**Al-Zayn: Jurnal Ilmu Sosial & Hukum** e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 3 Nomor 4, 2025
DOI: https://doi.org/10.61104/alz.v3i4.2022

# Tindak Pidana Pencurian Data Elektronik Ditinjau Berdasarkan Undang-Undang ITE

**Albert Daniel Hamonangan Tampubolon[1], Hartanto[2], Uyan Wiryadi[3]**
Universitas Krisnadwipayana, Indonesia[1-3]
*Email Korespondensi: alberttampubolon@gmail.com*

*Article received: 04 Juli 2025, Review process: 13 Juli 2025*
*Article Accepted: 25 Agustus 2025, Article published: 11 September 2025*

***ABSTRACT***
*The advancement of information and communication technology has significantly enhanced digital transaction systems but has also created serious challenges with the rise of cybercrime, particularly electronic data theft through skimming. This study aims to analyze the evidentiary framework of electronic data theft and the criminal liability of perpetrators based on Indonesia's legal framework, particularly under Law No. 11 of 2008 on Electronic Information and Transactions and its amendments. This research employs a normative juridical approach, utilizing library research and qualitative descriptive analysis. The findings reveal that proving skimming offenses involves a combination of Article 184 of the Criminal Procedure Code and electronic evidence as stipulated in Article 5 (1) and (2) and Article 44(b) of the ITE Law, while perpetrators' criminal liability is governed by Article 30(2) in conjunction with Article 46(2) of the ITE Law and the principle of "joint participation" under Article 55 of the Criminal Code. This study highlights the importance of strengthening regulations, improving digital literacy, and enhancing cross-institutional collaboration to protect personal data and mitigate the growing threat of skimming-related cybercrime in the digital transformation era.*
***Keywords:*** *Skimming, Cybercrime, Data Protection, ITE Law, Criminal Law*

**ABSTRAK**
*Perkembangan teknologi informasi dan komunikasi mendorong peningkatan sistem transaksi digital, namun juga memunculkan tantangan serius berupa meningkatnya kejahatan siber, khususnya pencurian data elektronik melalui metode skimming. Penelitian ini bertujuan menganalisis pembuktian tindak pidana pencurian data elektronik dan pertanggungjawaban pidana pelakunya berdasarkan kerangka hukum Indonesia, khususnya mengacu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya. Penelitian menggunakan pendekatan yuridis normatif dengan teknik pengumpulan data melalui studi kepustakaan dan analisis kualitatif deskriptif. Hasil penelitian menunjukkan bahwa pembuktian tindak pidana skimming dilakukan dengan menggunakan kombinasi Pasal 184 KUHAP dan bukti elektronik sebagaimana diatur dalam Pasal 5 ayat (1) dan (2) serta Pasal 44 huruf b UU ITE, sementara pertanggungjawaban pidana pelaku diatur melalui Pasal 30 ayat (2) jo Pasal 46 ayat (2) UU ITE serta unsur "turut serta" pada Pasal 55 KUHP. Penelitian ini menegaskan pentingnya penguatan regulasi, peningkatan literasi digital, serta kolaborasi lintas lembaga guna memperkuat perlindungan data pribadi dan mencegah maraknya kejahatan skimming di era transformasi digital*
***Kata Kunci:*** *Skimming, Cybercrime, Perlindungan Data, UU ITE, Hukum Pidana*

 

## PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) telah memberikan dampak signifikan terhadap berbagai aspek kehidupan manusia, termasuk dalam sektor ekonomi, sosial, dan hukum. Pemanfaatan teknologi digital mendorong terciptanya inovasi dalam pelayanan publik dan sistem transaksi keuangan yang semakin cepat, efisien, dan praktis. Namun, kemajuan ini juga melahirkan tantangan baru berupa meningkatnya risiko kejahatan siber (*cybercrime*) yang memanfaatkan teknologi sebagai sarana melakukan tindak pidana. Menurut laporan Interpol (2024), lebih dari 70% kejahatan digital di kawasan Asia Tenggara melibatkan pencurian data elektronik dan akses ilegal terhadap sistem perbankan, menunjukkan bahwa perkembangan teknologi tidak hanya menghadirkan peluang, tetapi juga kerentanan baru bagi keamanan data dan transaksi daring.

Fenomena kejahatan siber semakin kompleks karena pelakunya dapat melakukan serangan lintas negara tanpa kehadiran fisik di lokasi kejadian. Hal ini menandai era baru kriminalitas digital di mana interaksi antara pelaku, korban, dan sistem dilakukan sepenuhnya melalui jaringan komputer. Salah satu bentuk kejahatan yang paling menonjol adalah pencurian data elektronik melalui metode skimming. Praktik ini dilakukan dengan menyalin data nasabah dari *magnetic stripe* kartu ATM atau kartu kredit, kemudian memanfaatkan informasi tersebut untuk melakukan transaksi ilegal. Laporan Europol (2023) mencatat bahwa praktik skimming global menyebabkan kerugian finansial mencapai USD 1,6 miliar per tahun, sementara kasus di Indonesia menunjukkan tren peningkatan signifikan dalam lima tahun terakhir.

Di Indonesia, pengaturan hukum terkait kejahatan siber telah diatur melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan diperbarui dengan Undang-Undang Nomor 19 Tahun 2016. Namun, modus operandi pelaku skimming berkembang lebih cepat daripada regulasi yang ada. Pelaku biasanya memasang perangkat tambahan pada mesin ATM, seperti *deep insert skimmer* dan kamera tersembunyi, untuk menyalin data kartu dan PIN nasabah. Data tersebut kemudian dikirim secara nirkabel dan digunakan untuk melakukan transaksi ilegal. Studi terbaru oleh Kaspersky Lab (2024) menunjukkan bahwa Indonesia menempati peringkat ke-4 dunia sebagai negara dengan tingkat kerentanan perbankan digital tertinggi, akibat rendahnya literasi keamanan siber di kalangan masyarakat.

Dampak kejahatan skimming tidak hanya menimbulkan kerugian finansial bagi nasabah dan perbankan, tetapi juga mengganggu stabilitas sistem keuangan nasional. Kepercayaan masyarakat terhadap transaksi elektronik menurun ketika kasus skimming semakin marak dan penegakan hukumnya dianggap kurang optimal. Selain itu, karakteristik skimming sebagai bentuk transnational organized crime menimbulkan tantangan tambahan bagi aparat penegak hukum, terutama dalam hal pembuktian digital dan kerja sama antarnegara. Oleh karena itu, diperlukan pendekatan terpadu melalui pembaruan regulasi, peningkatan teknologi keamanan, serta literasi digital masyarakat agar risiko kejahatan berbasis

 

teknologi dapat ditekan seminimal mungkin (UNODC, 2024).

Berbagai penelitian sebelumnya menyoroti pentingnya integrasi kebijakan perlindungan data pribadi, peningkatan standar keamanan transaksi, serta penegakan hukum berbasis bukti elektronik dalam menanggulangi praktik skimming. Pendekatan kolaboratif antara regulator, penyedia layanan perbankan, aparat penegak hukum, dan masyarakat menjadi kunci untuk memperkuat sistem pertahanan digital nasional. Regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia diharapkan mampu memberikan dasar hukum yang lebih kuat untuk melindungi konsumen. Temuan dari OECD (2023) juga menegaskan bahwa negara yang memiliki sistem keamanan siber terintegrasi cenderung mengalami tingkat kejahatan digital yang lebih rendah dibanding negara dengan regulasi lemah.

Penelitian ini bertujuan untuk menganalisis pembuktian tindak pidana pencurian data elektronik atau skimming dan pertanggungjawaban pidana pelakunya berdasarkan ketentuan hukum positif di Indonesia, khususnya mengacu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya. Dengan fokus ini, penelitian diharapkan dapat memberikan kontribusi terhadap pengembangan kebijakan hukum siber yang lebih adaptif, komprehensif, dan responsif terhadap perkembangan modus operandi kejahatan digital di era transformasi teknologi.

## METODE

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu metode yang menitikberatkan pada kajian terhadap norma, asas, dan ketentuan hukum positif yang berlaku dalam sistem perundang-undangan Indonesia. Pendekatan ini dipilih karena permasalahan penelitian berkaitan dengan pembuktian dan pertanggungjawaban pidana atas tindak pencurian data elektronik (*skimming*) yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya pada Undang-Undang Nomor 19 Tahun 2016. Data penelitian diperoleh melalui studi kepustakaan dengan menelaah bahan hukum primer, seperti peraturan perundang-undangan, Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), dan Undang-Undang Perlindungan Data Pribadi (UU PDP), serta bahan hukum sekunder berupa buku, jurnal ilmiah, putusan pengadilan, dan laporan internasional relevan. Seluruh data dianalisis menggunakan pendekatan kualitatif deskriptif dengan teknik penalaran deduktif, dimulai dari konsep umum mengenai kejahatan siber dan skimming, kemudian diarahkan pada penerapan hukum dan interpretasi norma pada kasus-kasus spesifik. Dengan metode ini, penelitian diharapkan mampu memberikan gambaran komprehensif mengenai penerapan aturan hukum, pembuktian tindak pidana, serta pertanggungjawaban pelaku dalam konteks kejahatan skimming, sekaligus menjadi acuan bagi penguatan kebijakan perlindungan data dan keamanan siber di Indonesia.

 

## HASIL DAN PEMBAHASAN

### *Pembuktian Terjadinya Tindak Pidana Pencurian Data Elektronik/Skimming Pada Kasus Yang Terjadi Di Mesin ATM*

Penyelesaian tindak pidana skimming pada umumnya ditempuh melalui jalur litigasi atau pengadilan. Hal ini dimaksudkan agar pelaku segera dapat dijatuhi hukuman sesuai dengan perbuatannya yang termasuk tindak pidana penipuan. Dalam hukum pidana, setiap perbuatan yang dilarang oleh aturan hukum selalu disertai dengan ancaman sanksi pidana tertentu. Dengan demikian, siapa pun yang melanggar aturan tersebut harus mempertanggungjawabkan perbuatannya melalui mekanisme peradilan pidana yang berlaku (Bambang Waluyo, 2020).

Penyelesaian perkara pidana merupakan bagian dari penegakan hukum yang berlandaskan asas, tujuan hukum, konstitusi, dan nilai moral bangsa. Dalam kasus skimming, nasabah sebagai korban harus melaporkan kejadian kepada pihak bank dan Kepolisian agar dapat diproses sesuai hukum acara pidana, sehingga pelaku dapat dimintai pertanggungjawaban dan dijatuhi pidana. Menurut Badriyah Khaleed, hukum acara pidana adalah kerangka hukum yang mengatur tata cara administrasi peradilan dalam perkara pidana sejak tahap penyelidikan awal hingga putusan akhir. Proses ini dapat berakhir dengan pembebasan tanpa syarat melalui putusan bebas, atau sebaliknya dengan penjatuhan pidana sesuai keyakinan hakim atas kejahatan yang dilakukan terdakwa (Badriyah Khaleed, 2014).

Dalam tindak pidana skimming, nasabah sebagai korban perlu melaporkan peristiwa pencurian kepada pejabat berwenang agar dapat segera ditindaklanjuti dan pelaku ditangkap. Penanganan kasus ini memerlukan proses penyelidikan dan penyidikan yang penting untuk mengungkap kebenaran, mengejar pelaku, sekaligus melindungi orang yang tidak bersalah. KUHAP sendiri telah membedakan tugas antara penyelidik dan penyidik sebagaimana diatur dalam Pasal 1 angka 4 KUHAP jo Pasal 8 UU No. 2 Tahun 2002 tentang Kepolisian RI.

Pembuktian memiliki peran penting dalam proses peradilan karena menentukan bersalah atau tidaknya terdakwa. Jika alat bukti yang sah menurut undang-undang tidak cukup membuktikan kesalahan, terdakwa dibebaskan; sebaliknya jika terbukti, terdakwa dijatuhi hukuman. Pasal 184 KUHAP mengatur alat bukti yang sah secara limitatif, yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Di luar itu, alat bukti tidak diakui dan tidak memiliki kekuatan pembuktian.

Dalam perkembangan hukum, Pasal 5 ayat (1) dan (2) serta Pasal 44 huruf b UU No. 19 Tahun 2016 tentang ITE mengakui informasi elektronik, dokumen elektronik, dan hasil cetakannya sebagai alat bukti yang sah. Hal ini memberikan kepastian hukum terhadap sistem dan transaksi elektronik, termasuk tindak pidana skimming. Dengan demikian, pembuktian tindak pidana skimming menggunakan kombinasi alat bukti Pasal 184 KUHAP serta bukti elektronik sesuai

 

UU ITE agar proses peradilan berjalan sesuai hukum acara yang berlaku di Indonesia.

***Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Elektronik/Skimming Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik***

Analisis pertanggungjawaban pidana terhadap pelaku tindak pidana pencurian data elektronik atau skimming dapat dilihat dalam Putusan No. 570/Pid.Sus/2022/PN Btm dan Putusan No. 916/Pid.Sus/2021/PN Dps. Pada kedua putusan tersebut, terdakwa terbukti dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik untuk memperoleh informasi atau dokumen elektronik, sebagaimana diatur dalam Pasal 30 ayat (2) jo Pasal 46 ayat (2) UU No. 19 Tahun 2016 tentang Perubahan UU ITE jo Pasal 55 ayat (1) ke-1 KUHP. Hal ini menunjukkan bahwa perbuatan para terdakwa memenuhi unsur tindak pidana yang diatur undang-undang.

Skimming ATM sendiri merupakan bentuk pencurian data nasabah dengan memasang alat skimmer pada slot kartu ATM untuk menyalin data pada magnetic stripe. Tindakan ini merugikan nasabah maupun pihak bank karena data nasabah yang seharusnya hanya dapat dikelola oleh pihak bank, berhasil diakses oleh pelaku dengan memanfaatkan pengetahuan teknologi. Oleh sebab itu, kejahatan skimming dikategorikan sebagai salah satu bentuk cybercrime yang kompleks karena melibatkan kemampuan teknis tinggi.

Dampak skimming ATM tidak hanya dirasakan oleh nasabah, tetapi juga menimbulkan kerugian bagi bank dan bahkan negara. Kerugian keuangan, gangguan dalam sistem pembayaran, hingga keluarnya kas negara untuk menanggulangi masalah ini menunjukkan bahwa skimming memiliki efek luas yang merugikan banyak pihak. Dengan demikian, skimming termasuk perbuatan melawan hukum berupa akses ilegal terhadap sistem elektronik yang menegaskan pentingnya penegakan hukum yang tegas terhadap pelakunya.

Pertanggungjawaban pidana atas kejahatan skimming ATM sebagaimana dalam Putusan No. 570/Pid.Sus/2022/PN Btm dengan terdakwa Claudia Cornelia Matulessy dan Putusan No. 916/Pid.Sus/2021/PN Dps dengan terdakwa Cezmi Yamac, didasarkan pada Pasal 30 ayat (2) jo Pasal 46 ayat (2) UU No. 19 Tahun 2016 tentang Perubahan UU ITE jo Pasal 55 ayat (1) ke-1 KUHP. Dalam perkara ini, unsur "setiap orang" telah terpenuhi karena para terdakwa terbukti sebagai subjek hukum yang cakap bertanggung jawab secara individual, sesuai dengan doktrin dan yurisprudensi Mahkamah Agung yang menyamakan pengertian "setiap orang" dengan "barang siapa." Fakta persidangan juga menunjukkan bahwa kedua terdakwa dewasa, sehat jasmani maupun rohani, serta dapat dimintai pertanggungjawaban hukum.

Selain itu, unsur "dengan sengaja dan tanpa hak atau melawan hukum" juga terpenuhi, mengingat para terdakwa secara sadar menggunakan perangkat skimmer untuk mengakses data elektronik nasabah tanpa kewenangan. Perbuatan tersebut tidak hanya melanggar norma hukum positif, tetapi juga bertentangan

 

dengan asas-asas perlindungan data perbankan. Dengan demikian, kedua unsur utama dalam pasal yang didakwakan dapat dibuktikan melalui keterangan saksi, barang bukti, dan pengakuan terdakwa di persidangan.

Secara keseluruhan, pertimbangan hakim dalam kedua putusan tersebut menegaskan bahwa skimming ATM merupakan bentuk cybercrime yang serius karena berdampak luas, tidak hanya merugikan nasabah, tetapi juga pihak perbankan dan negara. Oleh karena itu, penerapan ketentuan pidana dalam UU ITE jo KUHP menjadi instrumen penting dalam memastikan kepastian hukum serta efek jera bagi pelaku kejahatan siber.

Pengertian tanpa hak atau melawan hukum dalam tindak pidana siber, termasuk skimming, merupakan unsur penting yang harus dibuktikan. Menurut (Andi Hamzah, 1986) melawan hukum berarti bertentangan dengan kewajiban yang ditetapkan undang-undang, sedangkan "tanpa hak" dimaknai sebagai bertentangan dengan hukum objektif karena pelaku tidak memiliki wewenang atau otoritas yang sah dalam melakukan suatu perbuatan. Dengan demikian, setiap tindakan yang tidak didukung dasar kewenangan hukum dapat digolongkan sebagai "tanpa hak" sekaligus "melawan hukum."

Sementara itu, (Saleh, 1983) menegaskan bahwa melawan hukum diartikan sebagai "bertentangan dengan hukum" baik secara etimologis maupun substansial. Pertama, secara bahasa istilah melawan hukum memang mengandung makna pertentangan dengan hukum. Kedua, sifat melawan hukum merupakan unsur mutlak dari setiap perbuatan pidana, artinya tanpa adanya sifat melawan hukum, suatu perbuatan tidak dapat dikategorikan sebagai tindak pidana. Dengan demikian, unsur melawan hukum tidak hanya bersifat formal (bertentangan dengan peraturan perundang-undangan), tetapi juga bersifat material, yakni apabila suatu perbuatan dipandang tercela oleh rasa keadilan dalam masyarakat.

Berdasarkan pandangan tersebut, jelas bahwa unsur "tanpa hak atau melawan hukum" dalam kejahatan skimming ATM telah terpenuhi, karena pelaku secara sadar dan tanpa otorisasi yang sah mengakses serta memanfaatkan data elektronik milik nasabah. Tindakan ini tidak hanya bertentangan dengan UU ITE sebagai hukum positif, tetapi juga merugikan masyarakat dan melanggar norma keadilan yang hidup di dalam masyarakat.

Berdasarkan keterangan saksi dan barang bukti di persidangan, terbukti bahwa Terdakwa Claudia Cornelia Matulessy dalam Putusan No. 570/Pid.Sus/2022/PN Btm dan Terdakwa Cezmi Yamac dalam Putusan No. 916/Pid.Sus/2021/PN Dps dengan sadar dan tanpa paksaan melakukan tindakan memasang perangkat skimming pada mesin ATM untuk memperoleh informasi elektronik milik nasabah tanpa hak dan tanpa persetujuan pihak bank. Unsur "dengan sengaja dan tanpa hak atau melawan hukum" oleh karena itu telah terpenuhi, mengingat perbuatan tersebut bertentangan baik dengan norma hukum positif maupun kepentingan hukum perbankan.

Selanjutnya, unsur "mengakses komputer dan/atau sistem elektronik dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik" juga terbukti. Fakta hukum menunjukkan bahwa para terdakwa menggunakan

 

perangkat berupa *deep insert skimmer* dan kamera tersembunyi yang dipasang pada mesin ATM untuk menyalin data kartu nasabah dan merekam PIN. Data yang berhasil diperoleh kemudian dipindahkan menggunakan perangkat *encode card writer* ke kartu lain untuk dipakai melakukan transaksi ilegal. Perbuatan tersebut jelas memenuhi definisi sistem elektronik, informasi elektronik, dan dokumen elektronik sebagaimana diatur dalam UU ITE.

Unsur "mereka yang melakukan dan turut serta melakukan"juga terbukti, karena para terdakwa bekerja sama dengan pihak lain dalam pemasangan dan pengoperasian alat skimming. Dengan demikian, seluruh unsur dalam Pasal 30 ayat (2) jo Pasal 46 ayat (2) UU No. 19 Tahun 2016 tentang ITE jo Pasal 55 ayat (1) ke-1 KUHP terpenuhi. Atas perbuatannya, Majelis Hakim menjatuhkan pidana penjara 5 tahun dan denda Rp5.000.000.000 kepada Claudia Cornelia Matulessy, serta pidana penjara 2 tahun 6 bulan dan denda Rp300.000.000 kepada Cezmi Yamac. Putusan ini menegaskan bahwa skimming merupakan tindak pidana siber serius yang menuntut pertanggungjawaban pidana tegas untuk memberikan kepastian hukum dan efek jera.

Kejahatan skimming sebagai bentuk pencurian data elektronik merupakan ancaman serius dalam era digital. Modus operandi kejahatan ini dilakukan dengan cara memasang skimmer dan perangkat pendukung lainnya untuk memperoleh data nasabah tanpa izin, kemudian memanfaatkannya untuk melakukan transaksi ilegal. Praktik tersebut tidak hanya merugikan korban secara finansial, tetapi juga melemahkan kepercayaan publik terhadap sistem perbankan dan transaksi elektronik. Dalam perspektif hukum pidana, perbuatan skimming dapat dikualifikasikan sebagai tindak pidana pencurian, penipuan, maupun akses ilegal terhadap sistem elektronik sebagaimana diatur dalam KUHP dan UU ITE.

Penanggulangan skimming dapat ditempuh melalui dua pendekatan, yakni sarana penal dan non-penal. Sarana penal dilakukan dengan penegakan hukum pidana melalui penerapan pasal-pasal terkait, antara lain Pasal 362 KUHP tentang pencurian, Pasal 378 KUHP tentang penipuan, serta Pasal 30 dan 32 UU ITE mengenai akses ilegal dan manipulasi data elektronik. Sedangkan sarana non-penal bersifat preventif, misalnya melalui peningkatan keamanan sistem perbankan, edukasi literasi digital bagi masyarakat, serta pengawasan intensif terhadap aktivitas transaksi elektronik. Pendekatan non-penal juga mencakup kebijakan perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP), yang mempertegas kewajiban penyelenggara sistem elektronik dalam menjaga kerahasiaan data nasabah.

Meskipun regulasi telah tersedia, penegakan hukum terhadap kejahatan skimming masih menghadapi kendala, khususnya dalam hal pembuktian digital dan keberadaan pelaku lintas negara. Oleh karena itu, dibutuhkan sinergi antara aparat penegak hukum, regulator, pihak perbankan, dan masyarakat dalam upaya penanggulangan. Selain itu, regulasi perlu diperbarui secara adaptif terhadap modus kejahatan baru, serta penerapan teknologi keamanan seperti enkripsi data dan autentikasi ganda harus dijadikan standar. Dengan demikian, pertanggungjawaban pidana pelaku skimming dapat ditegakkan secara efektif,

 

sementara perlindungan hukum terhadap korban dapat lebih optimal dalam rangka menjaga stabilitas sistem perbankan dan kepercayaan publik.

Penanggulangan kejahatan skimming dapat dilakukan melalui dua jalur, yakni sarana penal dan sarana non-penal, yang pelaksanaannya melibatkan perbankan, nasabah, serta pemerintah/penegak hukum.

a. Upaya oleh pihak perbankan.

Perbankan berperan penting dalam memperkuat sistem keamanan transaksi, baik melalui pemasangan kamera pengawas, peningkatan teknologi ATM, maupun sistem deteksi transaksi mencurigakan. Selain itu, perbankan wajib menyelesaikan pengaduan nasabah dengan cepat serta melakukan edukasi agar nasabah lebih berhati-hati ketika bertransaksi, sehingga ruang gerak pelaku kejahatan dapat diminimalisir.

b. Upaya oleh nasabah.

Kesadaran nasabah merupakan faktor kunci pencegahan. Nasabah perlu berhati-hati menjaga kerahasiaan PIN, tidak membuang sembarangan struk transaksi, serta mewaspadai indikasi perangkat tambahan pada mesin ATM. Edukasi publik mengenai modus skimming juga penting agar masyarakat dapat melakukan pencegahan secara mandiri.

c. Upaya oleh pemerintah/penegak hukum.

Pemerintah melalui UU ITE dan UU Perlindungan Data Pribadi (UU PDP) menegaskan larangan akses ilegal terhadap sistem elektronik dan pencurian data pribadi. Perubahan UU ITE (UU No. 1 Tahun 2024) semakin memperkuat kerangka hukum, baik melalui pendekatan preventif (literasi digital, regulasi keamanan data, compliance monitoring) maupun represif (penyelidikan, penyidikan, penuntutan, hingga putusan pengadilan). Penegakan hukum juga ditunjang dengan kerja sama lintas lembaga, peningkatan kapasitas aparat melalui pelatihan forensik digital, serta kolaborasi internasional untuk menghadapi karakteristik transnational crime.

Kombinasi pendekatan penal dan non-penal ini mencerminkan strategi kebijakan kriminal yang komprehensif. Pendekatan penal bertujuan memberikan efek jera melalui sanksi pidana, sementara pendekatan non-penal menitikberatkan pada upaya pencegahan dengan membangun kesadaran hukum masyarakat, memperkuat infrastruktur keamanan digital, dan melibatkan semua pihak dalam perlindungan data pribadi.

Dengan adanya sinergi antara perbankan, masyarakat, dan pemerintah, diharapkan upaya penanggulangan skimming tidak hanya menekan angka kejahatan, tetapi juga memperkuat ekosistem digital yang aman, tertib, dan terpercaya. Hal ini penting demi terwujudnya transformasi digital yang selaras dengan perlindungan hak asasi manusia, kepastian hukum, serta pembangunan ekonomi berkelanjutan.

## SIMPULAN

Kesimpulan, tindak pidana pencurian data elektronik atau *skimming* merupakan bentuk kejahatan siber kompleks yang berdampak signifikan terhadap

 

keamanan transaksi perbankan dan kepercayaan publik terhadap sistem keuangan digital. Pembuktian tindak pidana ini dilakukan dengan mengacu pada Pasal 184 KUHAP serta bukti elektronik sebagaimana diatur dalam Pasal 5 ayat (1) dan (2) dan Pasal 44 huruf b Undang-Undang Nomor 19 Tahun 2016 sebagai perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pertanggungjawaban pidana pelaku skimming ditegaskan melalui Pasal 30 ayat (2) jo Pasal 46 ayat (2) UU ITE serta unsur "turut serta" sebagaimana dimaksud dalam Pasal 55 KUHP, yang memungkinkan setiap pihak yang terlibat untuk dimintai pertanggungjawaban hukum. Hasil penelitian ini menegaskan perlunya penguatan regulasi, kolaborasi antar-lembaga, dan peningkatan literasi digital masyarakat, agar perlindungan data pribadi dan keamanan transaksi elektronik dapat terjamin. Dengan adanya penegakan hukum yang efektif, diharapkan upaya pencegahan kejahatan siber, khususnya praktik skimming, dapat berjalan optimal dan memberikan kepastian hukum bagi seluruh pihak terkait.

## DAFTAR RUJUKAN

Andi Hamzah. (1986). *Kamus Hukum*. Rineka Cipta.

Badriyah Khaleed. (2014). *Panduan Hukum Acara Pidana*. Medpress Digital.

Bambang Sunggono. (2003). *Metodologi Penelitian Hukum*. Raja Grafindo Persada.

Bambang Waluyo. (2020). *Penyelesaian Perkara Pidana: Penerapan Keadilan Restoratif dan Transformatif* (Cetakan pertama). Sinar Grafika.

Enrick, M. (2019). Pembobolan ATM menggunakan teknik skimming kaitannya dengan pengajuan restitusi. *Jurist-Diction,* 2(2), 555–572. https://doi.org/10.20473/jd.v2i2.14252

Europol. (2023). *Payment card fraud report: Annual European analysis*. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu

Firdaus, R. A. (2024). Perlindungan hukum dan pencegahan kejahatan siber di era digital dalam sistem hukum di Indonesia. *STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam,* 4(1), 1–14.

Ibrahim, J. (2006). *Teori dan Metodologi Penelitian Hukum Normatif*. Bayumedia Publishing.

Interpol. (2024). *ASEAN cybercrime threat assessment report 2024*. International Criminal Police Organization. https://www.interpol.int

Kaspersky Lab. (2024). *Global ATM skimming statistics 2024*. Kaspersky Security Bulletin. https://www.kaspersky.com

Ninggeding, N. Y., Bayuaji, R., & Indriastuty, D. E. (2023). Penegakan hukum terhadap cyber crime di bidang perbankan di Indonesia. *Jurnal Ilmu Hukum Wijaya Putra, 1*(2), 215–224. https://doi.org/10.38156/jihwp.v1i2.107

OECD. (2023). *OECD digital security risk management for economic and social prosperity: Policy report*. OECD Publishing. https://doi.org/10.1787/9789264232440-en

Saleh, R. (1983). *Hukum Pidana*. Aksara Baru.

United Nations Office on Drugs and Crime. (2024). *Cybercrime and electronic evidence: Global threat assessment*. UNODC. https://www.unodc.org

Zainuddin Ali. (2009). *Metode Penelitian Hukum*. Sinar Grafika.

 