BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi digital telah mendorong terjadinya penggabungan antara bidang Teknologi Informasi, Media, dan Telekomunikasi. Sebelumnya, ketiga bidang tersebut berkembang secara terpisah dan dalam urutan yang linear. Kini terjadi penyatuan yang menghasilkan integrasi sistem. Bentuk nyata dari konvergensi ini terlihat dari munculnya berbagai produk teknologi baru yang menggabungkan fungsi sistem informasi dengan sistem komunikasi yang berbasis komputer. Produk-produk tersebut kemudian saling terhubung dalam suatu jaringan yang dikenal sebagai *sistem elektronik*, dengan cakupan mulai dari lokal, regional, hingga global. Kehadiran *sistem elektronik* inilah yang melahirkan ruang baru yang populer disebut *cyberspace*. [1]

Cyberspace menghadirkan pola komunikasi dan koordinasi yang berbeda secara signifikan dibandingkan interaksi di dunia nyata. Di dalam *cyberspace*, seseorang bisa berhubungan dengan orang lain tanpa perlu bertemu langsung secara fisik. Lebih jauh, individu juga dapat berinteraksi dengan pihak baru, berdiskusi, bahkan dalam kondisi tertentu merencanakan tindak kejahatan.[2]

---

[1] Unzur Jefri Tambunan, Puguh Aji Hari Setiawan, dan Dewi Iryani, 2024, *"Penegakan Hukum Tindak Pidana Carding Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Pembangunan Hukum Tindak Pidana Siber (Cybernetics)"*, GAGASAN HUKUM Vol. 6 No.02, 2024, hlm. 142.

[2] Astar Hadi, 2005,*"Matinya dunia cyberspace",*LKiS Pelangi Aksara,Yogyakarta, hlm. 41.

Cyber crime Adalah bentuk kejahatan modern yang muncul yang seiring dengan berkembangnya teknologi. Kejahatan ini terus berkembang mengikuti transformasi zaman dan pemanfaatan teknologi digital. Istilah *cyber crime* digunakan untuk menggambarkan tindak pidana yang terkait dengan *cyberspace* serta pemanfaatan komputer sebagai alat utama. Kemajuan pesat dalam *cyberspace* telah membuka peluang bagi sejumlah oknum-oknum yang tidak bertanggung jawab, yang kemudian dikenal sebagai *cyber crime.*[3]

Dalam tinjauan hukum, tindak pidana siber (*cyber crime*) dapat dipahami melalui dua sudut pandang. Pertama, dalam lingkup sempit, tindak pidana siber mencakup tindakan yang secara langsung ditujukan untuk mengganggu atau merusak aspek integritas, ketersediaan, maupun kerahasiaan suatu data dan sistem elektronik. Kedua, dalam pengertian yang lebih luas, tindak pidana siber tidak hanya terbatas pada serangan terhadap sistem, melainkan juga meliputi setiap jenis kejahatan yang menggunakan sarana komputer, jaringan, atau infrastruktur digital lainnya sebagai media pelaksanaannya perangkat elektronik, termasuk tindak pidana konvensional yang modusnya dialihkan melalui teknologi digital.

Salah satu contoh nyata dari *cyber crime* adalah praktik *carding*. Jenis kejahatan ini menggunakan internet sebagai sarana utama untuk melakukan akses tanpa izin terhadap sistem, misalnya pada situs tertentu, dengan tujuan memperoleh informasi pemegang kartu kredit Informasi tersebut selanjutnya digunakan untuk

[3] *Ibid*, hlm.42.

melakukan pembelanjaan secara tidak sah atau menarik dana yang seharusnya hanya bisa diakses oleh pemilik kartu kredit yang resmi.[4]

Modus dalam kejahatan *carding* semakin kompleks sehingga menimbulkan keresahan di tengah pesatnya perkembangan transaksi digital. Praktik ini dapat menyebabkan nasabah mengalami kerugian finansial, bahkan tanpa melakukan aktivitas transaksi sama sekali. Pada umumnya, kejahatan *carding* dilakukan dengan memanfaatkan data pribadi pemilik kartu debit maupun kartu kredit secara tidak sah, lalu menggunakan informasi tersebut untuk berbelanja di platform *e-commerce* atau melakukan pembayaran melalui aplikasi layanan digital.[5]

Kasus *carding* yang pernah terjadi di Indonesia salah satunya pada bulan Juli tahun 2010, Direktorat Reserse Kriminal Khusus menangkap seorang pegawai kafe Starbucks di Tebet, Jakarta Selatan, yaitu DDB, yang berusia 26 tahun dan terbukti terlibat dalam pencurian data kartu kredit pelanggan. Dia mengumpulkan informasi kartu kredit dari konsumen yang berkunjung ke tempat kerjanya dengan cara mencetak ulang struk dan mencatat kode verifikasinya. Dengan metode ini, dia berhasil mengakses ratusan informasi kartu kredit. Data kartu kredit yang berhasil dikumpulkan kemudian digunakan untuk melakukan pembelian perangkat elektronik Ipod Nano dan Ipod Touch secara daring di Apple Online Store Singapura, dengan total transaksi lebih dari 50 kali. Produk yang dibeli oleh pelaku kemudian dikirim dan dijual kembali kepada orang lain. Kasus ini terjadi antara

---

[4] Novryan Alvin Kurniawan, 2014. *"Pencegahan Kejahatan carding Sebagai Kejahatan Transnasional Menurut Hukum Internasional"*, Jurnal, Fakultas Hukum Universitas Brawijaya, Malang, hlm. 6.

[5] Willa Wahyuni, "Modus Cyber *Carding* dan Cara Mengantisipasinya", https://www.hukumonline.com/berita/a/modus-cyber-*carding*-dan-cara-mengantisipasinya lt64e6b81cc36f1/, dikunjungi pada tanggal 5 Maret 2025 Jam 05.40.

bulan Maret hingga Juni 2010, dan terungkap setelah lebih dari 41 nasabah melaporkan adanya transaksi tidak sah pada kartu kredit mereka. Sekitar bulan April, sebuah bank swasta sudah mengajukan keluhan dari nasabah kepada penyelidik untuk dilakukan penyelidikan lebih lanjut. Tersangka dikenakan Pasal 362 KUHP mengenai penipuan dan atau Pasal 378 KUHP tentang pencurian, serta Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik, dengan ancaman hukuman penjara lebih dari lima tahun.[6]

Kasus selanjutnya terjadi di tahun 2023 lalu, Polda Bali berhasil mengungkap kasus *carding* yang melibatkan seorang pria berinisial MA (41 tahun) asal Jakarta Selatan. MA ditangkap setelah terbukti mencuri data dari 1.293 kartu kredit milik orang lain, yang berasal dari berbagai bank, baik dalam maupun luar negeri, dan data tersebut digunakan untuk melakukan transaksi ilegal. Kejahatan ini dilakukan dengan modus operandi memanfaatkan data kartu kredit yang dibeli dari *dark web*, yang kemudian digunakan untuk membeli berbagai layanan daring, seperti pemesanan hotel dan tiket pesawat.

Dalam menjalankan aksinya, MA memperoleh data kartu kredit dari situs *dark web* dengan harga sekitar 20 USD per data, yang dibayarkan menggunakan mata uang kripto untuk menghindari pelacakan. Setelah mendapatkan data kartu kredit, MA menggunakannya untuk memesan voucher hotel dan tiket pesawat melalui platform pemesanan seperti *Airbnb* dan *Booking.com*. Produk yang dibeli secara ilegal ini kemudian dijual kembali dengan harga diskon 30-50% kepada

[6] Vennie Melyani, "Karyawan Starbucks Tebet Bajak Ratusan Kartu Kredit", www.tempo.co/hukum/karyawan-starbucks-tebet-bajak-ratusan-kartu-kredit- dikunjungi pada 27 Agustus 2025, Jam 01.49.

pelanggan yang tertarik melalui akun Instagram milik pacarnya, RN. RN berperan dalam membantu memasarkan tiket dan *voucher* hotel tersebut tanpa mengetahui secara pasti asal-usulnya. Hingga akhirnya Tim Siber Polda Bali baru dapat mengungkap kasus ini dengan menemukan akun Instagram yang menawarkan diskon hotel dan vila dengan harga mencurigakan. Setelah dilakukan penyelidikan lebih lanjut, MA dan RN ditemukan di Mall Bali Galeria, Kuta, Badung, dan segera diamankan oleh pihak kepolisian. Saat diperiksa, RN mengaku bahwa ia hanya membantu mempromosikan penawaran tersebut atas permintaan MA dan tidak menyadari bahwa transaksi yang dilakukan berasal dari kejahatan siber.[7]

Terdakwa dihadapkan pada tuntutan melanggar Pasal 32 ayat (1) yang berhubungan dengan pengiriman, perubahan, penambahan, dan tindakan lainnya yang berhubungan dengan informasi elektronik tanpa persetujuan, sesuai ketentuan dalam Undang-undang Nomor 19 Tahun 2016 yang mengubah Undang-undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik. Hukuman yang dapat dijatuhkan kepada terdakwa bisa mencapai penjara selama 8 tahun dan denda maksimum sebesar Rp 2 miliar. Pasal 32 ayat (1) dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan bahwa setiap orang diharuskan mendapatkan izin terlebih dahulu sebelum melakukan tindakan tertentu terhadap informasi elektronik milik orang lain. Dalam hal ini, MA dituduh melakukan carding dengan cara menggunakan kartu kredit tanpa izin dari pemiliknya. Selanjutnya, Pasal 48 ayat (1) dari Undang-Undang yang

[7] Rolandus Nampu,"Polda Bali Tangkap Pelaku Kejahatan Pencurian 1.293 Data Kartu Kredit", https://www.antaranews.com/berita/3656613/polda-bali-tangkap-pelaku-kejahatan-pencurian-1293-data-kartu-kredit, dikunjungi pada 5 Maret 2025, Jam 09.10.

sama menentukan hukuman maksimal bagi pelanggaran yang dijelaskan dalam Pasal 32 ayat (1), yaitu hukuman penjara paling lama 8 tahun dan denda maksimum sebesar Rp 2 miliar.[8]

Oleh karena itu, hukum pidana bersifat tidak berlaku surut atau non-retroaktif, serta menjamin kepastian hukum dan perlindungan hak asasi manusia, sehingga tidak ada orang yang dapat dihukum berdasarkan aturan hukum yang belum ada pada saat tindakan tersebut dilakukan.[9]

Menurut Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP) yang menyatakan tidak ada suatu perbuatan yang dapat dipidana kecuali sudah ditentukan dalam undang-undang *(nullum delictum nulla poena sine praevia lege poenali*), maka diatur macam-macam keabsahan hukum yang terdapat dalam. Pemikiran ini menekankan bahwa suatu perbuatan baru dapat digolongkan sebagai kejahatan apabila telah ditetapkan secara jelas dalam peraturan perundang-undangan sebelum perbuatan itu dilakukan. *Carding* dalam konteks ini dapat dipandang sebagai tindak pidana pencurian karena pelaku secara melawan hukum menggunakan atau memperoleh keuntungan dari nomor kartu kredit orang lain, meskipun bukan merupakan pencurian fisik atas harta benda atau aset. Sebaliknya, apabila cara yang dilakukan dalam *carding* telah memenuhi unsur-unsur tindak pidana lain yang diatur dalam KUHP, maka pasal-pasal tersebut dapat pula dikenakan kepada pelaku *(carder)*.[10]

---

[8] Dhevanda Ashar Evrast Avrizal dan Okti Indah Lesta, 2024, *"Mengungkap Jejak Digital : Elektronik Kasus Carding di Bali Pada Tahun 2023"* , Jurnal Kritis Hukum, hlm. 50.

[9] Muh. Yasrul Hajar, 2012, *"Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Carding"*, Skripsi Sarjana Hukum, Universitas Muhammadiyah Surakarta, Surakarta, hlm. 3.

[10] *Ibid.*

Selain di dalam pengaturan yang terdapat dalam KUHP, *carding* juga diatur dalam Undang-Undang Nomor 1 Tahun 2024 yang merupakan Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (UU ITE), di mana terdapat ketentuan dalam Pasal 30 yang mengatur tindakan ilegal sebagai berikut :

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Dan di dalam Pasal 32 ayat (2) mengatur tentang mengambil informasi atau data elektronik :

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

Selanjutnya dalam Pasal 35 mengatur Tindakan manipulasi :

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Lebih lanjut diatur Pasal 36 merupakan penekanan jika berdampak kerugian bagi orang lain :

> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal27 sampai dengan Pasal34 yang mengakibatkan kerugian bagi Orang lain.

Dan pada Pasal 37 jika tindak pidana dilakukan diluar wilayah indonesia :

> Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

Dalam ketentuan hukum pidana materiil di Indonesia belum ada Pasalkhusus yang secara jelas menyebutkan tentang tindakan peretasan kartu kredit atau *carding* beserta dampak kerugian finansial. Namun, karena sifatnya yang multi-aspek, mencakup aspek akses ilegal terhadap sistem elektronik, pencurian atau pengambilalihan data, pemalsuan informasi, serta penyalahgunaan data untuk keuntungan pribadi. Sehingga harus menjerat pelaku dengan beberapa Pasaldalam KUHP dan UU ITE, tergantung pada modus operandi yang digunakan. [11]

Sebagai contoh Pasal 30 ayat (2) UU ITE menyatakan, "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik". Ketentuan ini sering dikaitkan dengan *carding* karena unsur perbuatannya mencakup pembobolan sistem perusahaan perbankan untuk mengakses, mendistribusikan, memanipulasi, atau menyalin data rekening nasabah. Namun, Pasal ini tidak secara eksplisit mengatur pencurian data kartu kredit maupun dampak finansial yang timbul. Oleh karena itu, agar lebih komprehensif, penerapan Pasal 36 UU ITE diperlukan jika tindakan tersebut

[11] Herman, Handrawan, *Et.Al.* 2023, *"Kejahatan Carding Sebagai Bentuk Cyber crime dalam Hukum Pidana Indonesia",* Halu Oleo Legal Research Volume 5, Issue 2, 2023, hlm. 638.

menyebabkan kerugian bagi korban, sehingga hukuman yang diberikan lebih sesuai dengan dampak kejahatan yang terjadi.

Ketentuan dalam Pasal penjeratan pelaku *carding* cenderung memiliki cakupan luas dan mengatur perbuatan yang lebih umum, seperti akses ilegal terhadap sistem elektronik, pengambilan atau pemalsuan data, serta penyalahgunaan informasi elektronik. .[12] Hal ini menunjukkan bahwa regulasi yang ada masih bersifat umum dan belum secara spesifik mengakomodasi tindak *carding* sebagai kejahatan yang berdiri sendiri. Akibatnya, penerapan hukum dalam kasus ini bergantung pada interpretasi terhadap unsur-unsur dalam Pasal yang ada, sehingga memungkinkan menimbulkan perbedaan dalam penegakan hukum.[13]

Seiring dengan kemajuan ilmu pengetahuan dan teknologi yang kadang disalahgunakan untuk melakukan tindak kriminal, muncul fenomena *cyber crime* yang menuntut adanya respons hukum. Penanganan terhadap kejahatan siber ini dapat dilakukan melalui instrumen hukum pidana, termasuk dalam hal penerapan sistem pembuktian. Hal ini menjadi penting mengingat kejahatan siber sering kali memiliki karakteristik berbeda dengan tindak pidana konvensional, khususnya dalam hal alat bukti, mekanisme perolehan bukti digital, serta validitas bukti tersebut di hadapan hukum.[14] Penegakan hukum pidana pada dasarnya bertujuan untuk menentukan apakah seseorang dapat dianggap bersalah atas suatu tindak

[12] *Ibid.*

[13] Ni Ketut S. A Pratiwi, Rudepel P. Leo, Simplexius Asa, 2024, "Modus OperandI, Upaya Penanggulangan serta Hambatan Tindak Pidana *Carding* di Wilayah Hukum Kepolisian Daerah Nusa Tenggara Timur", Jurnal Inovasi dan Humaniora Volume 2, No. 3, 2024, hlm. 284.

[14] Erwin Taroreh, *Et.al,* 2024 *"Tinjauan Yuridis Terhadap PelakuPeretasan Kartu Kredit (Carding) Menurut Undang-UndangNomor 19 Tahun 2016 Tentang Perubahan Atas Undang-UndangNomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik",* Jurnal Uners Law Review, 2024, hlm. 8882.

pidana atau tidak. Selain mempertimbangkan asas *legalitas*—yakni bahwa suatu perbuatan hanya dapat dipidana jika telah diatur dalam perundang-undangan sebelumnya—penilaian tersebut juga harus didasarkan pada adanya bukti yang sah serta kemampuan pelaku untuk mempertanggungjawabkan perbuatannya, yang mencerminkan unsur kesalahan (*mens rea*). Dengan demikian, tidak hanya tindakan itu sendiri yang menjadi fokus, tetapi juga niat, kesadaran, dan tanggung jawab hukum pelaku dalam melakukan perbuatan pidana tersebut.[15]

Upaya penanggulangan yang dilakukan Indonesia terhadap kejahatan *carding* melibatkan berbagai lembaga dan pendekatan. Otoritas Jasa Keuangan (OJK), Kepolisian Negara Republik Indonesia (Polri), dan sektor perbankan berperan aktif dalam pencegahan dan penindakan dari tindak pidana *carding*.[16]

Regulasi hukum mengenai kompensasi atau penggantian kerugian bagi nasabah yang menjadi korban praktik *carding* diatur dalam Peraturan Otoritas Jasa Keuangan (OJK) Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Jasa Keuangan. Peraturan ini mencakup beberapa prinsip perlindungan konsumen, yaitu transparansi, perlakuan yang adil, keandalan, kerahasiaan dan keamanan data/informasi konsumen, serta penanganan pengaduan dan penyelesaian sengketa secara sederhana, cepat, dan terjangkau.[17]

---

[15] Vivi Arfiani Siregar dan R. Dimas Ariwibowo, 2021 *"Fenomena Kejahatan Carding Berdasarkan dalam Hukum Pidana Indonesai Indonesia"*, Jurnal Das Sollen, Volume 6, No. 2 , 2021, hlm. 101.

[16] Galang Ramadhan Djokdja, Sherly Adam & Margie Gladies Sopacua, 2022, *"Pertanggungjawaban Pidana Pelaku Pembobolan Kartu Kredit Dalam Tindak Pidana Di Bidang Perbankan"*, TATOHI Jurnal Ilmu Hukum Vol 2, No 2, 2022, hlm. 181.

[17] Nugroho Wisnu Pujoyono, 2020, "Penal Policy dalam Upaya Preventif Kejahatan *Carding* Di Indonesia", Jurnal Ilmiah Nasional Mahasiswa Hukum Volume 3, Nomor 1, 2020, hlm. 90.

Prinsip perlindungan yang berhubungan dengan privasi dan keamanan informasi pelanggan sangat krusial. Kebocoran data pelanggan yang mengakibatkan kerugian dapat terjadi karena lemahnya sistem perlindungan bank atau kelalaian dalam manajemen perbankan. Maka dari itu, bank harus melindungi kerahasiaan dan memperkuat sistem keamanannya untuk menghindari kejahatan perbankan yang merugikan pelanggan. Di samping itu, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan juga menetapkan kewajiban bank untuk memberikan informasi terkait risiko transaksi kepada nasabah sesuai dengan Pasal 29 ayat (4). Hak pelanggan untuk mendapatkan informasi ini memungkinkan mereka mempersiapkan diri terhadap kemungkinan risiko serta mencegah kelalaian yang bisa menjadikan mereka target kejahatan perbankan.[18]

Berdasarkan prinsip privasi dan keselamatan data/informasi konsumen (pasal 2 huruf d) pada peraturan OJK, ada kewajiban bagi bank untuk memperhatikan kepentingan nasabah, yang juga ditunjang oleh prinsip privasi. Prinsip ini mengharuskan bank untuk menjaga kerahasiaan semua hal yang berkaitan dengan data dan informasi nasabah, baik yang berhubungan dengan kondisi keuangannya maupun informasi pribadi. Menjaga kerahasiaan kondisi keuangan nasabah adalah aspek yang sangat krusial dalam menjalankan operasi di sektor perbankan.[19]

Dalam aspek penegakan hukum, tindak pidana *carding* diproses melalui mekanisme hukum yang berlaku, dengan kepolisian berkoordinasi dengan instansi

[18] Zulkarnain dan Tata Sutabri, 2023, *"Analisis Kejahatan Carding Pada BNI 46",* Blantika : Multidisciplinary Jornal Volume 2 Number 1, 2023.hlm.161.

[19] Ruth Hernita, 2018, *"Pertanggungjawaban secara Pidana Oleh Bank Terhadap Tindak Pidana Carding",* Fakultas Hukum, Universitas Jember.

terkait untuk mengungkap kasus berdasarkan hasil penyelidikan dan penyidikan. Selanjutnya, koordinasi dengan kejaksaan dilakukan untuk menuntut pelaku sesuai dengan Pasal yang didakwakan hingga proses pemberian sanksi bagi pelaku yang terbukti bersalah.[20]

Kasus *carding* di Indonesia pada kurun waktu tiga tahun yakni 2019-2021 terjadi sebanyak 11 kasus yang telah sampai pada putusan pengadilan.[21] Dengan fakta bahwa Indonesia memiliki jumlah pengguna internet yang terus meningkat dibuktikan sejak tahun 2018, tingkat penetrasi internet di Indonesia tercatat sebesar 64,8%. Angka ini meningkat menjadi 73,7% pada 2020, 77,01% pada 2022, dan mencapai 78,19% pada 2023.[22]

Kejahatan siber seperti *carding* dengan melakukan pencurian informasi kartu kredit untuk transaksi ilegal menjadi ancaman serius bagi keamanan finansial global. Singapura, misalnya, mengalami peningkatan signifikan dalam kasus kejahatan siber. Pada tahun 2024, total kasus penipuan meningkat 10,6% menjadi 51.501 kasus, dengan kerugian mencapai S$1,1 miliar, naik 70,6% dibandingkan tahun sebelumnya.[23] Untuk menanggulangi kejahatan penipuan berbasis siber, pemerintah Singapura telah membentuk Pada Maret 2022, *Anti-Scam Command* berhasil membekukan lebih dari 9.000 rekening bank dan pada semester pertama

[20] Bambang Hartono, 2013, *Op.cit*., hlm .182.

[21] I Gede Krisna Ginara, 2022, *"Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber crime dalam Hukum Pidana Indonesia"*, Jurnal No. 1, Vol. 3, 2022, hlm. 141.

[22] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), "*Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang"*, https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang dikunjungi pada 7 Maret 2025 Jam 08.30.

[23] PTI, *"World Singapore Loses $1.1 Billion To Scams In 2024: Police Report Singapore Loses $1.1 Billion To Scams In 2024: Police Report"*, https://www.ndtvprofit.com/world/singapore-loses-s11-billion-to-scams-in-2024-per-police-report?utm_ dikunjungi pada 13 Mei 2025 Jam 16.58.

2023 berhasil memulihkan sekitar SGD 50,8 juta yang diperoleh dari tindak penipuan..[24]

Di Singapura, peraturan mengenai pencurian dan penyalahgunaan informasi kartu kredit secara illegal yang dikategorikan sebagai *fraud-related offence*, yang diatur dalam *Computer Misuse Act 1993* (CMA) dan *Singapore Penal Code* 1871. Peraturan perundang-undang tersebut memuat larangan akses ilegal ke sistem komputer dan modifikasi data tanpa izin dan juga dapat menjerat pelaku melalui ketentuan pidana tentang penipuan dan penyalahgunaan data keuangan. Tindakan yang dilakukan dengan maksud untuk melakukan kejahatan lain, seperti penipuan atau pencurian, dapat dijerat dengan *Section* 4 CMA, yang berbunyi :

> *"Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence."*

Ketentuan ini berlaku apabila akses ilegal dilakukan dengan niat untuk melakukan kejahatan lain, seperti penipuan data finansial, yang merupakan modus umum dalam tindak *carding*. Sanksi yang dapat dikenakan terhadap pelanggaran tersebut yaitu pidana penjara hingga 10 tahun dan/atau denda hingga 50.000 dolar Singapura.

Selain dari pada itu juga terdapat dalam Pasal 416A ayat (1) *Singapore Penal Code* bahwa Siapa pun yang memperoleh, memiliki, atau menyediakan

---

[24] Muhammad Darisman, *"Kasus penipuan di Singapura terus naik, kerugian tembus Rp,37T",https://kumparan.com/kumparanbisnis/kasus-penipuan-di-singapura-terus-naikkerugian-tembus-//* dikunjungi pada 7 Maret Jam 10.00.

informasi pribadi orang lain tanpa izin dengan maksud untuk melakukan tindak pidana dapat dijerat sanksi pidana dengan denda hingga SGD 10.000 atau penjara maksimal 3 tahun, atau keduanya.[25]

> *"(1) A person (A) shall be guilty of an offence who, knowing or having reason to believe that any personal information about another person (B) (being an individual) was obtained without B's consent — (a) obtains or retains the personal information; or (b) supplies, offers to supply, transmits or makes available, by any means, the personal information."*

Singapura mengatur *carding* secara eksplisit melalui CMA dan *Singapore Penal Code* 1871, yang secara jelas mencakup akses ilegal ke sistem komputer dengan tujuan pencurian atau penyalahgunaan data elektronik. Sementara itu, di Indonesia, dalam UU ITE, tidak terdapat Pasal yang secara langsung menyebutkan pencurian data kartu kredit. Penegakan hukumnya bergantung pada interpretasi pasal-pasal yang bersifat lebih umum, seperti akses ilegal, pencurian dan pemindahan data, serta pemalsuan data elektronik.

Peraturan mengenai tindak pidana *carding* dan pencegahan kejahatannya berbeda-beda di setiap negara, tergantung pada sistem hukum yang dianut. Menurut Sudikno Mertokusumo, sistem hukum adalah suatu kesatuan yang terdiri dari unsur-unsur yang saling berinteraksi untuk mencapai tujuan bersama.[26] Berlakunya sistem hukum dalam suatu negara dipengaruhi oleh sub sistem yang terdiri atas substansi

[25] Gregor Urbas, 2008, "*An Overview ofcyber crime Legislation and Cases in Singapore",* Working Paper Series No. 001, hlm. 14.

[26] Misbahul Huda, 2020, *Perbandingan Sistem Hukum,* CV Cendekia Press, Bandung, hlm. 9

hukum, struktur hukum, dan budaya hukum.[27] Berbagai sistem hukum, baik *civil law, common law,* maupun sistem hukum campuran, memiliki pendekatan berbeda dalam menangani ancaman digital, termasuk *carding.* Oleh karena itu, memahami perbandingan hukum di berbagai yurisdiksi menjadi penting untuk mengidentifikasi praktik terbaik dalam regulasi dan penegakan hukum terhadap kejahatan siber.

Perbandingan hukum berperan dalam memahami serta menganalisis regulasi terkait perlindungan data pribadi, khususnya dalam menangani kejahatan siber seperti *carding*. Permasalahan *carding* tidak hanya berdampak pada satu negara tetapi juga dapat mempengaruhi hubungan antarnegara karena luasnya dari dampak kejahatan transnasional. Oleh karena itu, harmonisasi regulasi perlindungan data pribadi di kawasan Asean menjadi krusial untuk memastikan keamanan privasi secara regional. Perbedaan kebijakan di masing-masing negara dapat menimbulkan tantangan dalam penegakan hukum, terutama dalam menghadapi kejahatan siber lintas batas yang membutuhkan kerja sama internasional.

Indonesia mengesahkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 sebagai langkah untuk menyesuaikan diri dengan perkembangan teknologi dan tantangan kejahatan siber. Sementara itu, Singapura telah lebih dulu memiliki *Computer Misuse Act* (CMA) 1993, yang menjadi landasan dalam menangani kejahatan siber sejak awal. Perbedaan waktu dalam pengesahan regulasi ini mencerminkan dinamika hukum yang berbeda di masing-masing negara. Serta untuk mengambil pembelajaran dari pengalaman

[27] *Ibid*, hlm. 1

negara lain dalam upaya memperkuat kerangka hukum nasional guna membangun ekosistem digital yang aman, terstruktur, dan berkeadilan.

Beranjak dari latar belakang masalah yang telah diungkapkan di atas, penulis sangat tertarik untuk mengangkat isu ini ke dalam suatu karya tulis ilmiah yang berjudul **"Pengaturan Terhadap Tindak Pidana Pencurian Data Kartu Kredit *(Carding)* (Perbandingan Pengaturan : Studi di Indonesia dan Singapura)".**

Dalam penelitian ini, penulis memilih negara Singapura sebagai bahan perbandingan karena Singapura merupakan salah satu negara yang dikategorikan sebagai negara dengan keamanan siber yang baik di Asia Tenggara. Dalam *Global Cybersecurity Index* (GCI) 2020, Singapura mendapatkan skor 98,52 pada peringkat global dalam hal keamanan siber.[28] Sedangkan Indonesia mendapatkan skor 94,88. Singapura juga memiliki *Cyber Security Agency* (CSA) sebagai badan pemerintah yang didedikasikan untuk mengawasi dan mengembangkan strategi nasional dalam keamanan siber.

Berdasarkan *National Cyber Security Index* (NCSI) 2021, Singapura juga mendapatkan skor tertinggi dalam beberapa indikator, yaitu pendidikan dan pengembangan profesional, perlindungan layanan esensial, analisis ancaman siber, manajemen krisis siber, dan perlindungan data pribadi.[29]

[28] International Telecommunication Union, Global Cybersecurity Index (GCI) 2020.

[29] Lucas Romero, 2023, "National Cyber Security Index of Singapore 2021", https://www.statista.com , dikunjungi pada 7 Maret 2025 Jam 15.45.

B. Rumusan Masalah

Berdasarkan latar belakang telah penulis paparkan diatas, dalam rangka mengkaji mengenai Pengaturan Terhadap Tindak Pidana Pencurian Data Kartu Kredit *(Carding)* (Perbandingan Pengaturan : Studi di Indonesia dan Singapura), maka dapat dirumuskan masalah dalam penelitian yang melimitasi skripsi ini, yakni:

1. Bagaimana Perbandingan Pengaturan terhadap Tindak Pidana Pencurian Data Kartu Kredit (*Carding)* di Indonesia dan Singapura?
2. Apa Kelebihan dan Kekurangan terhadap Pengaturan Tindak Pidana Pencurian Data Kartu Kredit (*Carding)* di Indonesia dan Singapura?

C. Tujuan Penelitian

Berkaitan dengan identifikasi rumusan masalah diatas, maka tujuan yang ingin dicapai dalam skripsi ini diantaranya:

1. Mengetahui dan menganalisis mengenai penerapan hukum pidana untuk kejahatan pencurian informasi kartu kredit *(carding)* sesuai dengan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 1 Tahun 2024 yang merupakan amandemen kedua dari Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (UU ITE), serta peraturan yang berlaku di Singapura, seperti Singapore *Penal Code* 1871 dan *Computer Misuse Act* (CMA) 1993.
2. Memahami serta menganalisis kelebihan dan kekurangan dalam ketentuan hukum mengenai tindak pidana pencurian data kartu kredit

(carding) di Indonesia dan Singapura.

D. Manfaat Penelitian

Berdasarkan tujuan yang telah ditetapkan sebelumnya, diharapkan penelitian ini dapat memberikan manfaat sebagai berikut :

1. Manfaat Teoritis

Hasil penelitian ini diharapkan dapat memberikan tambahan pengetahuan, baik dalam bentuk pengembangan teori maupun analisis yang dilakukan, serta berfungsi sebagai bahan acuan yang berguna bagi penelitian lebih lanjut mengenai perbandingan ketentuan hukum pidana terkait tindak pidana *carding* di Indonesia dan Singapura.

2. Manfaat Praktis

a. Bagi Peneliti, hasil penelitian ini dapat menambah pengetahuan dan memperluas wawasan peneliti serta menambah ilmu pengetahuan mengenai Pengaturan Terhadap Tindak Pidana Pencurian Data Kartu Kredit *(Carding)* (Perbandingan Pengaturan : Studi di Indonesia dan Singapura).

b. Bagi Pemerintah Indonesia, penelitian ini memberikan kontribusi berupa tambahan wawasan bahwa penanganan tindak pidana *carding* memerlukan pemahaman yang lebih komprehensif, baik dari segi aspek teknis maupun ketentuan hukum yang berlaku.

c. Bagi Universitas Andalas, penelitian ini dapat berfungsi sebagai tambahan referensi dan bahan bacaan bagi Mahasiswa/i Fakultas Hukum, khususnya pada program studi Hukum Pidana, terkait pengaturan tindak pidana pencurian data kartu

kredit (*carding*), dengan fokus pada perbandingan pengaturan antara Indonesia dan Singapura.

E. Metode Penelitian

1. Pendekatan Masalah

Pendekatan penelitian mengacu pada metode atau cara melakukan penelitian.[30] Penelitian ini mengaplikasikan berbagai metodologi, yaitu metodologi normatif, metodologi komparatif, dan metodologi konseptual. Metodologi normatif memiliki tujuan untuk menganalisis teori hukum dan bagaimana hukum tersebut diterapkan dalam kenyataan di masyarakat. Seringkali, peraturan yang ada sudah ideal, tetapi dalam praktiknya, terjadi pelanggaran yang menyebabkan tujuan hukum tidak selalu tercapai. [31] Penelitian ini menggunakan tiga pendekatan utama yakni pendekatan yang didasarkan pada peraturan perundang-undangan (*statute approach*), pendekatan komparatif (*comparative approach*) yang melibatkan perbandingan hukum dan pendekatan konseptual (*conceptual approach*) yang berfokus pada kerangka teoritis. Berikut ini menjelaskan masing-masing pendekatan tersebut secara rinci :

a. Pendekatan Perundang-Undangan

Pendekatan perundang-undangan adalah cara yang mengkaji norma hukum yang berikaitan dengan inti penelitian. Pendekatan ini memanfaatkan undang-undang dan peraturan yang ada. [32]

---

[30] Suharsimi Arikunto, 2002, *Prosedur Penelitian: Suatu Pendekatan Praktek*, Jakarta, Rineka Cipta, hlm. 23.

[31] Soerjono Soekanto, 2014, *"Pengantar Penelitian Hukum"*, Jakarta:, Universitas Indonesia Press, hlm. 21.

[32] Johnny Ibrahim, 2006*, Teori dan Metodelogi Penelitian Hukum Normatif*, Bayumedia Publishing, Surabaya, hlm 295

b. Pendekatan Komparatif

Dalam penelitian ini, penulis menggunakan menerapkan pendekatan perbandingan atau penelitian hukum komparatif. Metode ini dilakukan dengan menganalisis regulasi suatu negara dan membandingkannya dengan aturan dari satu atau lebih negara lain yang mengatur hal yang sama.[33] Selain itu, pendekatan ini juga memberikan kesempatan untuk membandingkan keputusan hakim di berbagai negara yang menangani perkara serupa, sehingga kita bisa mendapatkan wawasan yang lebih mendalam mengenai penerapan hukum di setiap wilayah hukum.[34]

Dalam studi ini, fokus perbandingan difokuskan pada elemen-elemen dari sistem hukum sebagai dasar analisis, yang meliputi: (1) struktur hukum, mencakup lembaga-lembaga yang ada; (2) substansi hukum, yang berisi aturan-aturan serta perilaku yang diatur; dan (3) budaya hukum, yaitu prinsip-prinsip yang dianut dalam sistem hukum tersebut.

Ketiga elemen ini bisa dianalisis baik secara terpisah maupun sekaligus, untuk mencari persamaan maupun perbedaan di antara sistem hukum yang sedang dibandingkan. Dalam penelitian ini, penulis membandingkan substansi hukum tentang carding yang diatur oleh Hukum Pidana Indonesia dengan Hukum Pidana Singapura, yang pada dasarnya bertujuan untuk memahami perbandingan substansi hukum terkait carding dalam kerangka hukum pidana di Indonesia dan Singapura.

[33] Peter Mahmud,2011, *Penelitian Hukum*, Kencana, Surabaya hlm 97.
[34] Zainuddin Ali, Metode Penelitian Hukum, Jakarta:Sinar Grafika, hlm.78

c. Pendekatan Konseptual

Pendekatan konseptual adalah metode dalam penelitian hukum yang fokus pada analisis penyelesaian masalah dengan mempelajari konsep-konsep hukum yang menjadi landasan suatu peraturan. Metode ini juga bisa digunakan untuk memahami nilai-nilai yang terkandung dalam peraturan hukum yang berkaitan dengan penerapan konsep-konsep tersebut.[35] Pendekatan ini umumnya dipakai untuk menelaah gagasan-gagasan yang berkaitan dengan penetapan norma dalam suatu undang-undang, sekaligus mengevaluasi apakah penerapannya sejalan dengan prinsip-prinsip yang terkandung dalam konsep hukum yang mendasarinya.[36]

2. Jenis dan Sumber Bahan Hukum

a. Jenis Bahan Hukum

1). Bahan hukum utama, yaitu materi atau peraturan hukum yang memiliki kekuatan mengikat dan diatur dalam urutan tertentu. Bahan hukum utama adalah referensi hukum yang memiliki kekuasaan, yang berarti memiliki kewenangan. Sumber hukum utama meliputi undang-undang, dokumen resmi atau catatan dalam proses legislasi, serta keputusan dari hakim.[37] Adapun yang menjadi bahan hukum primer adalah :

a) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

b) Kitab Undang-Undang Hukum Pidana

[35] *Ibid.*
[36] *Ibid.*
[37] Peter Mahmud*, Op.Cit*, hlm 141.

c) Kitab Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.
d) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
e) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
f) Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Tentang Informasi dan Transaksi Elektronik
g) *Singapore Penal Code* 1871
h) *Computer Misuse Act* (CMA) 1993

2). Bahan hukum sekunder terdiri dari semua referensi hukum yang bukan termasuk dokumen resmi atau undang-undang.[35] Bahan hukum sekunder memiliki peranan sebagai tambahan yang menjelaskan dan memperdalam pemahaman mengenai bahan hukum primer, yang umumnya berupa tulisan dari para ahli hukum.

3). Bahan hukum tersier adalah sumber hukum yang memberikan penjelasan tentang bahan hukum primer dan bahan hukum sekunder. Contoh dari bahan tersier termasuk ensiklopedia, kamus, dan indeks kumulatif, serta lainnya.[38]

3. Teknik Pengumpulan Data

Dalam melaksanakan penelitian ini, bahan hukum primer, bahan hukum

[38] Soerjono Soekanto, *Op Cit*, hlm 12.

sekunder, dan bahan hukum tersier diperoleh melalui studi literatur baik secara fisik dengan mengunjungi perpustakaan maupun melalui pencarian daring. Studi literatur dengan cara fisik akan dilaksanakan di Perpustakaan Universitas Andalas, Perpustakaan Fakultas Hukum Universitas Andalas, serta perpustakaan pribadi. Penelitian pustaka secara daring akan dilakukan dengan mengakses situs perpustakaan digital dan website hukum yang berhubungan.

4. Metode Pengolahan Data

Setelah semua data yang diperoleh, yaitu data sekunder yang meliputi bahan hukum primer, bahan hukum sekunder, dan sumber hukum tersier, kemudian dilakukan penyusunan data lewat tahap penyuntingan karena dalam proses pengumpulan data tidak semua informasi yang didapatkan dimasukkan, melainkan hanya yang relevan saja.

5. Metode Analisis Data

Dalam melakukan analisis data dan mendapatkan kesimpulan dari penelitian, bahan hukum yang bersifat primer, sekunder, dan tersier akan diperiksa dengan menggunakan berbagai teknik, yaitu:

a. Metode Deskriptif, yaitu teknik yang digunakan penulis untuk memaparkan apa adanya tentang suatu peristiwa hukum atau kondisi hukum.[39]
b. Metode Komparatif, yaitu teknik yang digunakan untuk membandingkan pendapat-pendapat sarjana hukum yang terdapat di dalam bahan hukum sekunder.[40]

[39] I Made, Pasek Diantha, 2016, *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*, Prenada Media, Jakarta, hlm. 152.
[40] *Ibid.*

c. Metode Evaluasi, yaitu teknik yang digunakan untuk mengevaluasi hasil atau kesimpulan yang didapat dari teknik deskripsi dan teknik komparasi yang sudah dilakukan sebelumnya, untuk menentukan sikap peneliti atas deskripsi dan komparasi yang ada.[41]

d. Metode Argumentatif, yaitu teknik untuk memberikan masukan dan/atau pandangan penulis setelah mendapatkan evaluasi dari teknik deskripsi dan teknik komparasi. Teknik ini digunakan untuk menjawab permasalahan yang diteliti oleh penulis.[42]

[41] *Ibid*. hlm, 153.
[42] *Ibid.* hlm, 154.