum suatu negara atas individu, objek, atau peristiwa yang terjadi di wilayahnya. Dalam hukum internasional, yurisdiksi biasanya didasarkan pada batas-batas geografis negara. Namun, dengan adanya komunikasi multimedia yang bersifat global dan tanpa batas, penetapan yurisdiksi menjadi lebih rumit dan menantang. Untuk mengatasi tantangan yurisdiksi dalam cybercrime, berbagai asas digunakan untuk menentukan hukum yang berlaku, seperti asas *territoriality, nationality, passive nationality, protective principle, dan universality*[42]. Asas *universality*, khususnya, sangat penting dalam menangani kasus cybercrime, karena hukum dapat diterapkan secara universal terhadap kejahatan yang dianggap mengancam komunitas internasional.

Yurisdiksi juga mencerminkan kedaulatan negara, yang memungkinkan negara untuk menciptakan, mengubah, atau mengakhiri hubungan atau kewajiban hukum. Berdasarkan prinsip umum dalam hukum internasional, setiap negara memiliki kedaulatan atas individu dan objek di wilayahnya sendiri. Namun, negara tidak dapat mengambil tindakan di wilayah negara lain tanpa izin, sehingga kerja sama internasional menjadi penting dalam penegakan hukum terhadap kejahatan siber lintas batas. Dengan demikian, untuk menangani kejahatan *carding* yang bersifat transnasional, Indonesia perlu memperkuat regulasi dan kerja sama internasional. Penegakan hukum yang lebih dapat menyesuaikan dengan perkembangan teknologi informasi dan komunikasi juga

[42] Asep Ahmad Fauji, "PENERAPAN PRINSIP UNCITRAL MODEL LAW DALAM PEMBUKTIAN KASUS TRANSAKSI ELEKTRONIK DI INDONESIA," *University Of Bengkulu Law Journal* 2, no. 1 (April 22, 2017): 90–102, https://doi.org/10.33369/ubelaj.2.1.90-102.

dibutuhkan dalam memastikan yurisdiksi yang lebih jelas dan efektif dalam rangka pemberantasan kejahatan di dunia maya.

Yurisdiksi suatu negara dapat dibedakan menjadi dua, yaitu yurisdiksi perdata dan pidana. Yurisdiksi perdata berfokus pada kewenangan hukum suatu negara dalam menangani kasus yang melibatkan hukum privat, baik yang memiliki unsur nasional maupun asing. Sementara itu, yurisdiksi pidana berkaitan dengan kewenangan negara dalam menindak pelanggaran hukum publik yang melibatkan unsur asing. Dalam konteks internasional, asas *aut dedere aut judicare* menjadi pedoman penting dalam menangani tindak pidana, termasuk kejahatan siber. Asas ini menekankan kewajiban setiap negara untuk bekerja sama dengan negara lain dalam menuntut dan mengadili pelaku tindak pidana internasional, yang sering kali melibatkan berbagai yurisdiksi. Tanpa ratifikasi *Convention on Cybercrime*, *asas aut dedere aut judicare* tidak memiliki daya operasional dalam praktik penegakan hukum di Indonesia. Ratifikasi konvensi ini akan mentransformasikan asas tersebut dari sekadar norma hukum internasional abstrak menjadi kewajiban hukum konkret yang dapat diimplementasikan melalui mekanisme ekstradisi dan *mutual legal assistance*.

Menghadapi tantangan yurisdiksi di dunia maya, teori Darrel Menthe mengemukakan bahwa interaksi dalam dunia virtual terutama didasarkan pada pemberian dan pengambilan informasi[43]. Yurisdiksi dalam dunia maya menjadi lebih kompleks karena melibatkan interaksi lintas batas yang tidak selalu mudah diidentifikasi secara geografis. Untuk mengatasi kejahatan siber yang berdampak luas, prinsip yurisdiksi ekstrateritorial menjadi sangat relevan. Dalam prinsip tersebut, setiap negara memungkinkan dalam memberikan tuntutan kepada pelaku kejahatan yang dalam melakukan kejahatannya tersebut, pelaku berada di laur wilayah negara yang dirugikan, dan memberikan kerugian yang besar bagi negara tersebut. Pasal 2 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), mengatur permasalahan tersebut, yang berisi bahwa peraturan tersebut berlaku bagi semua orang yang berada di Indonesia

[43] Sahat Maruli Tua Situmeang, "Cyber Law" (CV Cakra, 2020), https://elibrary.unikom.ac.id/id/eprint/4445/.

maupun di luar wilayah, dimana tindakan mereka tersebut berdampak hukum di Indonesia[44].

Penerapan prinsip yurisdiksi ekstrateritorial ini menimbulkan tantangan dalam praktiknya, terutama terkait dengan pengakuan dan ratifikasi oleh negara lain. Tanpa ratifikasi oleh negara lain, pemberlakuan prinsip ini tidak dapat secara efektif mengikat negara-negara tersebut, meskipun UU ITE telah mengatur ketentuan tersebut. Diperlukan pengaturan khusus dalam konteks kejahatan siber, yang mana memiliki karakteristik yang berbeda dengan tindak pidana konvensional, yaitu mulai dari modus operandi, pelaku, hingga oada tempat kejadian perkara. Oleh karena itu, UU ITE di Indonesia dirancang untuk melengkapi Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dalam mengatasi kejahatan siber.

Dalam hal pembuktian, kejahatan siber sering kali menimbulkan dilema karena hukum diharapkan untuk mengikuti perkembangan teknologi. Pada saat yang sama, ada kebutuhan untuk pengakuan hukum terhadap alat bukti digital dalam proses pengadilan. Pengaturan ini penting untuk memastikan bahwa alat bukti digital dapat diterima dan memiliki kekuatan yang cukup di pengadilan. Secara keseluruhan, penerapan hukum dalam mengatasi kejahatan siber memerlukan pendekatan yang komprehensif dan kerja sama internasional. Meskipun Indonesia telah mengatur hal ini dalam UU ITE, tantangan yang dihadapi adalah memastikan bahwa prinsip-prinsip yurisdiksi yang diterapkan dapat diakui dan dijalankan secara efektif oleh negara-negara lain, terutama dalam menghadapi kejahatan siber yang lintas batas. Pembuktian dalam proses pemeriksaan di pengadilan memegang peranan penting karena menentukan apakah seseorang yang diadili terbukti bersalah atau tidak. Pembuktian yang didasarkan pada alat bukti yang sah sesuai dengan undang-undang menjadi dasar keputusan untuk menjatuhkan hukuman atau membebaskan terdakwa. Oleh karena itu, proses pembuktian harus dilakukan dengan sangat hati-hati, teliti, dan penuh pertimbangan guna memastikan keadilan.

[44] Apriolla, *TINDAK PIDANA KEJAHATAN UU ITE* (GUEPEDIA, n.d.).

Dalam konteks kejahatan carding yang sering melibatkan lintas negara, prinsip kedaulatan negara harus dihormati. Indonesia tidak dapat sembarangan menangkap dan mengadili pelaku kejahatan yang berada di luar yurisdiksinya. Kerja sama internasional menjadi solusi utama untuk menghadapi kejahatan yang bersifat transnasional ini. Opsi yang diberikan *Convention on Cybercrime* kepada negara-negara pihak untuk melakukan ekstradisi atau *Mutual Legal Assistance* (MLA) dimana memberikan kemungkinan bagi negara untuk melakukan tuntutan dan mengadili pelaku dari kejahatan siber. Ketentuan ini menegaskan bahwa apabila tidak ada perjanjian ekstradisi antara dua negara, konvensi ini dapat digunakan sebagai dasar untuk meminta ekstradisi.

Mekanisme kerjasama internasional yang diatur dalam *Convention on Cybercrime* sangat menguntungkan bagi Indonesia dalam upaya pemberantasan *cybercrime*, termasuk *carding*. Dukungan dapat diperoleh Indonesia dalam melakukan penegakan hukum dan memberantas terhadap pelaku dari kejahatan siber, dengan catatan pelaku kejahatan tersebut berada pada yuridksi dari 68 negara yang menjadi anggota konvensi. Dengan demikian, harapannya dapat menciptakan pola pemberantasan yang lebih terkoordinasi dan efektif.

Dalam pelaksanaannya, *National Central Bureau* (NCB) Interpol Indonesia biasanya menerima laporan mengenai seorang warga negara lain yang menjadi korban dari negara ketika terjadi kejahatan carding lintas batas. Setelah menerima laporan tersebut, Unit Kejahatan Siber Polri dan NCB Interpol Indonesia dapat bekerja sama untuk menyelidiki dan menentukan apakah penyelidikan lebih lanjut diperlukan. Tahap penting lainnya dalam proses ini adalah kolaborasi internasional dengan NCB negara lain tempat korban berada[45].

Teknik modern seperti telekonferensi untuk mendapatkan kesaksian dari saksi korban yang berada di luar negeri dapat digunakan sebagai alat bukti dalam persidangan kasus carding. Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) menyatakan dalam Pasal 44 bahwa dokumen dan informasi elektronik, termasuk hasil telekonferensi, dapat diterima

[45] Danne Dean Vanessa, "Proses Penyelidikan Kejahatan Carding Lintas Negara - Hukum / Diskusi Hukum," Dictio Community, April 24, 2018, https://www.dictio.id/t/proses-penyelidikan-kejahatan-carding-lintas-negara/51562.

sebagai alat bukti. Klausul ini memungkinkan untuk menangani prosedur pembuktian dalam kasus carding dengan cara yang lebih fleksibel dan efektif. Selain itu, komunitas hukum Indonesia telah mengadopsi model pemeriksaan saksi jarak jauh berbasis telekonferensi. Hal ini menghilangkan kebutuhan untuk pertemuan tatap muka dengan memungkinkan komunikasi suara atau video antara para pihak. Meskipun merupakan teknologi yang sudah mapan, memasukkannya ke dalam sistem hukum merupakan langkah penting untuk memastikan bahwa hukum acara pidana dapat mengikuti kemajuan teknologi[46].

Namun, meskipun ketentuan alat bukti konvensional sudah diakomodasi oleh pembaruan hukum acara pidana, penanganan kejahatan *carding* memerlukan ketentuan khusus. Hal ini disebabkan oleh karakteristik unik dari *cybercrime*, yang modus operandinya berbeda dari tindak pidana konvensional. Oleh karena itu, pendekatan hukum yang digunakan tidak cukup hanya dengan mengandalkan Kitab Undang-Undang Hukum Pidana (KUHP) saja, tetapi juga membutuhkan perangkat hukum yang lebih spesifik seperti UU ITE. Jika pelaku *carding* berada di luar Indonesia, penegak hukum seperti Polri atau Jaksa Agung dapat meminta bantuan Interpol untuk menangkap pelaku. Setelah ditangkap, permintaan ekstradisi dapat diajukan melalui jalur diplomatik, sesuai dengan ketentuan Pasal 44 Undang-Undang Nomor 1 Tahun 1979 tentang Ekstradisi. Jika tidak ada perjanjian ekstradisi dengan negara tempat pelaku berada, Indonesia dapat menggunakan pendekatan diplomatik dan mengajukan *Mutual Legal Assistance* (MLA) untuk meminta ekstradisi[47].

Dalam kejahatan siber lintas batas, pembuktian tidak dapat dilepaskan dari persoalan yurisdiksi, karena alat bukti digital kerap berada di bawah penguasaan otoritas asing. Tanpa mekanisme kerja sama internasional yang efektif, pembuktian menjadi tidak optimal dan berpotensi menggugurkan proses penuntutan. Dengan memanfaatkan instrumen hukum internasional seperti

[46] Fathul Wahid, "Kamus Istilah Teknologi Informasi," *Yogyakarta: Andi*, 2002, https://scholar.google.com/scholar?cluster=17635279872035410263&hl=en&oi=scholarr.

[47] Humas, "Sepintas Mengenal Hukum Ekstradisi (Bagian Pertama)," Sekretariat Kabinet Republik Indonesia, January 31, 2023, https://setkab.go.id/sepintas-mengenal-hukum-ekstradisi-bagian-pertama/.

Convention on Cybercrime dan mengintegrasikan ketentuan yang ada dalam undang-undang nasional seperti UU ITE dan UU Ekstradisi, Indonesia dapat meningkatkan efektivitas pemberantasan kejahatan *carding* dan *cybercrime* secara umum.

4. Kesimpulan

Pencegahan carding di Indonesia memerlukan ratifikasi Convention on Cybercrime untuk memperkuat kerangka hukum internasional dalam menangani kejahatan siber lintas negara. Dengan melakukan ratifikasi tersebut, Indonesia dapat memperbaiki kerjasama internasional, harmonisasi hukum, dan respons terhadap ancaman kejahatan siber, sambil memastikan perlindungan yang lebih baik terhadap sistem keuangan dan data pribadi masyarakat. Selain itu, pembaruan undang-undang, khususnya terkait cybercrime juga diperlukan. Meskipun saat ini Indonesia telah memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), peraturan tersebut belum sepenuhnya mencakup seluruh aspek carding yang berkembang pesat. Sehingga diperlukan peraturan yang lebih spesifik dan mutakhir, agar penegakan hukum dapat lebih efektif dalam menghadapi ancaman yang semakin canggih. Dengan adanya regulasi yang lebih komprehensif, penegakan hukum akan lebih efektif dalam mengatasi kasus carding dan mencegah kerugian finansial serta kerusakan reputasi yang dapat ditimbulkan dari kejahatan siber.

5. Informasi Pendanaan

Tidak ada

6. Ucapan Terima Kasih

Ucapan terima kasih ditujukan kepada semua pihak-pihak yang terlibat dan bersedia memberikan bantuan dan dukungannya dalam kelancaran

penelitian ini. Peneliti juga memberikan ucapan terima kasih kepada keluarga, dosen pembimbing, serta semua pihak terkait lainnya yang bersedia berpartisipasi dan bekerjasama dalam upaya menyelesaikan penelitian ini.

7. Referensi

Adolf, Huala. *Hukum Perdagangan Internasional*. Pt Rajagrafindo Persada, 2020.

Ali, Zainuddin. *Metode Penelitian Hukum*. Sinar Grafika, 2021.

Amirullah, Amirullah. "Arti Penting Ratifikasi European Union Convention on Cybercrime 2001 Bagi Indonesia." Universitas Padjajaran, 2008.

Andika, Stefanus. "PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA LINTAS NEGARA MELALUI PERJANJIAN EKSTRADISI (SUATU CATATAN MENARIK UNTUK DISKUSI)." *Era Hukum - Jurnal Ilmiah Ilmu Hukum* 16 (July 3, 2019). https://doi.org/10.24912/erahukum.v16i2.4532.

Apriolla. *TINDAK PIDANA KEJAHATAN UU ITE*. GUEPEDIA, n.d.

Aslam, Zulfiqar Hafizh. "CARDING SEBAGAI BENTUK BUDAYA KONSUMERISME MODERN : STUDI KASUS KOMUNITAS SKATEBOARD SURABAYA." Undergraduate, UIN Sunan Ampel Surabaya, 2014. http://digilib.uinsa.ac.id/437/.

"Aturan Akses Ilegal Dan Penyadapan Dalam KUHP Baru." Accessed August 26, 2024. https://nasional.kompas.com/read/2023/03/05/10105771/aturan-akses-ilegal-dan-penyadapan-dalam-kuhp-baru.

Dimas, Raden Dimas Ari Wibowo, and Vivi Arfiani Siregar. "FENOMENA KEJAHATAN CARDING BERDASARKAN DALAM HUKUM PIDANA INDONESIA:" *JURNAL HUKUM DAS SOLLEN* 6, no. 2 (December 30, 2021): 99–124. https://doi.org/10.32520/das-sollen.v6i2.1833.

dob. "Ada 5.000 Kasus Perbulan, Indonesia Emergency Kejahatan Siber." CNBC Indonesia. Accessed August 24, 2024.

https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber.

Enggarani, Nuria Siswi. "PENANGGULANGAN KEJAHATAN INTERNET DI INDONESIA," September 2012. http://publikasiilmiah.ums.ac.id/handle/11617/4010.

Fahamsyah, Ermanto, Vicko Taniady, Kania Venisa Rachim, and Novi Wahyu Riwayanti. "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention." *De Jure: Jurnal Hukum dan Syar'iah* 14, no. 1 (June 29, 2022): 140–59. https://doi.org/10.18860/j-fsh.v14i1.15731.

Fauji, Asep Ahmad. "PENERAPAN PRINSIP UNCITRAL MODEL LAW DALAM PEMBUKTIAN KASUS TRANSAKSI ELEKTRONIK DI INDONESIA." *University Of Bengkulu Law Journal* 2, no. 1 (April 22, 2017): 90–102. https://doi.org/10.33369/ubelaj.2.1.90-102.

Galih, Yuliana Surya. "YURISDIKSI HUKUM PIDANA DALAM DUNIA MAYA." *Jurnal Ilmiah Galuh Justisi* 7, no. 1 (June 20, 2019): 59–74. https://doi.org/10.25157/jigj.v7i1.2138.

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 (February 27, 2022): 138–42. https://doi.org/10.22225/jph.3.1.4673.138-142.

Gukguk, Roni Gunawan Raja, and Nyoman Serikat Putra Jaya. "TINDAK PIDANA NARKOTIKA SEBAGAI TRANSNASIONAL ORGANIZED CRIME." *Jurnal Pembangunan Hukum Indonesia* 1, no. 3 (September 24, 2019): 337–51. https://doi.org/10.14710/jphi.v1i3.337-351.

Hardani, Nur Hikmatul Auliya, Helmina Andriani, Roushandy Asri Fardani, Jumari Ustiawaty, Evi Fatmi Utami, Dhika Juliana Sukmana, and Ria Rahmatul Istiqomah. *Metode Penelitian Kualitatif & Kuantitatif*. CV. Pustaka Ilmu, 2020.

Hardeveld, Gert Jan van, Craig Webber, and Kieron O'Hara. "Discovering Credit Card Fraud Methods in Online Tutorials." In *Proceedings of the 1st*

International Workshop on Online Safety, Trust and Fraud Prevention, 1–5. OnSt '16. New York, NY, USA: Association for Computing Machinery, 2016. https://doi.org/10.1145/2915368.2915369.

Hartono, Bambang, and Recca Ayu Hapsari. "Mutual Legal Assistance Pada Pemberantasan Cyber Crime Lintas Yurisdiksi Di Indonesia." *SASI* 25, no. 1 (August 24, 2019): 59–71. https://doi.org/10.47268/sasi.v25i1.136.

Humas. "Sepintas Mengenal Hukum Ekstradisi (Bagian Pertama)." Sekretariat Kabinet Republik Indonesia, January 31, 2023. https://setkab.go.id/sepintas-mengenal-hukum-ekstradisi-bagian-pertama/.

Kian, Antonius Maria Laot. "Tindak Pidana Credit/Debit Card Fraud dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia." *Hasanuddin Law Review* 1, no. 1 (May 17, 2015): 47–60. https://doi.org/10.20956/halrev.v1i1.39.

KOMINFO, PDSI. "Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber." Website Resmi Kementerian Komunikasi dan Informatika RI. Accessed August 25, 2024. http:///index.php/content/detail/4698/Indonesia-Peringkat-ke-2-Dunia-Kasus-Kejahatan-Siber/0/sorotan_media.

Mertokusumo, Sudikno. *Mengenal hukum (suatu pengantar)*. Liberty, 1986.

Mubaraq, Akhdiyat. "TINJAUAN YURIDIS TINDAK PIDANA PERETASAN KARTU KREDIT MELALUI INTERNET ATAU CARDING TERHADAP WARGA NEGARA ASING (Studi Putusan Nomor 102/Pid.Sus/ PN. Wns)." Other, UNIVERSITAS HASANUDDIN, 2021. https://repository.unhas.ac.id/id/eprint/11544/.

Naufal, M. M., and H. Sofwan Jannah. "Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam." *Al-Mawarid: Jurnal Hukum Islam* 12, no. 1 (2012): 42565.

Nisa, Khoirotun. "Urgensi Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi Dan Transaksi Elektronik Dalam Penanganan Atas Kejahatan Carding Di Bank X." *Journal of Islamic Business Law* 4, no. 3 (2020): 1–11.

Obi, Ndifon Neji, and Sovereign Felix Nyong. "Rethinking Civil Society Participation in the Implementation of the UN Convention Against

Corruption in Nigeria." *Journal of Economics and Sustainable Development* 9, no. 16 (2018): 16.

Putra, Akbar Kurnia. "HARMONISASI KONVENSI CYBER CRIME DALAM HUKUM NASIONAL." *Jurnal Ilmu Hukum* 5, no. 2 (2015). https://scholar.google.co.id/citations?view_op=view_citation&hl=en&user=7-B5s7EAAAAJ&citation_for_view=7-B5s7EAAAAJ:ULOm3_A8WrAC.

Putra, Dea Alamanda. "ANALISIS YURIDIS PEMIDANAAN TERHADAP PELAKU TINDAK PIDANA CARDING (STUDI KASUS DI DITRESKIRMSUS POLDA JATENG)." Other, Universitas Negeri Semarang, 2017. https://lib.unnes.ac.id/30219/.

Raharjo, Agus. *Cybercrime: pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti, 2002.

Ramli, Ahmad M. *Perencanaan pembangunan hukum nasional bidang teknologi informasi dan komunikasi*. Badan Pembinaan Hukum Nasional, Departemen Hukum dan Hak Asasi Manusia RI, 2009.

Setyo, Adi. "BULETIN HUKUM PERBANKAN DAN KEBANKSENTRALAN 29 Volume 4 Nomor 2, Agustus 2006 PERKEMBANGAN CYBERCRIME DAN UPAYA PENANGANANNYA DI INDONESIA OLEH POLRI Oleh : Kombes (Pol) Drs." Accessed August 26, 2024. https://www.academia.edu/4941347/BULETIN_HUKUM_PERBANKAN_DAN_KEBANKSENTRALAN_29_Volume_4_Nomor_2_Agustus_2006_PERKEMBANGAN_CYBERCRIME_DAN_UPAYA_PENANGANANNYA_DI_INDONESIA_OLEH_POLRI_Oleh_Kombes_Pol_Drs.

Sinaga, V. Selvie. *Hukum Perjanjian Internasional: Diskursus Tentang Konvensi wina 1969*. Penerbit Unika Atma Jaya Jakarta, 2019.

Situmeang, Sahat Maruli Tua. "Cyber Law." CV Cakra, 2020. https://elibrary.unikom.ac.id/id/eprint/4445/.

Soekanto, Soerjono, and Sri Mamudji. *Penelitian hukum normatif: suatu tinjauan singkat*. Penerbit CV. Rajawali, 1986.

Soeparna, Intan. "Kejahatan Telematika Sebagai Kejahatan Transnasional." *Fakultas Hukum, Universitas Airlangga*, Agustus 2008.

https://www.academia.edu/208360/Kejahatan_Telematika_sebagai_Kejahatan_Transnasional.

Sudaryono, Sudaryono, and Natangsa Subakti. *HUKUM PIDANA Dasar-Dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP*. Muhammadiyah University Press, 2022.

Sugiyono. *Metode penelitian kuantitatif, kualitatif dan R&D*. Bandung: Alfabeta, 2020.

Sumarwani, S. "TINJAUAN YURIDIS PEMIDANAAN CYBERCRIME DALAM PERPEKTIF HUKUM PIDANA POSITIF." *Jurnal Pembaharuan Hukum*, no. 3 (2014).

"UU 1/2024: Perubahan Kedua UU No. 11 Tahun 2008 tentang ITE." Accessed August 26, 2024. https://jdih.maritim.go.id/uu-12024-perubahan-kedua-uu-no-11-tahun-2008-tentang-ite.

Vanessa, Danne Dean. "Proses Penyelidikan Kejahatan Carding Lintas Negara - Hukum / Diskusi Hukum." Dictio Community, April 24, 2018. https://www.dictio.id/t/proses-penyelidikan-kejahatan-carding-lintas-negara/51562.

Wahid, Abdul, and Labib Mohammad. *Kejahatan mayantara (cyber crime)*. Bandung: Refika Aditama, 2005.

Wahid, Fathul. "Kamus Istilah Teknologi Informasi." *Yogyakarta: Andi*, 2002. https://scholar.google.com/scholar?cluster=17635279872035410263&hl=en&oi=scholarr.

Biografi Penulis

Yogi Wirandicha

Mahasiswa Ilmu Hukum, Fakultas Hukum Universitas Riau.

Dr. Zulfikar Jayakusuma, SH., MH
Dosen Hukum, Fakultas Hukum, Universitas Riau.

Ledy Diana, SH., MH
Dosen Hukum, Fakultas Hukum, Universitas Riau.