



Jurnal Kajian Hukum dan Sosial

Vol .3 No.1 2026

Faculty of Law, Universitas Jenderal Soedirman, E-ISSN: 3124-3460

HR. Boenyamin 708, Purwokerto, Banyumas, Central Java, Indonesia.

✉ jks@unsoed.ac.id jos.unsoed.ac.id/index.php/jkhs/index

AKSES ILEGAL TERHADAP SISTEM PEMBAYARAN ELEKTRONIK: PERSPEKTIF PERTANGGUNGJAWABAN PIDANA DAN KRIMINOLOGI SIBER

Fathia Rahmat^{1*}, Aline Winar Apmilusari², Zakia Rosida³, Hafidz Harstian Pradana⁴, Aldi Farhan Razaki⁵

¹²³⁴⁵Universitas Jenderal Soedirman

*Corresponding Author: ✉ fathia.rahmat@mhs.unsoed.ac.id

Abstrak

Perkembangan teknologi informasi dalam sektor perbankan mendorong transformasi sistem pembayaran elektronik, namun di sisi lain membuka celah baru bagi kejahatan siber berupa akses ilegal (unauthorized access) terhadap sistem elektronik. Penelitian ini bertujuan untuk menganalisis pertanggungjawaban pidana pelaku dan mengeksplorasi model pencegahan terhadap tindak pidana siber berbasis kartu pembayaran melalui studi kasus Putusan Nomor 838/Pid.Sus/2021/PN Dps mengenai perkara illegal Flazz BCA. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan kriminologi siber melalui studi dokumen terhadap putusan pengadilan serta literatur hukum terkait. Hasil penelitian menunjukkan bahwa perbuatan Terdakwa yang melakukan penarikan tunai menggunakan kartu magnetic stripe berisi data perbankan orang lain secara melawan hukum telah memenuhi unsur Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE. Majelis Hakim menjatuhkan pidana penjara serta pidana tambahan berupa perampasan barang bukti untuk negara. Berdasarkan perspektif kriminologi, etiologi kejahatan ini didorong oleh motivasi pelaku untuk memperoleh keuntungan ekonomi dengan memanfaatkan celah teknologi digital, serta dipicu oleh kerentanan sistem kartu magnetic stripe yang mempermudah praktik skimming. Dampak dari kejahatan ini menimbulkan kerugian materiil bagi pihak perbankan yang wajib mengganti dana nasabah, sekaligus kerugian immateriil berupa menurunnya reputasi bank dan kepercayaan publik. Sebagai model pencegahan, efektivitas langkah non-penal sangat bergantung pada penguatan manajemen risiko sistem perbankan, salah satunya melalui kebijakan Bank Indonesia dalam implementasi migrasi total ke teknologi kartu berbasis chip yang memiliki sistem keamanan autentikasi lebih kuat.

Kata Kunci: Akses Ilegal, Magnetic Stripe, Skimming, UU ITE.

Submitted: 29 Mei 2026

Reviewed: 10 Juli 2026

Accepted: 3 Agustus 2026

Sitasi / How to Cite:

Rahmat, Fathia, Aline Winar Apmilusari, Zakia Rosida, Hafidz Harstian Pradana, dan Aldi Farhan Razaki. Akses Ilegal terhadap Sistem Pembayaran Elektronik: Perspektif Pertanggungjawaban Pidana dan Kriminologi Siber. Jurnal Kajian Hukum dan Sosial, 3, no. 1, (2026): [Halaman] [10.20884/1.jkhs.2026.3.1.20858](https://doi.org/10.20884/1.jkhs.2026.3.1.20858)
Use "Modern Humanities Research Association 3rd Edition" filled Editorial

PENDAHULUAN

Perkembangan teknologi informasi dalam sektor perbankan telah mendorong transformasi sistem pembayaran elektronik yang lebih cepat dan efisien, namun pada saat yang sama juga membuka peluang terjadinya kejahatan siber dalam bentuk akses ilegal terhadap sistem elektronik. Fenomena tersebut terlihat dalam Putusan Nomor 838/Pid.Sus/2021/PN Dps, di mana pelaku menggunakan kartu magnetic stripe yang telah berisi data perbankan milik orang lain untuk melakukan transaksi penarikan tunai pada mesin ATM secara melawan hukum. Permasalahan ini mencerminkan isu fundamental berupa kerentanan sistem keamanan transaksi elektronik, terutama pada teknologi kartu

yang masih memungkinkan penyalinan data secara ilegal oleh pihak yang tidak berwenang.¹ Selain itu, modus operandi dalam perkara ini juga mengindikasikan adanya jaringan kejahatan siber yang memanfaatkan teknologi digital untuk memperoleh keuntungan ekonomi secara tidak sah melalui manipulasi sistem pembayaran.² Tindakan tersebut menunjukkan adanya praktik cloning kartu dan penyalahgunaan data elektronik yang memanfaatkan kelemahan teknologi kartu pembayaran berbasis pita magnetik. Dalam perspektif hukum siber, tindakan tersebut dapat dikategorikan sebagai unauthorized access terhadap sistem elektronik, yang tidak hanya merugikan nasabah tetapi juga berpotensi menurunkan tingkat kepercayaan publik terhadap keamanan sistem perbankan digital.³ Dengan demikian, perkara ini menunjukkan bahwa permasalahan mendasar terletak pada ketidakseimbangan antara perkembangan teknologi sistem pembayaran elektronik dengan kesiapan sistem keamanan dan regulasi dalam mengantisipasi kejahatan siber di sektor keuangan.

Perkembangan transaksi keuangan digital di Indonesia menunjukkan peningkatan yang sangat signifikan dalam beberapa tahun terakhir, yang secara tidak langsung juga meningkatkan potensi kejahatan siber di sektor perbankan. Berdasarkan laporan Bank Indonesia, nilai transaksi uang elektronik pada tahun 2023 mencapai lebih dari Rp495 triliun, meningkat pesat dibandingkan beberapa tahun sebelumnya, yang menunjukkan semakin luasnya penggunaan instrumen pembayaran elektronik di masyarakat.⁴ Peningkatan volume transaksi tersebut berbanding lurus dengan meningkatnya ancaman terhadap keamanan sistem elektronik, terutama dalam bentuk pencurian data, carding, dan penyalahgunaan kartu pembayaran. Data dari Badan Siber dan Sandi Negara menunjukkan bahwa pada tahun 2022 terdapat lebih dari 700 juta serangan siber yang terdeteksi di Indonesia, yang sebagian besar menargetkan sistem informasi dan layanan digital.⁵ Selain itu, laporan mengenai kejahatan siber di Indonesia juga menunjukkan adanya lebih dari 117.000 laporan kasus kejahatan siber pada tahun 2023, dengan berbagai modus seperti penipuan online, phishing, dan pencurian data elektronik.⁶ Peningkatan jumlah laporan tersebut menunjukkan bahwa kejahatan berbasis teknologi informasi semakin sering terjadi seiring dengan berkembangnya transaksi digital di masyarakat. Dengan demikian, data kuantitatif dari berbagai laporan di Indonesia tersebut memperlihatkan bahwa kasus penyalahgunaan kartu pembayaran seperti dalam Putusan Nomor 838/Pid.Sus/2021/PN Dps merupakan bagian dari tren meningkatnya kejahatan siber yang berkaitan dengan sistem pembayaran elektronik.

Jenis cybercrime yang tercermin dalam Putusan Nomor 838/Pid.Sus/2021/PN Dps berkaitan dengan akses ilegal terhadap sistem elektronik serta penggunaan data kartu perbankan milik orang lain, yang dalam literatur keamanan siber sering dikategorikan sebagai carding atau payment card fraud. Dalam perkara tersebut, Terdakwa melakukan transaksi penarikan tunai menggunakan kartu magnetic stripe yang telah memuat data perbankan milik pihak lain, sehingga perbuatannya memenuhi unsur “mengakses komputer atau sistem elektronik tanpa hak” sebagaimana diatur dalam Pasal 30 UU ITE. Cybercrime jenis ini pada dasarnya merupakan bentuk kejahatan berbasis teknologi informasi yang memanfaatkan celah keamanan sistem pembayaran elektronik untuk memperoleh

¹ Steven Furnell and Nathan Clarke, ‘Power to the People? The Evolving Recognition of Human Aspects of Security’, *Computers & Security*, 31.8 (2012), 983–88 <<https://doi.org/10.1016/j.cose.2012.08.004>>.

² Russell Smith, Peter Grabosky, and Gregor Urbas, ‘Cyber Criminals on Trial’, *Criminal Justice Matters*, 58.1 (2004), 22–23 <<https://doi.org/10.1080/09627250408553240>>.

³ Eric Rutger Leukfeldt and Majid Yar, ‘Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis’, *Deviant Behavior*, 37.3 (2016), 263–80 <<https://doi.org/10.1080/01639625.2015.1012409>>.

⁴ Bank Indonesia, *Laporan Sistem Pembayaran Indonesia 2023* (Jakarta, 2023).

⁵ Agatha Olivia Victoria, ‘OJK: Keamanan Data Dalam Transaksi Keuangan Digital Jadi Tantangan’, *Antara News*, 2023.

⁶ Danang Arradian, ‘Inilah 13 Macam Kejahatan Siber Terbesar Di Indonesia Sepanjang 2023’, *Sindonews.Com*, 2023.

keuntungan finansial secara tidak sah.⁷ Praktik carding biasanya melibatkan proses pencurian atau penggandaan data kartu pembayaran, yang kemudian digunakan untuk melakukan transaksi tanpa sepengetahuan pemilik asli kartu tersebut.⁸ Dalam konteks kriminologi siber, tindakan tersebut juga sering dikaitkan dengan aktivitas cyber-enabled financial crime yang berkembang seiring meningkatnya penggunaan sistem pembayaran digital dan jaringan perbankan elektronik.⁹ Oleh karena itu, perbuatan dalam putusan tersebut tidak hanya menunjukkan pelanggaran terhadap sistem elektronik, tetapi juga mencerminkan bentuk kejahatan finansial modern yang memanfaatkan teknologi digital. Fenomena ini menegaskan bahwa perkembangan teknologi informasi membawa konsekuensi berupa munculnya modus kejahatan baru yang menuntut peningkatan keamanan sistem serta penegakan hukum yang lebih adaptif terhadap kejahatan siber.

Pengaturan pada cybercrime umumnya muncul karena perkembangan teknologi lebih cepat daripada pembentukan norma pidana, sehingga banyak perbuatan baru (misalnya manipulasi kartu prabayar seperti Flazz BCA) tidak disebut secara eksplisit dalam undang-undang yang ada. Dalam konteks Indonesia, penelitian tentang penegakan hukum cybercrime menunjukkan bahwa sejumlah ketentuan, khususnya dalam UU ITE, dianggap samar dalam mendefinisikan jenis-jenis kejahatan siber sehingga menimbulkan kebingungan klasifikasi delik dan ketidakpastian hukum bagi pelaku dan korban.¹⁰ Pasal 30 UU ITE merumuskan secara umum larangan mengakses komputer dan/atau sistem elektronik milik orang lain “dengan cara apa pun” dan tanpa hak atau melawan hukum, tanpa menyebut secara spesifik media atau instrumen seperti kartu prabayar (misalnya Flazz), sehingga muncul ruang penafsiran apakah tindakan modifikasi saldo kartu termasuk akses ke “sistem elektronik” atau sekadar ke media penyimpanan nilai uang elektronik.¹¹ Pasal 32 UU ITE melarang perbuatan mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan, memindahkan, atau menyembunyikan informasi atau dokumen elektronik milik orang lain, tetapi tidak membedakan secara eksplisit antara data transaksi perbankan, uang elektronik, maupun data lain yang tidak bernilai finansial, sehingga pengkualifikasian manipulasi saldo pada kartu Flazz sebagai “data interference” bergantung pada konstruksi hakim dan penyidik.¹² Pasal 35 UU ITE mengatur manipulasi informasi elektronik “dengan tujuan agar informasi tersebut dianggap seolah-olah data yang otentik”, yang secara konseptual dekat dengan praktik illegal top up/kloning Flazz, tetapi tidak ada penjelasan khusus mengenai instrumen pembayaran prabayar, sehingga penafsiran unsur “seolah-olah data yang otentik” sangat bergantung pada diskresi penegak hukum.¹³ Untuk kasus seperti illegal Flazz BCA, ketidakjelasan dapat terjadi pada beberapa titik: apakah dikualifikasikan sebagai pemalsuan instrumen pembayaran elektronik, penipuan komputer, akses ilegal ke sistem, atau kombinasi delik, karena rumusan normanya tidak secara tegas mengatur kartu prabayar tertentu. Penafsiran unsur delik dalam kasus-kasus seperti illegal Flazz BCA sangat bergantung pada diskresi

⁷ Furnell and Clarke.

⁸ Thomas J. Holt and Adam M. Bossler, ‘An Assessment of the Current State of Cybercrime Scholarship’, *Deviant Behavior*, 35.1 (2014), 20–40 <<https://doi.org/10.1080/01639625.2013.822209>>.

⁹ Tyler Moore, Richard Clayton, and Ross Anderson, ‘The Economics of Online Crime’, *Journal of Economic Perspectives*, 23.3 (2009), 3–20 <<https://doi.org/10.1257/jep.23.3.3>>.

¹⁰ Wendi Darman Laia, Martono Anggustin, and Lesson Sihotang, ‘Application of Criminal Law in Online Gambling Case’, *International Journal of Law, Crime and Justice*, 2.1 (2025), 108–21 <<https://doi.org/10.62951/ijlcj.v2i1.440>>.

¹¹ M. Syuib and Maisarah Maisarah, ‘Tindak Pidana Pencurian Jaringan Wifi Menurut Pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik’, *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, 6.1 (2021), 51 <<https://doi.org/10.22373/justisia.v6i1.10611>>.

¹² Muhammad Randy Ammar et al., “Hukum Teknologi Informasi Tentang Penipuan Transaksi Jual Beli Online,” *Jurnal Sosio-Komunika* 2, no. 1 (May 30, 2023): 244–60, <https://doi.org/10.57036/jsk.v2i1.39>.

¹³ Yolanda Sari KS and others, ‘Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik’, *Locus: Jurnal Konsep Ilmu Hukum*, 2.2 (2022), 53–67 <<https://doi.org/10.56128/jkih.v2i2.22>>.

aparatus penegak hukum dan hakim, yang dapat melahirkan putusan berbeda untuk pola perbuatan yang sama, serta bertentangan dengan asas kepastian hukum dan legalitas akibatnya jenis cybercrime spesifik seperti illegal Flazz BCA cenderung “dipaksa” masuk ke beberapa pasal sekaligus (Pasal 30, 32, 35, 36 UU ITE dan/atau pasal penipuan KUHP), yang menimbulkan ketidakpastian delik apa yang paling tepat, membuka peluang disparitas penegakan hukum, dan memperkuat karakter “pasal karet” dalam praktik.

Penelitian mengenai kejahatan siber di bidang kartu pembayaran telah banyak dilakukan, namun sebagian besar masih berfokus pada aspek normatif penegakan hukum atau kebijakan kriminal secara umum. Pertama, Adhi dan Soponyono mengkaji kebijakan penanggulangan tindak pidana carding dari perspektif politik hukum pidana dengan menitikberatkan pada formulasi kebijakan penal dan non-penal tanpa menganalisis penerapan norma dalam putusan pengadilan tertentu.¹⁴ Kedua, Novitasari, Santoso, dan Shanty membahas penerapan ketentuan hukum terhadap tindak pidana carding melalui analisis sebuah putusan pengadilan, tetapi pembahasannya masih terbatas pada kesesuaian penerapan Undang-Undang Informasi dan Transaksi Elektronik dengan fakta persidangan.¹⁵ Ketiga, Adhi dan Soponyono menganalisis penegakan hukum carding melalui politik hukum pidana dan kebijakan penal-nonpenal, tanpa mengkaji putusan, etiologi, viktimisasi, maupun keamanan sistem pembayaran elektronik secara komprehensif.¹⁶ Berbeda dengan ketiga penelitian tersebut, artikel ini mengintegrasikan analisis pertanggungjawaban pidana dengan perspektif kriminologi siber dalam satu kerangka studi kasus terhadap Putusan Nomor 838/Pid.Sus/2021/PN Dps. Analisis tidak hanya diarahkan pada pemenuhan unsur tindak pidana dan pertimbangan hakim, tetapi juga mengkaji motivasi pelaku, faktor viktimisasi, dampak terhadap korban dan industri perbankan, serta formulasi strategi pencegahan yang lebih adaptif terhadap perkembangan sistem pembayaran elektronik.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis pertanggungjawaban pidana terhadap pelaku akses ilegal dalam sistem pembayaran elektronik berdasarkan Putusan Nomor 838/Pid.Sus/2021/PN Dps serta menjelaskan fenomena tersebut melalui perspektif kriminologi siber. Hasil penelitian diharapkan memberikan kontribusi terhadap pengembangan kajian hukum pidana dan hukum siber dengan memperkaya pemahaman mengenai hubungan antara penegakan hukum, karakteristik kejahatan siber, dan kerentanan sistem pembayaran elektronik. Selain itu, artikel ini diharapkan menjadi referensi bagi akademisi, pembentuk kebijakan, aparat penegak hukum, dan industri jasa keuangan dalam merumuskan kebijakan hukum pidana serta strategi mitigasi risiko yang lebih responsif terhadap perkembangan kejahatan siber pada sektor pembayaran digital.

METODE

Penelitian ini merupakan penelitian hukum doktrinal yang menggunakan pendekatan kasus dan pendekatan konseptual dengan didukung perspektif kriminologi siber. Pendekatan kasus digunakan untuk menganalisis penerapan ketentuan hukum pidana terhadap Putusan Pengadilan Negeri

¹⁴ Hannah Maartje Kool, Asier Moneva, and Rutger Leukfeldt, ‘Exploring Trust Signals and Pathways on Cybercrime-as-a-Service Markets: The Case of Remote Access Trojans’, *Trends in Organized Crime*, 2026 <<https://doi.org/10.1007/s12117-026-09606-7>>.

¹⁵ Kool, Moneva, and Leukfeldt.

¹⁶ Muhammad Isnaeni Puspito Adhi and Eko Soponyono, ‘Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law’, *LAW REFORM*, 17.2 (2021), 135–44 <<https://doi.org/10.14710/lr.v17i2.41736>>.

Denpasar Nomor 838/Pid.Sus/2021/PN Dps yang berkaitan dengan tindak pidana akses ilegal terhadap sistem pembayaran elektronik melalui penyalahgunaan kartu Flazz BCA. Sementara itu, pendekatan konseptual digunakan untuk mengkaji konsep *unauthorized access*, *carding*, *skimming*, pertanggungjawaban pidana, serta teori-teori kriminologi siber yang relevan sebagai dasar dalam menganalisis karakteristik kejahatan dan faktor-faktor yang memengaruhi terjadinya tindak pidana. Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi Putusan Pengadilan Negeri Denpasar Nomor 838/Pid.Sus/2021/PN Dps, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, Peraturan Bank Indonesia mengenai implementasi standar teknologi chip pada kartu ATM dan kartu debit, serta peraturan perundang-undangan lain yang berkaitan dengan sistem pembayaran elektronik. Bahan hukum sekunder diperoleh dari artikel jurnal nasional dan internasional bereputasi, buku ilmiah, serta hasil penelitian terdahulu yang membahas *cybercrime*, *carding*, *skimming*, keamanan sistem pembayaran elektronik, dan kriminologi siber. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia, serta sumber referensi lain yang digunakan untuk memperjelas terminologi hukum dan teknologi informasi. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dan studi dokumen. Selanjutnya, seluruh bahan hukum dianalisis secara kualitatif dengan metode analisis preskriptif. Analisis dilakukan melalui beberapa tahapan, yaitu mengidentifikasi fakta hukum yang terdapat dalam putusan pengadilan, menguji kesesuaian fakta tersebut dengan unsur-unsur tindak pidana akses ilegal sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik, menganalisis pertimbangan hukum hakim dalam menjatuhkan putusan, kemudian mengkaji motivasi pelaku, faktor viktimisasi, dampak terhadap korban dan industri perbankan, serta merumuskan alternatif kebijakan penal dan non-penal berdasarkan perspektif kriminologi siber. Hasil analisis tersebut digunakan untuk menjelaskan hubungan antara penegakan hukum pidana dengan upaya pencegahan kejahatan terhadap sistem pembayaran elektronik dalam konteks perkembangan teknologi informasi.

DESKRIPSI KASUS

Kasus ini merupakan bentuk tindak pidana siber (*cybercrime*) di sektor perbankan yang melibatkan akses ilegal terhadap sistem elektronik tanpa izin. Perkara ini diperiksa dan diadili di Pengadilan Negeri Denpasar dengan Terdakwa bernama Kakhader Valerevich Todua. Terdakwa terbukti secara sah dan meyakinkan melakukan transaksi penarikan tunai pada mesin ATM secara melawan hukum menggunakan data perbankan milik orang lain yang telah dipindahkan ke dalam media kartu baru. Peristiwa pidana ini terjadi pada sekitar bulan Juni 2021 di wilayah Denpasar dan Badung, Bali. Modus operandi yang digunakan oleh Terdakwa adalah memanfaatkan kartu *magnetic stripe* (kartu dengan pita magnetik) berupa kartu *Flazz* BCA yang sebelumnya telah diisi dengan data perbankan milik nasabah korban. Data ilegal tersebut diperoleh Terdakwa dari seseorang bernama Igor yang statusnya masih buron atau masuk dalam Daftar Pencarian Orang (DPO). Setelah menerima sekitar sembilan kartu tiruan tersebut, Terdakwa melakukan penarikan uang tunai kurang lebih sebanyak sepuluh kali pada beberapa mesin ATM Bank BRI. Secara teknis, timbulnya korban dalam kasus ini berakar dari praktik *skimming*, yaitu penyalinan data informasi nasabah yang tertanam pada pita magnetik kartu asli menggunakan alat perekam khusus (*card skimmer*). Alat pembaca tersebut biasanya dipasang secara ilegal pada slot mesin ATM sehingga mampu menduplikasi identitas elektronik milik korban tanpa mereka sadari. Kelemahan teknologi kartu berbasis *magnetic stripe* inilah yang dimanfaatkan oleh jaringan pelaku untuk menggandakan kartu dan menguras dana rekening secara tidak sah.

Berdasarkan fakta-fakta hukum yang terungkap selama proses persidangan, Jaksa Penuntut Umum (JPU) menilai perbuatan Terdakwa telah memenuhi unsur-unsur pelanggaran hukum siber. JPU mengajukan tuntutan agar Majelis Hakim menyatakan Terdakwa bersalah melanggar Pasal 30 ayat (1) *juncto* Pasal 46 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Jaksa menuntut agar pelaku dijatuhi sanksi pokok berupa pidana penjara selama tiga tahun dikurangi masa penahanan sementara, serta dibebani pidana denda sebesar sepuluh juta rupiah subsider empat bulan kurungan. Dalam amar putusannya, Majelis Hakim Pengadilan Negeri Denpasar menyatakan Terdakwa bersalah atas dakwaan melakukan *unauthorized access* atau mengakses sistem elektronik milik orang lain dengan sengaja dan tanpa hak. Hakim mempertimbangkan hal yang memberatkan, yaitu perbuatan Terdakwa telah nyata merugikan PT Bank BRI Cabang Gatot Subroto Unit Dalung secara finansial serta menurunkan kepercayaan masyarakat terhadap sistem digital perbankan. Di sisi lain, hakim juga mempertimbangkan hal-hal yang meringankan, seperti sikap Terdakwa yang sopan, kooperatif, mengakui semua perbuatannya, serta belum pernah dihukum sebelumnya. Atas pertimbangan tersebut, hakim menjatuhkan pidana penjara dan memerintahkan perampasan barang bukti kartu elektronik untuk negara. Kasus pembobolan sistemik ini memberikan implikasi kerugian materiil dan immateriil yang signifikan bagi dunia perbankan dan masyarakat. Di satu sisi, pihak bank harus menanggung beban finansial untuk mengganti dana nasabah yang hilang sesuai dengan regulasi perlindungan konsumen OJK. Di sisi lain, reputasi institusi keuangan terancam menurun akibat kekhawatiran publik terhadap keamanan transaksi siber. Sebagai solusi jangka panjang atas maraknya kejahatan bermodus *skimming* ini, Bank Indonesia telah mewajibkan migrasi total dari teknologi kartu *magnetic stripe* yang rentan menuju teknologi kartu berbasis *chip* yang memiliki sistem autentikasi jauh lebih kuat.

PEMBAHASAN

1. Pertanggungjawaban pidana terhadap pelaku akses ilegal kartu Flazz BCA

Terdakwa melakukan tindak pidana *cybercrime* dengan cara mengakses sistem elektronik perbankan secara tidak sah melalui penggunaan kartu *magnetic stripe* yang memuat data milik nasabah lain tanpa persetujuan dari pemilik data tersebut. Perbuatan tersebut dilakukan dengan memperoleh sejumlah kartu *magnetic stripe* yang berisi data kartu perbankan milik orang lain dari seseorang bernama Igor (DPO) yang kemudian digunakan oleh Terdakwa untuk melakukan transaksi pada mesin ATM. Berdasarkan fakta yang terungkap di persidangan, Terdakwa menerima sekitar sembilan kartu *magnetic stripe* berupa kartu Flazz BCA yang berisi data kartu perbankan milik orang lain dan selanjutnya menggunakannya untuk melakukan penarikan tunai kurang lebih sepuluh kali pada beberapa mesin ATM Bank BRI yang berada di wilayah Denpasar dan Badung pada sekitar bulan Juni 2021. Perbuatan tersebut menimbulkan kerugian bagi pihak bank karena bank harus mengganti kerugian yang dialami oleh nasabah serta menimbulkan kerugian nonmateriil berupa menurunnya tingkat kepercayaan masyarakat terhadap keamanan sistem transaksi elektronik.

Dalam tuntutananya, Jaksa Penuntut Umum menyatakan bahwa Terdakwa Kakhaber Valerevich Todua terbukti secara sah dan meyakinkan melanggar Pasal 30 ayat (1) jo. Pasal 46 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik serta menuntut agar Terdakwa dijatuhi pidana penjara selama tiga tahun dengan dikurangi masa penahanan sementara serta dikenakan pidana denda sebesar sepuluh juta rupiah yang apabila tidak dibayar diganti dengan pidana kurungan selama empat bulan. Dalam pertimbangannya, majelis hakim menilai bahwa unsur “setiap orang”, unsur “dengan sengaja dan tanpa hak atau melawan hukum”, serta unsur “mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun” telah terpenuhi berdasarkan fakta persidangan. Penilaian tersebut sejalan dengan pandangan bahwa pemenuhan unsur tindak pidana dalam kasus kejahatan siber dapat dilihat dari adanya tindakan akses terhadap sistem elektronik tanpa hak serta adanya kesengajaan dari pelaku dalam memanfaatkan data elektronik milik pihak lain.¹⁷ Dengan terpenuhinya seluruh unsur tersebut, Terdakwa dinyatakan bersalah melakukan tindak pidana akses ilegal terhadap sistem elektronik sebagaimana diatur dalam UU ITE.

Dalam putusan perkara akses ilegal terhadap sistem perbankan ini, salah satu pertimbangan yang biasanya digunakan hakim adalah sikap terdakwa yang mengakui perbuatannya serta bersikap kooperatif selama proses persidangan. Sikap tersebut sering dianggap sebagai indikator bahwa terdakwa menyadari kesalahannya dan memiliki kemungkinan untuk memperbaiki perilakunya di masa yang akan datang. Pertimbangan tersebut penting agar pemidanaan tidak hanya bersifat represif, tetapi juga memperhatikan aspek keadilan dan kemanusiaan dalam sistem peradilan pidana. Oleh karena itu, penggunaan hal meringankan dalam putusan ini dapat dinilai relevan karena mencerminkan keseimbangan antara kepastian hukum, keadilan, serta tujuan pemidanaan dalam hukum pidana modern.¹⁸

Amar putusan dalam perkara ini menunjukkan bahwa Majelis Hakim Pengadilan Negeri Denpasar menjatuhkan putusan terhadap terdakwa setelah mempertimbangkan seluruh fakta

¹⁷ Rafi Septia Budianto Pansariadi and Noenik Soekorini, ‘Tindak Pidana Cyber Crime Dan Penegakan Hukumnya’, *Binamulia Hukum*, 12.2 (2023), 287–98 <<https://doi.org/10.37893/jbh.v12i2.605>>.

¹⁸ Kemal Idris Balaka, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany, ‘Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital’, *Yustitiabelen*, 10.2 (2024), 105–30 <<https://doi.org/10.36563/yustitiabelen.v10i2.1167>>.

persidangan serta terpenuhinya unsur-unsur tindak pidana yang didakwakan. Majelis Hakim menyatakan bahwa terdakwa secara sah dan meyakinkan terbukti bersalah melakukan tindak pidana di bidang informasi dan transaksi elektronik sebagaimana yang didakwakan oleh Penuntut Umum. Berdasarkan pertimbangan tersebut, pengadilan menjatuhkan pidana pokok berupa pidana penjara kepada terdakwa dalam jangka waktu tertentu sebagai bentuk pertanggungjawaban atas perbuatannya. Selain pidana penjara, hakim juga memerintahkan agar terdakwa tetap berada dalam tahanan sesuai dengan ketentuan hukum acara pidana yang berlaku. Dalam amar putusan tersebut, majelis hakim turut menetapkan status barang bukti yang digunakan dalam tindak pidana untuk dirampas atau ditetapkan sesuai dengan kepentingan pembuktian dan penegakan hukum. Putusan tersebut juga memuat perintah agar terdakwa membayar biaya perkara sebagaimana lazimnya dalam putusan pidana. Dengan demikian, amar putusan tersebut mencerminkan bentuk penegakan hukum terhadap tindak pidana yang berkaitan dengan penyalahgunaan teknologi dalam kasus kartu FLAZZ BCA yang diperiksa dan diadili di Pengadilan Negeri Denpasar.

Tindakan mengakses sistem elektronik milik pihak lain tanpa hak melalui penggunaan kartu *magnetic stripe* yang berisi data perbankan orang lain merupakan perbuatan yang sangat dilarang dalam perkara ini secara hukum. Dalam konteks keamanan transaksi digital *unauthorised access* dan penipuan data kartu pembayaran merupakan bagian dari ancaman terhadap sistem pembayaran yang terus berkembang menurut literatur keamanan siber global.¹⁹ Ketentuan Pasal 30 ayat (1) UU ITE melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses sistem elektronik milik orang lain dengan cara apapun. Prinsip ini sejalan dengan realisasi risiko dari Tindakan carding yang menjadi fokus utama penegakan UU ITE terhadap *cybercrime* di Indonesia pada era digital.²⁰ Unsur utama dalam ketentuan ini terletak pada Tindakan memasuki atau menggunakan sistem elektronik milik orang lain tanpa hak yang menjadi fokus utama dalam penegakan hukum pidana.²¹ Penggunaan kartu *magnetic stripe* menunjukkan bahwa Terdakwa memperoleh akses ke sistem ATM melalui autentifikasi yang tidak sah dalam proses transaksi perbankan digital melalui perangkat. Dengan demikian, perbuatan Terdakwa secara konseptual memenuhi unsur akses tanpa hak terhadap sistem elektronik sesuai Pasal 30 ayat (1) jo Pasal 46 UU ITE yang berlaku.

Perbuatan Terdakwa dalam perkara ini perlu dianalisis secara kritis untuk membedakan antara delik akses ilegal dengan carding yang sering terjadi di masyarakat. Carding pada umumnya merujuk pada penggunaan data kartu ATM milik orang lain secara tidak sah untuk memperoleh keuntungan finansial secara langsung menurut kajian nasional.²² Namun dalam perspektif hukum siber carding lebih tepat dipahami sebagai modus operandi untuk memperoleh akses yang didasari oleh kajian nasional tentang penegakan hukum secara yuridis.²³ Tindakan “akses tanpa hak” ke sistem elektronik menjadi fokus utama dari delik yang terbukti dalam kasus ini secara spesifik, bukan sekedar hasil transaksi. Adanya perbuatan tersebut menunjukkan bahwa penegakan hukum atas *cybercrime*

¹⁹ Aya Aljaradat, Gargi Sarkar, and Sandeep K. Shukla, 'Modelling Cybersecurity Impacts on Digital Payment Adoption: A Game Theoretic Approach', *Journal of Economic Criminology*, 5 (2024), 89 <<https://doi.org/10.1016/j.jeconc.2024.100089>>.

²⁰ Unzur Jefri Tambunan, Puguhi Aji Hari Setiawan, and Dewi Iryani, "Penegakan Hukum Tindak Pidana Carding Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Pembangunan Hukum Tindak Pidana Siber (Cybernetics)," *Jurnal Gagasan Hukum* 6, no. 02 (December 23, 2024): 140–153, <https://doi.org/10.31849/jgh.v6i02.21830>.

²¹ Ludivia Hernandez Aros and others, 'Financial Fraud Detection through the Application of Machine Learning Techniques: A Literature Review', *Humanities and Social Sciences Communications*, 11.1 (2024), 11 <<https://doi.org/10.1057/s41599-024-03606-0>>.

²² Asma Cherif et al., "Credit Card Fraud Detection in the Era of Disruptive Technologies: A Systematic Review," *Journal of King Saud University - Computer and Information Sciences* 35, no. 1 (January 2023): 145–146, <https://doi.org/10.1016/j.jksuci.2022.11.008>.

²³ 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*, 3.1 (2022), 138 <<https://doi.org/10.22225/jph.3.1.4673.138-142>>.

memerlukan regulasi yang lebih kuat dalam menghadapi kejahatan digital lainnya yang terus berkembang secara komprehensif di era digital.²⁴ Dengan demikian, delik yang terbukti bukan sekedar carding, melainkan akses sistem elektronik tanpa hak yang merugikan pihak lain secara finansial.

Berdasarkan pertimbangan Majelis Hakim menyebutkan bahwa hal yang memberatkan dalam putusan ini adalah perbuatan Terdakwa telah merugikan pihak PT. Bank BRI Cabang Gatot Subroto Unit Dalung. Pertimbangan tersebut selaras dengan pandangan bahwa kejahatan siber menyasar sistem keuangan memiliki dampak luas terhadap stabilitas dan keamanan transaksi digital sehingga dapat dijadikan factor pemberat.²⁵ Dalam prespektif pidana menegaskan bahwa pertimbangan keadaan memberatkan harus berkaitan langsung dengan karakter perubahan dan tingkat kesalahan pelaku dalam tindak pidana modern yang sangat kompleks.²⁶ Majelis Hakim menimbang atas dasar perbuatan Terdakwa yang secara sengaja menggunakan data kartu perbankan milik orang lain tanpa hak secara ilegal dan merugikan secara finansial. Dengan adanya penggunaan perangkat teknologi untuk menggadakan data kartu menunjukkan adanya unsur perencanaan dan kesengajaan yang tinggi sehingga memperkuat alasan hakim menjadikannya sebagai keadaan yang memberatkan. Pertimbangan Majelis Hakim yang menekan adanya kerugian pihak bank selaras dengan penerapan faktor pemberat yang berfungsi mempertegas efek jera sekaligus menjaga kepercayaan publik terhadap keamanan.²⁷ Dengan demikian, penggunaan hal yang memberatkan oleh Majelis Hakim dalam putusan tersebut dapat dinilai relevan karena berkaitan dengan tingkat kesalahan pelaku, dampak kerugian, serta perlindungan.

Terdapat tiga hal yang meringankan Terdakwa dalam perkara ini berdasarkan pertimbangan hakim yaitu belum pernah dihukum sebelumnya, mengakui perbuatannya, serta bersikap sopan selama persidangan berlangsung. Pertimbangan tersebut menunjukkan bahwa Majelis Hakim tidak hanya menilai perbuatan pidana secara objektif, tetapi juga memperhatikan keadaan pribadi Terdakwa sebagai bagian dari penilaian tingkat kesalahan.²⁸ Dalam kajian hukum pidana faktor seperti pengakuan kesalahan, sikap kooperatif, serta penyesalahan pelaku sering dipandang sebagai indikator adanya kesadaran hukum yang dapat dipertimbangkan oleh hakim.²⁹ Selain itu, keadaan bahwa Terdakwa belum pernah dihukum sebelumnya menunjukkan bahwa pelaku tidak sehingga kemungkinan untuk dilakukan pembinaan masih terbuka secara signifikan. Pendekatan tersebut selaras dengan prinsip individualisasi pidana yang menekankan bahwa pemidanaan harus mempertimbangkan karakteristik pribadi pelaku selain akibat dari perbuatan yang dilakukan secara sangat nyata.³⁰ Dengan demikian, keadaan yang meringankan tidak hanya berfungsi sebagai formalitas putusan, tetapi juga sebagai sarana bagi hakim untuk mencapai keseimbangan antara tujuan

²⁴ Arnanda Yusliwidaka, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana, 'A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?', *Pandecta Research Law Journal*, 19.2 (2024), 453-54 <<https://doi.org/10.15294/pandecta.v19i2.13279>>.

²⁵ Lena Klasén, Niclas Fock, and Robert Forchheimer, 'The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age', *Forensic Science International*, 362 (2024), 112 <<https://doi.org/10.1016/j.forsciint.2024.112133>>.

²⁶ Asa Intan Primanta, 'Pertanggungjawaban Pidana Pada Penyalahgunaan Data Pribadi', *Jurist-Diction*, 3.4 (2020), 14 <<https://doi.org/10.20473/jd.v3i4.20214>>.

²⁷ Shafa Salsabila and Sidi Ahyar Wiraguna, 'Pertanggungjawaban Hukum Atas Pelanggaran Data Pribadi Dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia', *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, 2.2 (2025), 145-50 <<https://doi.org/10.62383/konsensus.v2i2.736>>.

²⁸ Kevin Athallah Lazuardi and Bambang Santoso, 'Koherensi Barang Bukti Elektronik Dalam UU ITE Dan KUHAP Sebagai Pertimbangan Hakim', *Verstek*, 12.2 (2024), 63 <<https://doi.org/10.20961/jv.v12i2.82107>>.

²⁹ Aditya Rahmad Saputra, I Ketut Seregig, and Yulia Hesti, 'Judges' Considerations In Making Decisions On Actors Who Distribute/ Transmission Of Information/ Documents Violated Electronics Decency (Decision Study Number: 471/Pid.Sus/2022/PN Tjk)', *Jurnal Gagasan Hukum* 4, no. 2 (January 29, 2023): 129-135, <https://doi.org/10.31849/jgh.v4i2.12930>.

³⁰ Jesper Ryberg, 'Sentencing Offenders the Right Way: On the Importance of Relating Penal Theory and Penal Practice', *Criminal Law Forum*, 36.2 (2025), 191-204 <<https://doi.org/10.1007/s10609-025-09507-4>>.

pembalasan, pencegahan, pembinaan. Oleh karena itu, pertimbangan Majelis Hakim mengenai keadaan yang meringankan dalam perkara ini dapat dinilai relevan karena mencerminkan penerapan pidana yang sangat proposional dan berkeadilan.

Pidana pokok merupakan bentuk sanksi utama dalam sistem hukum pidana yang dijatuhkan kepada pelaku tindak pidana sebagai bentuk pertanggungjawaban atas perbuatan yang dilakukan. Dalam hukum pidana Indonesia, pidana pokok berfungsi sebagai instrumen penegakan hukum yang bertujuan untuk memberikan efek jera sekaligus melindungi kepentingan hukum masyarakat.³¹ Pidana pokok pada umumnya dijatuhkan dalam bentuk pidana penjara, pidana denda, maupun pidana kurungan yang disesuaikan dengan tingkat kesalahan pelaku serta dampak yang ditimbulkan oleh tindak pidana tersebut.³² Oleh karena itu, penerapan pidana penjara dalam perkara ini dapat dipahami sebagai bentuk respons hukum yang bertujuan memberikan efek pencegahan terhadap tindak pidana serta memperkuat fungsi hukum pidana dalam mengendalikan perilaku yang merugikan masyarakat.³³ Dalam Putusan Nomor 838/Pid.Sus/2021/PN Denpasar, majelis hakim menjatuhkan pidana penjara kepada terdakwa yang terbukti melakukan penyalahgunaan kartu FLAZZ BCA secara ilegal. Penjatuhan pidana tersebut meunjukkan bahwa perbuatan terdakwa dipandang memiliki tingkat keseriusan yang cukup tinggi karena berkaitan dengan sistem transaksi elektronik yang melibatkan kepercayaan publik. Dengan demikian, pidana pokok yang dijatuhkan oleh majelis hakim dalam perkara ini dapat dinilai relevan karena sejalan dengan tujuan pidana yang menekankan perlindungan masyarakat, pemberian efek jera, dan upaya pencegahan tindak pidana.

Selain berfungsi sebagai bentuk pertanggungjawaban pidana, pidana pokok juga memiliki tujuan untuk menciptakan keseimbangan antara kepentingan pelaku, korban, dan masyarakat dalam sistem peradilan pidana. Dalam teori pidana, hukuman yang dijatuhkan harus mempertimbangkan prinsip proporsionalitas agar sebanding dengan tingkat kesalahan pelaku serta akibat yang ditimbulkan dari tindak pidana tersebut.³⁴ Dalam perkara penyalahgunaan kartu FLAZZ BCA, tindakan terdakwa tidak hanya melanggar hukum tetapi juga berpotensi merusak sistem keamanan transaksi elektronik yang digunakan oleh masyarakat luas. Oleh karena itu, penjatuhan pidana penjara menjadi amat penting untuk menunjukkan bahwa negara memberikan perlindungan terhadap sistem pembayaran elektronik dari penyalahgunaan yang dilakukan secara melawan hukum.³⁵ Selain itu, penerapan pidana pokok juga memiliki fungsi preventif agar pelaku maupun masyarakat lainnya tidak melakukan perbuatan serupa di masa mendatang. Dalam konteks ini, pidana penjara yang dijatuhkan oleh hakim dapat dipandang sebagai bentuk kebijakan hukum pidana yang bertujuan menjaga stabilitas dan keamanan sistem transaksi elektronik.³⁶ Dengan demikian, relevansi pidana pokok dalam putusan tersebut dapat dilihat dari kesesuaiannya dengan tujuan pidana yang mencakup aspek keadilan, pencegahan, serta perlindungan terhadap kepentingan umum.

Perampasan barang merupakan salah satu bentuk pidana tambahan yang dapat dijatuhkan oleh hakim terhadap barang yang berkaitan dengan suatu tindak pidana. Dalam hukum pidana,

³¹ James Manwaring, 'Proportionality's Lower Bound', *Criminal Law and Philosophy*, 15:3 (2021), 393–405 <<https://doi.org/10.1007/s11572-021-09577-6>>.

³² Thomas J Miceli, 'On Economic Theories of Criminal Punishment: Pricing, Prevention, or Proportionality?', *American Law and Economics Review*, 25:1 (2023), 1–26 <<https://doi.org/10.1093/aler/ahad003>>.

³³ P. H. Robinson, 'Does Criminal Law Deter? A Behavioural Science Investigation', *Oxford Journal of Legal Studies*, 24:2 (2004), 173–205 <<https://doi.org/10.1093/ojls/24.2.173>>.

³⁴ Murat AYDIN, 'Ceza Hukukunda Orantılılık', *Türkiye Adalet Akademisi Dergisi*, YOK.57 (2024), 141–68 <<https://doi.org/10.54049/taad.1418150>>.

³⁵ S. I. Benn, 'An Approach to the Problems of Punishment', *Philosophy*, 33:127 (1958), 325–41 <<https://doi.org/10.1017/S0031819100055017>>.

³⁶ Economic Crimes, *Economic Crimes and Corruption Nomos*, 2021 <<https://doi.org/https://doi.org/10.5771/9783748922599>>.

perampasan barang bertujuan untuk menghilangkan keuntungan yang diperoleh dari suatu tindak pidana sehingga pelaku tidak dapat menikmati hasil kejahatan yang dilakukannya.³⁷ Selain itu, perampasan barang juga berfungsi sebagai sarana untuk mencegah penggunaan kembali barang yang dapat memfasilitasi terjadinya tindak pidana.³⁸ Dalam Putusan Nomor 838/Pid.Sus/2021/PN Denpasar, majelis hakim menetapkan bahwa barang-barang yang berkaitan dengan tindak pidana penyalahgunaan kartu FLAZZ BCA dirampas untuk negara. Keputusan tersebut menunjukkan bahwa barang yang digunakan dalam tindak pidana dipandang memiliki hubungan langsung dengan perbuatan yang dilakukan oleh terdakwa. Oleh karena itu, perampasan barang menjadi Langkah yang penting untuk memastikan bahwa sarana yang digunakan dalam tindak pidana tidak dapat dimanfaatkan kembali.³⁹ Dengan demikian, penerapan pidana tambahan berupa perampasan barang dalam putusan tersebut dapat dinilai relevan karena sejalan dengan tujuan penegakan hukum dalam memberantas kejahatan berbasis teknologi.

Selain menghilangkan keuntungan ekonomi dari hasil kejahatan, perampasan barang juga memiliki fungsi strategis dalam sistem peradilan pidana untuk memutus sarana yang digunakan dalam tindak pidana. Dalam berbagai kasus kejahatan yang berkaitan dengan teknologi atau sistem transaksi elektronik, alat yang digunakan oleh pelaku sering kali menjadi faktor penting yang memungkinkan terjadinya tindak pidana.⁴⁰ Oleh karena itu, kebijakan perampasan barang tidak hanya dilihat dari nilai ekonominya tetapi juga dari perannya sebagai alat yang memfasilitasi tindak pidana. Dalam perkara penyalahgunaan kartu FLAZZ BCA, barang yang digunakan oleh terdakwa dapat dianggap sebagai sarana yang memungkinkan terjadinya pelanggaran terhadap sistem transaksi elektronik. Oleh sebab itu, tindakan perampasan barang oleh negara dapat dipandang sebagai Langkah preventif untuk mencegah terulangnya tindak pidana yang sama.⁴¹ Selain itu, kebijakan tersebut juga menunjukkan bahwa sistem hukum pidana berupaya menutup seluruh kemungkinan bagi pelaku untuk kembali memanfaatkan sarana kejahatan yang pernah digunakannya.⁴² Dengan demikian, pidana tambahan berupa perampasan barang dalam putusan ini memiliki relevansi yang kuat karena tidak hanya bersifat represif tetapi juga preventif dalam upaya penanggulangan tindak pidana.

2. Fenomena akses ilegal kartu Flazz BCA dianalisis dalam perspektif kriminologi siber

Kejahatan dapat terjadi apabila pelaku mempunyai pengetahuan untuk melakukan kejahatan tersebut dan memiliki justifikasi untuk melakukan kejahatan tersebut. Dalam kasus tersebut motivasi pelaku melakukan cybercrime dalam perkara ini pada umumnya dilatarbelakangi oleh keinginan untuk memperoleh keuntungan ekonomi secara cepat dengan memanfaatkan celah pada sistem teknologi yang digunakan dalam transaksi elektronik. Kejahatan ekonomi dewasa ini tidak hanya dilakukan dalam kehidupan nyata, dengan adanya kemajuan teknologi yang pesat, segala aspek kehidupan telah terhubung dalam sistem internet. Hal ini di samping menunjukkan adanya keefektifan dan efisiensi juga menimbulkan modus-modus operandi untuk melakukan kejahatan yang terstruktur. Dengan adanya peluang dan keterbukaan media sosial terhadap segala ilmu pengetahuan memunculkan

³⁷ Valsamis Mitsilegas, 'Reconceptualising Security in the Law of the European Union', *European Papers - A Journal on Law and Integration*, 9.3 (2024), 1438–73 <<https://doi.org/10.15166/2499-8249/817>>.

³⁸ Associate Radha Ivory, "Third-Party Rights: Giving The Hedgehog A Foxy Tail," 2023, <https://doi.org/10.1017/S1744552315000269>.

³⁹ *Introduction to Hungarian Law* <<https://doi.org/10.1017/9781108891875.003>>.

⁴⁰ *Tax Crimes and Enforcement in the European Union*, *Tax Crimes and Enforcement in the European Union*, 2023 <<https://doi.org/10.1093/oso/9780192862341.001.0001>>.

⁴¹ Michele Simonato, 'Confiscation and Fundamental Rights across Criminal and Non-Criminal Domains', *ERA Forum*, 18.3 (2017), 365–79 <<https://doi.org/10.1007/s12027-017-0485-0>>.

⁴² Ade Sofyan, 'Penerapan Asas Proporsionalitas Dalam Penjatuhan Pidana Terhadap Pelaku Tindak Pidana', *Hukum Responsif*, 15.2 (2024), 290 <<https://doi.org/10.33603/responsif.v15i2.9486>>.

tantangan baru terhadap penyalahgunaan ilmu pengetahuan untuk hal-hal yang tidak tepat. Pembayaran digital seperti kartu uang elektronik memberikan peluang bagi pihak tertentu untuk menyalahgunakannya melalui manipulasi data atau sistem yang ada dengan pengetahuan yang mereka peroleh. Oleh karena itu, tindakan tersebut menunjukkan bahwa faktor keuntungan finansial menjadi pendorong utama bagi pelaku dalam melakukan kejahatan siber.

Timbulnya korban dalam perkara ini berkaitan dengan adanya penyalahgunaan data kartu perbankan yang dilakukan melalui praktik skimming yang memungkinkan pelaku memperoleh informasi kartu milik nasabah tanpa sepengetahuan pemiliknya. Berdasarkan fakta yang terungkap di persidangan, penggunaan kartu magnetic stripe yang berisi data kartu perbankan milik orang lain tersebut kemudian dimanfaatkan untuk melakukan transaksi pada mesin ATM sehingga dana dalam rekening nasabah berpindah secara tidak sah. Keadaan ini menyebabkan nasabah menjadi pihak yang dirugikan karena terjadi pengurangan saldo akibat transaksi yang tidak pernah mereka lakukan maupun setuju. Modus kejahatan seperti ini pada umumnya dilakukan dengan cara menyalin data pada pita magnetik kartu ATM menggunakan alat khusus yang dipasang pada mesin ATM atau perangkat pembayaran lain sehingga data kartu dapat digandakan oleh pelaku.⁴³ Pemberitaan media juga menyebutkan bahwa praktik skimming masih menjadi ancaman dalam sistem transaksi perbankan karena pelaku dapat memanfaatkan kelemahan pada teknologi kartu berbasis magnetic stripe untuk memperoleh data nasabah secara ilegal.⁴⁴ Selain itu, sejumlah kasus menunjukkan bahwa lemahnya perlindungan konsumen dan celah dalam sistem keamanan perbankan dapat meningkatkan risiko terjadinya penyalahgunaan data kartu yang berdampak pada kerugian finansial bagi nasabah.⁴⁵ Dengan demikian, keadaan yang menyebabkan timbulnya korban dalam kasus ini tidak hanya berasal dari tindakan pelaku, tetapi juga dipengaruhi oleh kerentanan sistem keamanan kartu perbankan yang memungkinkan terjadinya pencurian dan penyalahgunaan data kartu oleh pihak yang tidak bertanggung jawab.

Motivasi pelaku dalam tindak pidana akses ilegal terhadap sistem perbankan pada umumnya berkaitan dengan faktor ekonomi dan keinginan untuk memperoleh keuntungan secara cepat. Perkembangan teknologi informasi telah mendorong sistem perbankan beralih ke sistem digital yang memudahkan masyarakat dalam melakukan transaksi keuangan. Namun kemajuan tersebut juga membuka peluang terjadinya kejahatan siber yang memanfaatkan sistem elektronik perbankan. Pelaku biasanya memanfaatkan kelemahan sistem keamanan untuk memperoleh data nasabah atau melakukan transaksi secara tidak sah. Dalam perspektif kriminologi, cybercrime sering terjadi karena pelaku melihat adanya kesempatan yang besar serta risiko yang relatif kecil dibandingkan keuntungan yang diperoleh.⁴⁶ Selain itu, kemampuan teknologi yang dimiliki oleh pelaku juga menjadi faktor penting dalam terjadinya tindak pidana ini. Individu yang memiliki pengetahuan mengenai sistem komputer dan jaringan cenderung lebih mudah melakukan akses ilegal terhadap sistem informasi perbankan.⁴⁷

Selain faktor ekonomi, tindak pidana akses ilegal terhadap sistem perbankan juga sering dilakukan secara terorganisir oleh kelompok tertentu. Dalam praktik cybercrime, pelaku tidak selalu

⁴³ Lentera Bisnis, 'Waspada! Ancaman Skimming Saat Transaksi Perbankan Di ATM', *Lentera Bisnis*, 2024.

⁴⁴ M.H Akhmad Zaenuddin, S.H, 'Kejahatan Skimming ATM, Begini Hukumnya', *Kompas.Com*, 2021.

⁴⁵ Kabar Bisnis Rise and Shine, 'Kasus Skimming Perbankan, Bukti Masih Lemahnya Perlindungan Ke Konsumen', *Kabarbisnis.Com*, 2018.

⁴⁶ Muhammad Khairul Faridi, 'Kejahatan Siber Dalam Bidang Perbankan', *Cyber Security Dan Forensik Digital*, 1.2 (2019), 57-61 <<https://doi.org/10.14421/csecurity.2018.1.2.1373>>.

⁴⁷ Nunuk Sulisrudatin, 'ANALISA KASUS CYBERCRIME BIDANG PERBANKAN BERUPA MODUS PENCURIAN DATA KARTU KREDIT', *JURNAL ILMIAH HUKUM DIRGANTARA*, 9.1 (2014), 26-39 <<https://doi.org/10.35968/jh.v9i1.296>>.

bekerja sendiri tetapi bekerja sama dengan pihak lain yang memiliki peran berbeda dalam melakukan kejahatan tersebut. Ada pihak yang bertugas memperoleh data nasabah, pihak yang melakukan penggandaan kartu atau manipulasi data, serta pihak yang melakukan transaksi penarikan dana. Perkembangan teknologi digital memudahkan pelaku memanfaatkan berbagai perangkat elektronik untuk menyalin ataupun memanipulasi informasi perbankan. Penelitian menunjukkan bahwa meningkatnya penggunaan teknologi digital dalam sektor keuangan juga meningkatkan risiko terjadinya kejahatan siber.⁴⁸ Selain itu, lemahnya sistem pengawasan dan keamanan informasi sering kali dimanfaatkan oleh pelaku untuk melakukan tindak pidana. Oleh karena itu, motivasi pelaku cybercrime tidak hanya dipengaruhi oleh faktor ekonomi tetapi juga oleh peluang yang muncul akibat perkembangan teknologi dan kelemahan sistem keamanan.

Pidana tambahan berupa perampasan barang merupakan salah satu bentuk kebijakan hukum pidana yang bertujuan untuk mendukung efektivitas penegakan hukum terhadap pelaku kejahatan. Dalam perkara cybercrime, perampasan barang biasanya dilakukan terhadap alat yang digunakan untuk melakukan tindak pidana seperti laptop, kartu elektronik, alat skimming, dan perangkat penyimpanan data. Perampasan tersebut menjadi relevan karena barang tersebut memiliki keterkaitan langsung dengan terjadinya tindak pidana. Selain itu, tindakan ini juga bertujuan untuk mencegah pelaku menggunakan kembali alat tersebut untuk melakukan kejahatan serupa. Penerapan pidana tambahan ini juga merupakan bagian dari upaya hukum untuk memberikan efek jera kepada pelaku kejahatan digital.⁴⁹ Hal ini sejalan dengan tujuan hukum pidana modern yang tidak hanya menghukum pelaku tetapi juga mencegah terulangnya kejahatan. Dengan demikian, perampasan barang bukti dalam cybercrime memiliki nilai strategis dalam sistem pemidanaan.

Selain sebagai bentuk efek jera, perampasan barang juga memiliki fungsi preventif dalam mencegah berkembangnya kejahatan berbasis teknologi. Hakim dalam menjatuhkan pidana tambahan biasanya mempertimbangkan hubungan antara barang bukti dengan tindak pidana yang dilakukan terdakwa. Jika terbukti bahwa barang tersebut merupakan sarana utama kejahatan maka secara hukum dapat dirampas untuk negara. Kebijakan ini juga menunjukkan bahwa hukum pidana berfungsi untuk melindungi masyarakat dari potensi kejahatan yang berulang.⁵⁰ Dalam praktiknya, barang yang tidak memiliki nilai ekonomis biasanya akan dimusnahkan untuk menghindari penyalahgunaan kembali. Selain itu, barang yang memiliki nilai ekonomis dapat dirampas untuk negara sesuai ketentuan hukum yang berlaku.⁵¹ Oleh karena itu, pidana tambahan berupa perampasan barang dapat dinilai sebagai langkah yang relevan dalam mendukung kebijakan pemberantasan cybercrime.⁵²

Dalam kasus tersebut selain menimbulkan kerugian bagi korban secara materiil yakni berupa kerugian finansial di sisi lain tindakan pelaku juga menimbulkan kerugian immateriil. Kejahatan siber berupa scamming yang menimbulkan kerugian finansial secara tidak langsung dapat menyebabkan

⁴⁸ Idris Balaka, Rahman Hakim, and Dwi Sulistyany.

⁴⁹ Rian Dwi Hapsari and Kuncoro Galih Pambayun, 'ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis', *Jurnal Konstituen*, 5.1 (2023), 1–17 <<https://doi.org/10.33701/jk.v5i1.3208>>.

⁵⁰ Aradea Murti Basunjaya and I Gusti Nyoman Krisnadi Yudiantara, 'Pemidanaan Cybercrime Melalui Perspektif Hukum Pidana Di Indonesia', *Jurnal Media Akademik (Jma)*, 3.7 (2025), 8–9 <<https://doi.org/https://doi.org/10.62281/v3i7.2497>>.

⁵¹ Bitus Tanjung and Marjan Miharja, 'Penerapan Sanksi Pidana Bagi Pelaku Tindak Pidana Peretasan (Studi Kasus Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN Ckr)', *Iblam Law Review*, 4.4 (2024), 100–110 <<https://doi.org/10.52249/ilr.v4i4.471>>.

⁵² Irfan Santoso and others, 'Kebijakan Hukum Pidana Terhadap Perbuatan Melawan Hukum Dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal - Pasal Tertentu UU ITE', *Locus Journal of Academic Literature Review*, 3.4 (2024), 329–35 <<https://doi.org/10.56128/ljoalr.v3i4.312>>.

dampak lain termasuk kebocoran data pribadi dan tekanan psikologis.⁵³ Dalam konteks pencurian data pribadi skimming pertama-tama dilakukan dengan menyalin data informasi korban yang terdapat pada ATM magnetic stripe sehingga hal ini termasuk dalam kualifikasi pencurian data pribadi.⁵⁴ Menjadi masalah lebih lanjut apabila pencurian data pribadi tersebut tidak berhenti hanya pada kasus yang telah terjadi akan tetapi disalahgunakan seperti dijual ke situs dark web yang pernah terjadi dalam kasus kebocoran Kemendikbud tahun 2024,⁵⁵ dalam beberapa kasus hal ini dapat menyebabkan terjadinya re-viktimisasi dimana korban rentan untuk menjadi korban kejahatan lainnya.⁵⁶ Dalam konteks tekanan psikologis korban kejahatan siber sering mengalami emosi negatif dengan tendensi menyalahkan diri sendiri yang menyebabkan trauma dan kecemasan berlebih.⁵⁷ Dengan adanya trauma tersebut dampak yang ditimbulkan bukan hanya pada trauma penggunaan teknologi ATM akan tetapi berdampak pada penggunaan teknologi lain dikarenakan munculnya ketakutan akan menjadi korban kejahatan siber lainnya. Oleh karena itu dampak secara immateriil selain berdampak langsung terhadap korban dengan adanya kasus-kasus tersebut secara tidak langsung dapat menimbulkan ketidakpercayaan dan kecemasan bagi masyarakat luas.

Dalam kerangka pemikiran masyarakat secara umum Perbankan sebagai penyedia layanan akan menjadi salah satu dan yang utama untuk dimintai pertanggungjawaban atas apa yang terjadi. Perbankan sebagai pihak penyedia layanan dalam menarik customer awam menggunakan penggantian kerugian apabila terjadi *fraud*,⁵⁸ dalam beberapa kasus bentuk tanggung jawab yang dilakukan oleh pihak perbankan yakni dengan melakukan penggantian dana kepada nasabah setelah melalui proses pengecekan fakta.⁵⁹ Hal ini sejalan dengan adanya Peraturan Otoritas Jasa Keuangan Nomor 1 Tahun 2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan Pasal 29 berbunyi “pelaku usaha jasa keuangan wajib bertanggung jawab atas kerugian konsumen yang timbul akibat kesalahan dan/atau kelalaian, pengurus, pegawai pelaku usaha jasa keuangan dan/atau pihak ketiga yang bekerja untuk kepentingan pelaku usaha jasa keuangan.”⁶⁰ Dengan adanya kebobolan sistemik ini menimbulkan dampak kerugian materiil yang besar bagi pihak perbankan dimana dalam hal ini perbankan harus mengalami peningkatan biaya operasional untuk penggantian dana nasabah, melakukan investigasi terhadap kasus, dan memperbaiki sistem layanan. Seperti yang terjadi pada tahun 2016 BRI harus menanggung biaya kerugian akibat *skimming* sampai dengan 2,7 miliar. Selain itu kerugian immateriil juga turut menjadi beban yang harus ditanggung oleh perbankan seperti dengan menurunnya kepercayaan masyarakat terhadap layanan perbankan yang secara signifikan dapat menurunkan reputasi bank. Dengan menurunnya reputasi bank permasalahan lebih lanjut yang akan timbul yakni menurunnya kepercayaan masyarakat terhadap produk-produk bank lainnya diluar

⁵³ Luke Balcombe, ‘The Mental Health Impacts of Internet Scams’, *International Journal of Environmental Research and Public Health*, 22.6 (2025), 938 <<https://doi.org/10.3390/ijerph22060938>>.

⁵⁴ Oktari Anggi Setya Pratama, ‘Pertanggungjawaban Pidana Pelaku Tindak Pidana Pencurian Data Elektronik Ditinjau Berdasarkan Undang-Undang ITE’, *Jurnal Sosial Humaniora Sigli (JSIH)*, 8.1 (2025), 261 <<https://doi.org/https://doi.org/10.61104/alz.v3i4.2022>>.

⁵⁵ Ahmad Al Qodri Azizi Dalimunthe and Mulkan Azhari, ‘Analisis Forensik Digital Terhadap Perdagangan Data Pribadi Di Dark Web Menggunakan Osint & Threat Intelligence’, *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, 4.1 (2025), 254–68 <<https://doi.org/10.62712/juktisi.v4i1.400>>.

⁵⁶ P.A.H. Sarkki and others, ‘Fear of Cybercrime Victimization: Examining the Relationship between Fear and Victimization’, *Journal of Criminal Justice*, 101 (2025), 102531 <<https://doi.org/10.1016/j.jcrimjus.2025.102531>>.

⁵⁷ Xiaowei Chen and others, *From Harm to Healing: Understanding Individual Resilience after Cybercrimes*, *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26)*, April 13th–17, 2026, Barcelona, Spain (arXiv, 2026), 1 <<https://doi.org/10.1145/3772318.3791486>>.

⁵⁸ Ingolf Becker and others, ‘International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms’, *Journal of Cybersecurity*, 3.2 (2017), 109–25 <<https://doi.org/10.1093/cybsec/tyx011>>.

⁵⁹ Reza Aditya Pamuji, ‘Perlindungan Hukum Bagi Nasabah Dan Tanggung Jawab Bank Dalam Kasus Card Skimming’, *Jurnal Lex Renaissance*, 3.1 (2018), 32 <<https://doi.org/10.20885/JLR.vol3.iss1.art12>>.

⁶⁰ Ayu Lestari, Muhaimin Muhaimin, and Diman Ade Mulada, ‘Tanggung Jawab Pihak Bank Kepada Nasabah Terhadap Kejahatan Skimming (Studi Di Bank Syariah Indonesia Mataram)’, *Commerce Law*, 2.1 (2022), 109 <<https://doi.org/10.29303/commercelaw.v2i1.1374>>.

dari produk alat pembayaran. Pada akhirnya bank harus memikirkan cara dan metode untuk membangun reputasinya kembali di kalangan masyarakat, bukan hanya untuk mempertahankan *customer* yang telah ada akan tetapi untuk menggaet kepercayaan *customer* baru.

SIMPULAN

Praktik skimming terhadap kartu ATM magnetic stripe dengan menyadap informasi yang terdapat dalam kartu ATM adalah tindak pidana yang berkaitan dengan suatu sistem teknologi. Modus operandi yang umum digunakan oleh pelaku yakni dengan cara memasang alat pembaca kartu atau card skimmer pada slot kartu di dalam mesin ATM sehingga ketika nasabah memasukkan kartu ATM maka data akan terbaca oleh alat skimmer dan pelaku dapat menduplikat kartu ATM tersebut. Pada dasarnya praktik ini telah dilakukan sejak lama yakni pertama kali tercatat pada tahun 2009 yang lalu yang terdapat di ATM Citibank, Woodland Hills, California. Pembobolan suatu sistem menandakan bahwa terdapat celah dalam suatu sistem tersebut sehingga rentan akan penyadapan dan perusakan, dalam hal ini manajemen resiko harus berperan aktif dalam memperkuat pertahanan serangan siber. Berbicara mengenai solusi untuk cyber crime ini tidak boleh berhenti hanya pada penegakan hukum nya akan tetapi berfokus pada bagaimana cara memperbaiki suatu sistem tersebut. Pada mulanya solusi preventif yang pernah dilakukan di Indonesia bersifat konvensional seperti memberikan edukasi kepada masyarakat untuk berhati-hati, penyebaran informasi melalui pers, dan Membentuk Tim Kerja Sama Pengawas ATM/Penguatan Kembali Peran Bank Dalam Pengawasan ATM. Oleh karena itu, solusi yang diterapkan di Indonesia ini belum secara signifikan menyelesaikan akar masalah, sehingga praktik skimming terhadap kartu ATM masih banyak dilakukan di Indonesia hingga tahun 2022.

Solusi lebih lanjut dapat diaplikasikan secara efektif dan efisien apabila solusi tersebut berangkat dari akar permasalahannya yakni sistem yang rentan akan pembobolan dan perusakan. Tepat pada tahun 2015 surat edaran BI No.17/52/DKSP menjadi tonggak awal Perihal Implementasi Standar Nasional Teknologi Chip dan Penggunaan Personal Identification Number Online 6 (Enam) Digit untuk Kartu ATM dan/atau Kartu Debit. Pada pokoknya inti dari penggantian sistem menggunakan teknologi chip ini bertujuan untuk meningkatkan keamanan dikarenakan kartu ATM berbasis chip tidak mudah untuk digandakan karena data yang ada tersimpan di dalam chip dan dilengkapi dengan autentikasi dua faktor. Pada surat edaran BI tersebut bank-bank yang masih menggunakan magnetic stripe pada kartu ATM diberi waktu hingga sampai tanggal 31 Desember 2021 untuk melakukan proses penggantian ke teknologi chip. Proses penggantian ini tentunya memerlukan waktu yang bertahap mengingat banyaknya nasabah yang menggunakan kartu fisik atm sebagai proses transaksi mereka. Solusi ini dinilai efektif meskipun memerlukan transisi yang cukup besar dan perlunya dukungan dari semua pihak terutama yakni nasabah itu sendiri sebagai sasaran utama edukasi keamanan transaksi. Di samping solusi non-penal, hukum pidana juga turut sumbangsih dengan menerapkan sanksi penal terhadap pelaku, perbuatan ini masuk dalam perbuatan “dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik dengan cara apapun.”

DAFTAR PUSTAKA

Adhi, Muhammad Isnaeni Puspito, and Eko Soponyono, ‘Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law’, *LAW REFORM*, 17 (2021), 135-44
<<https://doi.org/10.14710/lr.v17i2.41736>>

- Akhmad Zaenuddin, S.H, M.H, 'Kejahatan Skimming ATM, Begini Hukumnya', *Kompas.Com*, 2021
- Aljaradat, Aya, Gargi Sarkar, and Sandeep K. Shukla, 'Modelling Cybersecurity Impacts on Digital Payment Adoption: A Game Theoretic Approach', *Journal of Economic Criminology*, 5 (2024), 89 <<https://doi.org/10.1016/j.jeconc.2024.100089>>
- Aradea Murti Basunjaya, and I Gusti Nyoman Krisnadi Yudiantara, 'Pemidanaan Cybercrime Melalui Perspektif Hukum Pidana Di Indonesia', *Jurnal Media Akademik (Jma)*, 3 (2025), 8–9 <<https://doi.org/https://doi.org/10.62281/v3i7.2497>>
- Arradian, Danang, 'Inilah 13 Macam kejahatan Siber Terbesar Di Indonesia Sepanjang 2023', *Sindonews.Com*, 2023
- AYDIN, Murat, 'Ceza Hukukunda Orantilililkesi', *Türkiye Adalet Akademisi Dergisi*, YOK (2024), 141–68 <<https://doi.org/10.54049/taad.1418150>>
- Balcombe, Luke, 'The Mental Health Impacts of Internet Scams', *International Journal of Environmental Research and Public Health*, 22 (2025), 938 <<https://doi.org/10.3390/ijerph22060938>>
- Bank Indonesia, *Laporan Sistem Pembayaran Indonesia 2023* (Jakarta, 2023)
- Becker, Ingolf, Alice Hutchings, Ruba Abu-Salma, Ross Anderson, Nicholas Bohm, Steven J Murdoch, and others, 'International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms', *Journal of Cybersecurity*, 3 (2017), 109–25 <<https://doi.org/10.1093/cybsec/tyx011>>
- Benn, S. I., 'An Approach to the Problems of Punishment', *Philosophy*, 33 (1958), 325–41 <<https://doi.org/10.1017/S0031819100055017>>
- Bisnis, Lentera, 'Waspada! Ancaman Skimming Saat Transaksi Perbankan Di ATM', *Lentera Bisnis*, 2024
- Cahyadi, 'Perlindungan Hukum Terhadap Nasabah Dari Ancaman', *Jurnal Analisis Hukum*, 2 (2019), 169
- Chen, Xiaowei, Mindy Tran, Yue Deng, Bhupendra Acharya, and Yixin Zou, *From Harm to Healing: Understanding Individual Resilience after Cybercrimes, Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain* (arXiv, 2026), 1 <<https://doi.org/10.1145/3772318.3791486>>
- Cherif, Asma, Arwa Badhib, Heyfa Ammar, Suhair Alshehri, Manal Kalkatawi, and Abdessamad Imine, 'Credit Card Fraud Detection in the Era of Disruptive Technologies: A Systematic Review', *Journal of King Saud University - Computer and Information Sciences*, 35 (2023), 145–46 <<https://doi.org/10.1016/j.jksuci.2022.11.008>>
- Crimes, Economic, *Economic Crimes and Corruption Nomos*, 2021 <<https://doi.org/https://doi.org/10.5771/9783748922599>>
- Dalimunthe, Ahmad Al Qodri Azizi, and Mulkan Azhari, 'Analisis Forensik Digital Terhadap Perdagangan Data Pribadi Di Dark Web Menggunakan Osint & Threat Intelligence', *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, 4 (2025), 254–68 <<https://doi.org/10.62712/juktisi.v4i1.400>>
- Faridi, Muhammad Khairul, 'Kejahatan Siber Dalam Bidang Perbankan', *Cyber Security Dan Forensik*

Digital, 1 (2019), 57–61 <<https://doi.org/10.14421/csecurity.2018.1.2.1373>>

Furnell, Steven, and Nathan Clarke, 'Power to the People? The Evolving Recognition of Human Aspects of Security', *Computers & Security*, 31 (2012), 983–88 <<https://doi.org/10.1016/j.cose.2012.08.004>>

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 (2022), 138 <<https://doi.org/10.22225/jph.3.1.4673.138-142>>

Hapsari, Rian Dwi, and Kuncoro Galih Pambayun, 'ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis', *Jurnal Konstituen*, 5 (2023), 1–17 <<https://doi.org/10.33701/jk.v5i1.3208>>

Hernandez Aros, Ludivia, Luisa Ximena Bustamante Molano, Fernando Gutierrez-Portela, John Johver Moreno Hernandez, and Mario Samuel Rodríguez Barrero, 'Financial Fraud Detection through the Application of Machine Learning Techniques: A Literature Review', *Humanities and Social Sciences Communications*, 11 (2024), 11 <<https://doi.org/10.1057/s41599-024-03606-0>>

Holt, Thomas J., and Adam M. Bossler, 'An Assessment of the Current State of Cybercrime Scholarship', *Deviant Behavior*, 35 (2014), 20–40 <<https://doi.org/10.1080/01639625.2013.822209>>

Idris Balaka, Kemal, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany, 'Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital', *Yustitiabelen*, 10 (2024), 105–30 <<https://doi.org/10.36563/yustitiabelen.v10i2.1167>>

Introduction to Hungarian Law <<https://doi.org/https://doi.org/10.1017/9781108891875.003>>

Ivory, Associate Radha, 'THIRD-PARTY RIGHTS : GIVING THE HEDGEHOG A FOXY TAIL', 2023 <<https://doi.org/https://doi.org/10.1017/S1744552315000269>>

Kabar Bisnis Rise and Shine, 'Kasus Skimming Perbankan, Bukti Masih Lemahnya Perlindungan Ke Konsumen', *Kabarbisnis.Com*, 2018

Klasén, Lena, Niclas Fock, and Robert Forchheimer, 'The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age', *Forensic Science International*, 362 (2024), 112 <<https://doi.org/10.1016/j.forsciint.2024.112133>>

Kool, Hannah Maartje, Asier Moneva, and Rutger Leukfeldt, 'Exploring Trust Signals and Pathways on Cybercrime-as-a-Service Markets: The Case of Remote Access Trojans', *Trends in Organized Crime*, 2026 <<https://doi.org/10.1007/s12117-026-09606-7>>

Lazuardi, Kevin Athallah, and Bambang Santoso, 'Koherensi Barang Bukti Elektronik Dalam UU ITE Dan KUHAP Sebagai Pertimbangan Hakim', *Verstek*, 12 (2024), 63 <<https://doi.org/10.20961/jv.v12i2.82107>>

Lestari, Ayu, Muhaimin Muhaimin, and Diman Ade Mulada, 'Tanggung Jawab Pihak Bank Kepada Nasabah Terhadap Kejahatan Skimming (Studi Di Bank Syariah Indonesia Mataram)', *Commerce Law*, 2 (2022), 109 <<https://doi.org/10.29303/commercelaw.v2i1.1374>>

Leukfeldt, Eric Rutger, and Majid Yar, 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis', *Deviant Behavior*, 37 (2016), 263–80 <<https://doi.org/10.1080/01639625.2015.1012409>>

Manwaring, James, 'Proportionality's Lower Bound', *Criminal Law and Philosophy*, 15 (2021), 393–405

<<https://doi.org/10.1007/s11572-021-09577-6>>

- Miceli, Thomas J, 'On Economic Theories of Criminal Punishment: Pricing, Prevention, or Proportionality?', *American Law and Economics Review*, 25 (2023), 1–26
 <<https://doi.org/10.1093/aler/ahad003>>
- Mitsilegas, Valsamis, 'Reconceptualising Security in the Law of the European Union', *European Papers - A Journal on Law and Integration*, 9 (2024), 1438–73 <<https://doi.org/10.15166/2499-8249/817>>
- Moore, Tyler, Richard Clayton, and Ross Anderson, 'The Economics of Online Crime', *Journal of Economic Perspectives*, 23 (2009), 3–20 <<https://doi.org/10.1257/jep.23.3.3>>
- Muhammad Randy Ammar, Richardo Nezar M, Jievello Leonardo D, and Raihana Nasution, 'Hukum Teknologi Informasi Tentang Penipuan Transaksi Jual Beli Online', *JURNAL SOSIO-KOMUNIKA*, 2 (2023), 244–60 <<https://doi.org/10.57036/jsk.v2i1.39>>
- Pamuji, Reza Aditya, 'Perlindungan Hukum Bagi Nasabah Dan Tanggung Jawab Bank Dalam Kasus Card Skimming', *Jurnal Lex Renaissance*, 3 (2018), 32
 <<https://doi.org/10.20885/JLR.vol3.iss1.art12>>
- Pansariadi, Rafi Septia Budianto, and Noenik Soekorini, 'Tindak Pidana Cyber Crime Dan Penegakan Hukumnya', *Binamulia Hukum*, 12 (2023), 287–98 <<https://doi.org/10.37893/jbh.v12i2.605>>
- Pratama, Oktari Anggi Setya, 'Pertanggungjawaban Pidana Pelaku Tindak Pidana Pencurian Data Elektrnoik Ditinjau Berdasarkan Undang-Undang ITE', *Jurnal Sosial Humaniora Sigli (JSH)*, 8 (2025), 261 <<https://doi.org/https://doi.org/10.61104/alz.v3i4.2022>>
- Primanta, Asa Intan, 'Pertanggungjawaban Pidana Pada Penyalahgunaan Data Pribadi', *Jurist-Diction*, 3 (2020), 14 <<https://doi.org/10.20473/jd.v3i4.20214>>
- Robinson, P. H., 'Does Criminal Law Deter? A Behavioural Science Investigation', *Oxford Journal of Legal Studies*, 24 (2004), 173–205 <<https://doi.org/10.1093/ojls/24.2.173>>
- Ryberg, Jesper, 'Sentencing Offenders the Right Way: On the Importance of Relating Penal Theory and Penal Practice', *Criminal Law Forum*, 36 (2025), 191–204 <<https://doi.org/10.1007/s10609-025-09507-4>>
- Santoso, Irfan, Alvi Syahrin, Mahmud Mulyadi, and Agusmidah Agusmidah, 'Kebijakan Hukum Pidana Terhadap Perbuatan Melawan Hukum Dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal - Pasal Tertentu UU ITE', *Locus Journal of Academic Literature Review*, 3 (2024), 329–35 <<https://doi.org/10.56128/ljoalr.v3i4.312>>
- Saputra, Aditya Rahmad, I Ketut Seregig, and Yulia Hesti, 'Judges' Considerations In Making Decisions On Actors Who Distribute/ Transmission Of Information/ Documents Violated Electronics Decency (Decision Study Number: 471/Pid.Sus/2022/PN Tjk)', *Jurnal Gagasan Hukum*, 4 (2023), 129–35 <<https://doi.org/10.31849/jgh.v4i2.12930>>
- Sarkki, P.A.H., M.S. van 't Hoff-de Goede, M.A.G. van Leuken, S.G.A. van de Weijer, and E.R. Leukfeldt, 'Fear of Cybercrime Victimisation: Examining the Relationship between Fear and Victimisation', *Journal of Criminal Justice*, 101 (2025), 102531
 <<https://doi.org/10.1016/j.jcrimjus.2025.102531>>
- Shafa Salsabila, and Sidi Ahyar Wiraguna, 'Pertanggungjawaban Hukum Atas Pelanggaran Data Pribadi Dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia', *Konsesnsus :*

Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi, 2 (2025), 145–50
 <<https://doi.org/10.62383/konsensus.v2i2.736>>

Simonato, Michele, 'Confiscation and Fundamental Rights across Criminal and Non-Criminal Domains', *ERA Forum*, 18 (2017), 365–79 <<https://doi.org/10.1007/s12027-017-0485-0>>

Smith, Russell, Peter Grabosky, and Gregor Urbas, 'Cyber Criminals on Trial', *Criminal Justice Matters*, 58 (2004), 22–23 <<https://doi.org/10.1080/09627250408553240>>

Sofyan, Ade, 'Penerapan Asas Proporsionalitas Dalam Penjatuhan Pidana Terhadap Pelaku Tindak Pidana', *Hukum Responsif*, 15 (2024), 290
 <<https://doi.org/https://doi.org/10.33603/responsif.v15i2.9486>>

Sulisrudatin, Nunuk, 'ANALISA KASUS CYBERCRIME BIDANG PERBANKAN BERUPA MODUS PENCURIAN DATA KARTU KREDIT', *JURNAL ILMIAH HUKUM DIRGANTARA*, 9 (2014), 26–39 <<https://doi.org/10.35968/jh.v9i1.296>>

SyuiB, M., and Maisarah Maisarah, 'Tindak Pidana Pencurian Jaringan Wifi Menurut Pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik', *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, 6 (2021), 51
 <<https://doi.org/10.22373/justisia.v6i1.10611>>

Tanjung, Bitus, and Marjan Miharja, 'Penerapan Sanksi Pidana Bagi Pelaku Tindak Pidana Peretasan (Studi Kasus Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN Ckr)', *Iblam Law Review*, 4 (2024), 100–110 <<https://doi.org/10.52249/ilr.v4i4.471>>

Tax Crimes and Enforcement in the European Union, *Tax Crimes and Enforcement in the European Union*, 2023 <<https://doi.org/10.1093/oso/9780192862341.001.0001>>

Unzur Jefri Tambunan, Puguh Aji Hari Setiawan, and Dewi Iryani, 'Penegakan Hukum Tindak Pidana Carding Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Pembangunan Hukum Tindak Pidana Siber (Cybernetics)', *Jurnal Gagasan Hukum*, 6 (2024), 140–53 <<https://doi.org/10.31849/jgh.v6i02.21830>>

Victoria, Agatha Olivia, 'OJK: Keamanan Data Dalam Transaksi Keuangan Digital Jadi Tantangan', *Antara News*, 2023

Wendi Darman Laia, Martono Anggustin, and Lesson Sihotang, 'Application of Criminal Law in Online Gambling Case', *International Journal of Law, Crime and Justice*, 2 (2025), 108–21
 <<https://doi.org/10.62951/ijlcj.v2i1.440>>

Yolanda Sari KS, Madiasa Ablisar, Mahmud Mulyadi, and Jelly Leviza, 'Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik', *Locus: Jurnal Konsep Ilmu Hukum*, 2 (2022), 53–67 <<https://doi.org/10.56128/jkih.v2i2.22>>

Yusliwidaka, Arnanda, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana, 'A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?', *Pandecta Research Law Journal*, 19 (2024), 453–54
 <<https://doi.org/10.15294/pandecta.v19i2.13279>>