

Perlindungan Hukum Preventif Terhadap Kejahatan *Skimming* dalam Layanan Anjungan Tunai Mandiri

Andina Resty Eliza^{1*}, Rasina Padeni Nasution²

^{1,2} Program Studi Hukum, Fakultas Syari'ah dan Hukum, Universitas Islam Negeri Sumatera Utara, Sumatera Utara 20371, Indonesia

Email: ¹arestieliza@gmail.com, ²rasinasution@uinsu.ac.id

Preventive Legal Protection Against Skimming Crimes in Automated Teller Machine (ATM) Banking Services

Article info	Abstract
Received: 13 Nov 2025	The development of information technology in the banking sector has facilitated financial transactions through Automated Teller Machine (ATM) services. However, these advancements have also increased the risk of cybercrime, particularly skimming, which involves the unauthorized acquisition of customers' ATM card data for fraudulent purposes. This crime causes financial losses to customers and raises legal issues concerning consumer protection in banking services. This study aims to analyze the legal framework governing skimming crimes in Indonesia and examine banks' legal obligations in implementing preventive legal protection. The research employs an empirical juridical method with a descriptive-analytical approach using statutory analysis and interviews with banking institutions. The findings show that the legal regulation of skimming is governed by the Electronic Information and Transactions Law, the Consumer Protection Law, the Banking Law, as well as regulations issued by Bank Indonesia and the Financial Services Authority. Banks are required to implement the prudential banking principle by strengthening technological security systems, monitoring ATM operations, applying fraud detection mechanisms, and providing customer education on cybercrime risks. Despite these preventive measures, challenges remain due to the increasingly sophisticated methods used by cybercriminals and the limited public awareness of cybersecurity. Therefore, strengthening banking security, regulatory supervision, and public legal awareness is essential to prevent skimming.
Accepted: 21 Jan 2026	
Published: 07 Feb 2026	
Keywords: Preventive legal protection, Skimming, Automated teller machines, Cybercrime	

Doi: <https://doi.org/10.59011/vjlaws.5.1.2026.190-205>

* Corresponding Author

E-mail address: arestieliza@gmail.com

Copyright © 2026 The Author(s)

CC BY-NC 4.0 License

1. Pendahuluan

Perkembangan teknologi perbankan pada era digitalisasi yang semakin pesat telah membawa dampak yang luas terhadap berbagai aspek kehidupan masyarakat. Kemajuan teknologi tersebut memberikan kemudahan dalam berbagai aktivitas ekonomi, termasuk melalui kehadiran layanan Anjungan Tunai Mandiri (ATM), internet banking, dan mobile banking yang memudahkan nasabah dalam melakukan transaksi keuangan tanpa harus datang langsung ke bank. Namun, di sisi lain perkembangan tersebut juga membuka peluang munculnya berbagai bentuk kejahatan baru di bidang perbankan, yaitu *cyber crime* atau kejahatan siber.² Kejahatan siber merupakan bentuk kejahatan modern yang memanfaatkan teknologi informasi sebagai sarana maupun sasaran kejahatan. Bentuk-bentuk *cyber crime* di sektor perbankan antara lain *malware banking*, *phishing*, *pharming*, dan *skimming*.³

Perbuatan *skimming* merupakan kejahatan elektronik di sektor perbankan yang dilakukan dengan cara mencuri data nasabah melalui kartu Anjungan Tunai Mandiri. Data yang dicuri meliputi nomor kartu, nama pemegang kartu, tanggal kedaluwarsa, kode bank, serta nomor rekening yang terhubung dengan kartu tersebut.⁴ Dalam praktiknya, pelaku *skimming* umumnya memulai aksi dengan melakukan persiapan dan pengintaian.⁵ Mereka memilih lokasi sasaran, seperti mesin Anjungan Tunai Mandiri yang sepi, mesin EDC di minimarket yang kurang pengawasan, atau terminal pembayaran di lokasi yang dianggap rawan. Selanjutnya, pelaku melakukan observasi untuk mengetahui waktu operasional yang ramai, keberadaan kamera CCTV, serta pola pengawasan oleh petugas keamanan. Setelah lokasi dianggap sesuai, pelaku memasang berbagai perangkat, seperti *skimmer* (alat pembaca *magnetic stripe*), *overlay slot* kartu palsu, *keypad* palsu atau kamera mini untuk merekam PIN, serta perangkat penyimpanan data atau transmisi nirkabel (Bluetooth/GSM) untuk mengirimkan data kepada pelaku.⁶

Tahap berikutnya adalah pemasangan perangkat pada mesin sasaran. Pelaku memasang *overlay* atau *deep insert skimmer* pada slot kartu sehingga ketika korban memasukkan kartu, data magnetik pada pita kartu, seperti nomor kartu, tanggal kedaluwarsa, dan informasi lainnya, dapat terbaca dan tersimpan pada perangkat tersebut. Untuk memperoleh PIN, pelaku menempelkan *keypad* palsu yang merekam tekanan tombol atau memasang kamera kecil yang diarahkan ke *keypad* Anjungan Tunai Mandiri. Pada modus yang lebih canggih, pelaku menggunakan teknik *shimming* untuk menangkap data pada chip EMV atau memasang *malware* pada sistem Anjungan Tunai Mandiri maupun mesin EDC sehingga data dapat direkam secara digital. Setiap kali nasabah

² Dinh et al., "Determinants Affecting Digital Financial Consumer Protection: Evidence from 135 Countries."

³ Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*.

⁴ Ekawati, "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan."

⁵ Kaur et al., "ATM Card Cloning and Ethical Considerations."

⁶ Ekawati, "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan."

menggunakan mesin yang telah disusupi, perangkat *skimmer* merekam data kartu, sedangkan kamera atau *keypad* palsu merekam PIN yang dimasukkan oleh korban.⁷

Data yang berhasil dikumpulkan kemudian disimpan secara lokal pada perangkat atau dikirimkan secara nirkabel kepada pelaku yang berada di lokasi terdekat. Setelah data terkumpul, pelaku mengunduh dan menggabungkannya dengan PIN untuk membuat kartu hasil kloning atau melakukan *carding* maupun transaksi pembelian secara daring menggunakan data korban. Selanjutnya, kartu palsu tersebut digunakan untuk menarik uang tunai di mesin Anjungan Tunai Mandiri lain atau melakukan transaksi pembelian secara langsung. Dalam transaksi daring (*card-not-present transaction*), pelaku memanfaatkan nomor kartu, tanggal kedaluwarsa, dan kode CVV untuk berbelanja melalui situs *e-commerce*.⁸ Untuk memperoleh kode OTP atau notifikasi transaksi, pelaku terkadang melakukan *SIM swap* atau *phishing* guna mengambil alih nomor telepon korban sehingga proses autentikasi dua faktor dapat dilewati. Dana hasil kejahatan kemudian dipindahkan melalui rekening perantara (*money mule*) untuk menyamarkan asal-usul dana sebelum akhirnya disalurkan kepada pelaku.⁹

Kejahatan *skimming* telah terjadi di berbagai daerah di Indonesia, termasuk di Kota Medan. Salah satu kasus terjadi pada Juni–Juli 2022 di Bank Sumut yang berlokasi di Swalayan Diamond, Jalan Karya Wisata Nomor 26, Pangkalan Masyhur, Medan Johor. Dalam kasus tersebut, dua pelaku memasang alat *skimmer* pada mesin Anjungan Tunai Mandiri Bank Sumut sehingga sebanyak 83 hingga 239 nasabah menjadi korban pencurian dana melalui duplikasi data kartu *magnetic stripe*. Pelaku diduga merupakan warga negara asing dan dana hasil kejahatan dialihkan ke aset kripto. Berdasarkan hasil penyelidikan melalui rekaman CCTV, Polda Sumatera Utara berhasil mengidentifikasi pelaku, sedangkan Bank Sumut mengganti kerugian nasabah dalam waktu 1×24 jam.¹⁰ Kasus serupa kembali terjadi pada tahun 2024, ketika dana nasabah Bank Sumut sebesar Rp2,7 miliar dilaporkan hilang. Peristiwa tersebut terungkap setelah sejumlah nasabah mendatangi Kantor Bank Sumut di Jalan Imam Bonjol, Medan, untuk melaporkan hilangnya dana tabungan mereka.¹¹ Selain itu, kasus *skimming* juga terjadi di Kantor BNI Mandonga, Kota Kendari, Sulawesi Tenggara, yang mengakibatkan 98 nasabah menjadi korban pada layanan Anjungan Tunai Mandiri. Berbagai kasus tersebut menunjukkan bahwa kejahatan *skimming* masih menjadi ancaman nyata bagi keamanan sistem perbankan dan menimbulkan kerugian yang signifikan bagi nasabah.

Fenomena tersebut menunjukkan bahwa penanggulangan kejahatan *skimming* tidak cukup hanya dilakukan melalui pendekatan hukum pidana (*penal policy*), tetapi juga memerlukan kebijakan di luar hukum pidana (*non-penal policy*) yang bersifat preventif.

⁷ Ekawati.

⁸ Banirostan et al., “Analysis and Evaluation of Various Fraud Detection Methods for Electronic Payment Cards Transactions in Big Data.”

⁹ Ekawati, “Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan.”

¹⁰ Siregar, “239 Nasabah Bank Sumut Jadi Korban Skimming, Total Kerugian Rp5,5 Miliar.”

¹¹ Tribratanews.polri.go.id., “Polda Sumut Dan Koordinasi Ungkap Kasus Hilangnya Uang Nasabah Bank.”

Muladi menyatakan bahwa politik kriminal (*criminal policy*) pada hakikatnya merupakan upaya rasional masyarakat dalam menanggulangi kejahatan yang dapat ditempuh melalui jalur penal dan non-penal secara terpadu.¹² Dalam konteks *skimming*, penerapan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik maupun Kitab Undang-Undang Hukum Pidana memang penting untuk memberikan efek jera kepada pelaku. Namun, pendekatan tersebut bersifat represif karena baru diterapkan setelah kejahatan terjadi.

Oleh karena itu, kebijakan non-penal menjadi sangat relevan sebagai bentuk perlindungan hukum preventif, yaitu upaya pencegahan sebelum terjadinya kejahatan *skimming*.¹³ Kebijakan tersebut dapat diwujudkan melalui peningkatan sistem keamanan perbankan, seperti penggunaan kartu berbasis chip (*chip-based card*) dan perangkat *anti-skimming*, penguatan pengawasan internal bank berdasarkan prinsip kehati-hatian (*prudential banking principle*),¹⁴ edukasi kepada nasabah, serta penguatan regulasi oleh Otoritas Jasa Keuangan dan Bank Indonesia.¹⁵ Berdasarkan uraian tersebut, penulis tertarik untuk mengkaji perlindungan hukum preventif terhadap kejahatan *skimming* dalam layanan Anjungan Tunai Mandiri. Penelitian ini bertujuan untuk menganalisis pengaturan hukum mengenai kejahatan *skimming* dalam layanan Anjungan Tunai Mandiri di Indonesia serta menganalisis kewajiban hukum bank dalam menerapkan perlindungan preventif guna mencegah terjadinya kejahatan *skimming* pada layanan Anjungan Tunai Mandiri.

2. Konsep dan Teori

Teori merupakan suatu rumusan yang menjelaskan hubungan kausal yang logis antarvariabel dalam suatu bidang tertentu. Oleh karena itu, teori dapat dijadikan sebagai kerangka berpikir (*frame of thinking*) untuk memahami, menganalisis, dan menjelaskan berbagai permasalahan yang timbul dalam bidang tersebut.¹⁶

a. Teori Perlindungan Hukum

Teori perlindungan hukum merupakan teori utama yang digunakan dalam penelitian ini. Menurut Philipus M. Hadjon, perlindungan hukum adalah perlindungan terhadap harkat dan martabat manusia serta pengakuan atas hak asasi manusia yang dimiliki oleh setiap subjek hukum berdasarkan ketentuan hukum yang berlaku. Perlindungan hukum bertujuan untuk menjamin terpenuhinya kepastian hukum, keadilan, dan kemanfaatan hukum bagi setiap subjek hukum dalam memperoleh hak dan perlindungan atas kepentingannya.¹⁷ Perlindungan hukum preventif merupakan

¹² Muladi, *Kapita Selekta Sistem Peradilan Pidana*.

¹³ Ichsan, Herman, and Haris, "Upaya Non Penal Dalam Penanggulangan Tindak Pidana Skimming."

¹⁴ Wang et al., "Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector."

¹⁵ Alfian, "Politik Hukum Pidana Dalam Penanggulangan Kejahatan Siber Di Indonesia: Analisis Kriminologis Terhadap Efektivitas Kebijakan Penal Dan Non-Penal."

¹⁶ Wuisman, *Penelitian Ilmu-Ilmu Sosial : Jld 1 Asas-Asas*.

¹⁷ Hadjon, *Perlindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi*.

bentuk perlindungan hukum yang bertujuan mencegah terjadinya pelanggaran hukum sebelum sengketa atau kerugian terjadi. Bentuk perlindungan tersebut dapat diwujudkan melalui pengaturan standar keamanan sistem Anjungan Tunai Mandiri, edukasi kepada nasabah, serta penguatan pengawasan internal bank. Dalam penelitian ini, teori perlindungan hukum digunakan sebagai landasan untuk menganalisis efektivitas perlindungan hukum preventif yang diterapkan oleh Bank Sumut dalam mencegah terjadinya kejahatan *skimming* serta menjamin perlindungan hukum bagi nasabah sebagai pihak yang berpotensi menjadi korban kejahatan tersebut.

b. Teori Perlindungan Konsumen

Teori perlindungan konsumen berangkat dari asumsi bahwa konsumen berada pada posisi yang lebih lemah dibandingkan pelaku usaha sehingga memerlukan perlindungan hukum untuk mewujudkan keseimbangan dalam hubungan hukum antara para pihak.¹⁸ Dalam konteks penelitian ini, nasabah bank diposisikan sebagai konsumen jasa keuangan sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Sebagai pelaku usaha jasa keuangan, bank berkewajiban memberikan informasi yang benar, menjamin keamanan layanan, serta bertanggung jawab atas kerugian yang dialami nasabah sesuai dengan ketentuan peraturan perundang-undangan. Oleh karena itu, teori perlindungan konsumen digunakan sebagai landasan untuk menganalisis hak-hak nasabah sebagai korban kejahatan *skimming* serta kewajiban bank dalam memberikan perlindungan hukum preventif melalui penyelenggaraan layanan perbankan yang aman, andal, dan bertanggung jawab.

c. Teori Prinsip Kehati-hatian (*Prudential Banking Principle*)

Selain teori perlindungan hukum dan teori perlindungan konsumen, penelitian ini juga menggunakan teori prinsip kehati-hatian (*prudential banking principle*) sebagai landasan analisis. Prinsip kehati-hatian merupakan prinsip fundamental dalam penyelenggaraan kegiatan perbankan yang mengharuskan bank menjalankan usahanya secara hati-hati, cermat, aman, dan bertanggung jawab guna menjaga kepercayaan masyarakat serta stabilitas sistem perbankan. Prinsip ini menuntut bank tidak hanya berorientasi pada pelayanan transaksi, tetapi juga mampu mengidentifikasi, mengantisipasi, dan mengendalikan berbagai risiko yang dapat menimbulkan kerugian bagi nasabah, termasuk risiko kejahatan siber dalam layanan perbankan elektronik.¹⁹

Dalam sistem hukum perbankan Indonesia, prinsip kehati-hatian diwujudkan melalui kewajiban bank untuk menerapkan manajemen risiko, menjaga keamanan sistem teknologi informasi, melaksanakan pengawasan internal, serta menjamin terselenggaranya layanan perbankan yang aman dan andal. Penerapan prinsip tersebut juga mencakup kewajiban bank dalam mengidentifikasi, mencegah, dan memitigasi risiko operasional yang timbul dari penggunaan ATM, termasuk risiko

¹⁸ Shidarta, *Hukum Perlindungan Konsumen Indonesia*.

¹⁹ Damanik, "Prudential Banking Principles dalam Pemberian Kredit Kepada Nasabah."

kejahatan *skimming* yang dapat mengakibatkan kerugian bagi nasabah. Dengan demikian, prinsip kehati-hatian tidak hanya berfungsi sebagai pedoman dalam pengelolaan kegiatan perbankan, tetapi juga menjadi dasar normatif bagi bank dalam menerapkan berbagai langkah preventif untuk melindungi dana, data, dan kepentingan nasabah.²⁰

Dalam konteks penelitian ini, teori prinsip kehati-hatian digunakan untuk menganalisis kewajiban preventif bank dalam mencegah kejahatan *skimming* melalui penguatan sistem keamanan ATM, peningkatan pengawasan terhadap operasional mesin ATM, penerapan teknologi keamanan pada kartu dan sistem transaksi, serta pemberian edukasi kepada nasabah mengenai risiko kejahatan siber. Oleh karena itu, teori ini melengkapi teori perlindungan hukum dan teori perlindungan konsumen dengan menempatkan bank tidak hanya sebagai pihak yang bertanggung jawab atas kerugian setelah kejahatan terjadi, tetapi juga sebagai institusi yang berkewajiban membangun sistem perlindungan preventif melalui penerapan prinsip kehati-hatian.

3. Metode dan Bahan Hukum

Menurut Peter Mahmud Marzuki, penelitian hukum merupakan suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu-isu hukum yang dihadapi.²¹ Berdasarkan tujuan tersebut, penelitian ini menggunakan jenis penelitian yuridis empiris, yaitu penelitian hukum yang mengkaji penerapan ketentuan peraturan perundang-undangan dalam praktik melalui fakta-fakta yang terjadi di masyarakat (*law in action*). Penelitian yuridis empiris tidak hanya menelaah hukum sebagai norma tertulis (*law in books*), tetapi juga meneliti efektivitas pelaksanaan hukum dalam kehidupan masyarakat.²²

Penelitian ini bersifat deskriptif analitis, yaitu penelitian yang bertujuan menggambarkan secara sistematis, faktual, dan akurat mengenai karakteristik suatu fenomena hukum sekaligus menganalisisnya untuk memperoleh pemahaman terhadap permasalahan yang diteliti. Melalui sifat penelitian tersebut, penelitian ini bertujuan mendeskripsikan dan menganalisis bentuk perlindungan hukum preventif terhadap kejahatan *skimming* dalam layanan Anjungan Tunai Mandiri serta menilai efektivitas penerapannya di Bank Negara Indonesia (BNI) Cabang Medan.²³

Pendekatan yang digunakan adalah pendekatan yuridis empiris (*socio-legal research*), yaitu pendekatan yang memadukan kajian terhadap norma hukum dengan realitas penerapannya dalam masyarakat. Pendekatan ini digunakan untuk menganalisis kesesuaian antara ketentuan hukum yang mengatur perlindungan hukum preventif dengan implementasinya dalam praktik perbankan, khususnya dalam upaya pencegahan kejahatan *skimming*.

²⁰ Sulistyandari et al., "Implementation of Prudential Banking Principles: State Responsibility in Combating Banking Crimes in Indonesia."

²¹ Marzuki, *Penelitian Hukum*.

²² Muhammad, *Hukum Dan Penelitian Hukum*.

²³ Marzuki, *Penelitian Hukum*.

Sumber data dalam penelitian ini terdiri atas data primer dan data sekunder. Data primer diperoleh secara langsung dari lapangan melalui wawancara dengan narasumber di Bank Negara Indonesia (BNI) Cabang Medan. Sementara itu, data sekunder diperoleh melalui studi kepustakaan yang meliputi bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier yang berkaitan dengan objek penelitian.²⁴ Dengan demikian, teknik pengumpulan data yang digunakan dalam penelitian ini adalah wawancara (interview) dan studi kepustakaan (library research). Lokasi penelitian dilaksanakan di Bank Negara Indonesia (BNI) Cabang Medan.

Teknik analisis data dilakukan secara kualitatif melalui beberapa tahapan, yaitu reduksi data, penyajian data, triangulasi, dan penarikan kesimpulan. Reduksi data dilakukan dengan menyeleksi serta memfokuskan data hasil wawancara dan bahan hukum yang relevan dengan permasalahan penelitian. Selanjutnya, data disajikan secara sistematis dalam bentuk uraian deskriptif untuk memudahkan analisis terhadap hubungan antara fakta empiris dan ketentuan hukum yang berlaku. Untuk menjamin keabsahan data, dilakukan triangulasi dengan membandingkan hasil wawancara, peraturan perundang-undangan, serta pendapat para ahli. Tahap terakhir adalah penarikan kesimpulan secara induktif guna memperoleh jawaban atas rumusan masalah mengenai perlindungan hukum preventif terhadap kejahatan *skimming* dalam layanan Anjungan Tunai Mandiri.

4. Hasil dan Pembahasan

4.1 Pengaturan Hukum Kejahatan Skimming Dalam Layanan Anjungan Tunai Mandiri di Indonesia

Hukum positif merupakan keseluruhan ketentuan hukum yang mengatur kehidupan bermasyarakat, ditetapkan oleh otoritas yang berwenang, serta berlaku bagi masyarakat tertentu dalam batas wilayah dan waktu tertentu.²⁵ Dengan demikian, hukum positif adalah hukum yang berlaku dan mengikat dalam suatu negara sebagai dasar pengaturan hubungan hukum di masyarakat.

Berdasarkan hasil wawancara yang dilakukan peneliti dengan Bapak Teuku Muhammas Yovan selaku E-Channel and Digital Region 01 Section Head Bank Negara Indonesia (BNI), diketahui bahwa kasus *skimming* pada BNI pernah terjadi pada tahun 2020 melalui penyadapan pada mesin ATM. Kejahatan tersebut umumnya menasar mesin ATM dengan tingkat penggunaan sedang hingga tinggi, sehingga lokasi yang menjadi target pelaku umumnya berada di pusat perbelanjaan maupun kawasan permukiman. Di BNI sendiri, kasus *skimming* terjadi pada dua titik lokasi. Modus operandi yang digunakan pelaku adalah memasang perangkat *skimming* yang menyerupai *card reader* ATM sehingga data kartu nasabah dapat direkam tanpa disadari.

Lebih lanjut, Bapak Teuku Muhammas Yovan menjelaskan bahwa indikasi terjadinya *skimming* biasanya diketahui setelah adanya pengaduan dari nasabah yang merasa tidak melakukan transaksi, tetapi menemukan mutasi transaksi yang tidak dikenali

²⁴ Hadi, *Metodologi Research Jilid 1*.

²⁵ Lutskyi and Havrylyshyn, "Positive Law as a Manifestation of the Rational Correlation of the Will of the State and Its Citizens: Political and Legal Aspect."

pada rekeningnya. Setiap pengaduan tersebut diterima dan ditindaklanjuti melalui proses investigasi untuk mengidentifikasi penyebab terjadinya anomali transaksi. Apabila hasil investigasi menunjukkan adanya indikasi *skimming*, BNI melakukan penanganan sesuai prosedur yang berlaku, dimulai dari penerimaan laporan nasabah hingga penyelesaian terhadap kasus yang terjadi.

Dalam upaya menanggulangi kejahatan *skimming*, diperlukan adanya landasan hukum yang memberikan kepastian hukum terhadap perbuatan tersebut. Salah satu regulasi yang mengatur mengenai tindak pidana *skimming* adalah Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, khususnya ketentuan dalam Pasal 30, Pasal 32, dan Pasal 35, yang mengatur mengenai akses ilegal terhadap sistem elektronik, perbuatan memindahkan atau mengambil informasi elektronik secara melawan hukum, serta manipulasi informasi atau dokumen elektronik. Adapun ketentuan Pasal 30 menyatakan sebagai berikut:

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

Kemudian dalam undang-undang yang sama diatur dalam Pasal 32 yang berbunyi:

- 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
- 2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
- 3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal lain yang menjelaskan tentang kejahatan *skimming* ada dalam Pasal 35 yang berbunyi:

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

Penerapan hukum pidana pencurian elektronik dengan metode atau perbuatan skimming sendiri diatur dalam Undang-undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana dalam pasal 492 tentang pencurian yang berbunyi:

“Setiap Orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata bohong, menggerakkan orang supaya menyerahkan suatu Barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V”.

Aturan yang memberikan perlindungan hukum kepada nasabah dalam kejahatan skimming yang berisi hak dan kewajiban konsumen dalam kejahatan skimming ada pada Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen pasal 4 dan pasal 5. Pasal 4 tentang hak konsumen berbunyi:

Hak konsumen adalah:

- a. hak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa;
- b. hak untuk memilih barang dan/atau jasa serta mendapatkan barang dan/atau jasa tersebut sesuai dengan nilai tukar dan kondisi serta jaminan yang dijanjikan;
- c. hak atas informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa;
- d. hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan;
- e. hak untuk mendapatkan advokasi, perlindungan, dan upaya penyelesaian sengketa perlindungan konsumen secara patut;
- f. hak untuk mendapat pembinaan dan pendidikan konsumen;
- g. hak untuk diperlakukan atau dilayani secara benar dan jujur serta tidak diskriminatif;
- h. hak untuk mendapatkan kompensasi, ganti rugi dan/atau penggantian, apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya;
- i. hak-hak yang diatur dalam ketentuan peraturan perundang-undangan lainnya.

Selain itu terdapat pula kewajiban konsumen yang diatur dalam Pasal 5 tentang kewajiban konsumen berbunyi:

Kewajiban konsumen adalah:

- a. membaca atau mengikuti petunjuk informasi dan prosedur pemakaian atau pemanfaatan barang dan/atau jasa, demi keamanan dan keselamatan;
- b. beritikad baik dalam melakukan transaksi pembelian barang dan/atau jasa;
- c. membayar sesuai dengan nilai tukar yang disepakati;
- d. mengikuti upaya penyelesaian hukum sengketa perlindungan konsumen secara patut.

Perlindungan hukum terhadap nasabah merupakan kewajiban yang melekat pada bank sebagai pelaku usaha jasa keuangan diatur dalam UU No. 10 Tahun 1998 tentang Perbankan pasal 29 ayat (2) dan (3), juga pasal 40. Pasal 29 ayat (2) yang berbunyi:

“Bank wajib memelihara tingkat kesehatan bank sesuai dengan ketentuan kecukupan modal, kualitas aset, kualitas manajemen, likuiditas, rentabilitas, solvabilitas, dan aspek lain yang berhubungan dengan usaha bank, dan wajib melakukan kegiatan usaha sesuai dengan prinsip kehati-hatian.”

Dan Pasal 29 ayat (3) yang berbunyi:

“Dalam memberikan kredit atau pembiayaan berdasarkan Prinsip Syariah dan melakukan kegiatan usaha lainnya, bank wajib menempuh cara-cara yang tidak merugikan bank dan kepentingan nasabah yang mempercayakan dananya kepada bank.”

Selain itu juga terdapat dalam Pasal 40 yang berbunyi :

- 1) Bank Wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44, dan Pasal 44A.
- 2) Ketentuan sebagaimana dimaksud dalam ayat (1) berlaku pula bagi Pihak Terafiliasi.”

Perlindungan yang diberikan bank juga tertuang dalam pasal 10 Peraturan Bank Indonesia nomor 2 Tahun 2024 Tentang Keamanan Sistem Informasi Dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang Dan Pasar Valuta Asing, Serta Pihak Lain Yang Diatur dan Diawasi Bank Indonesia, yang mewajibkan penyelenggara sistem pembayaran menerapkan standar keamanan tertentu., yang mewajibkan penyelenggara sistem pembayaran menerapkan standar keamanan tertentu. Pasal 10 yang berbunyi:

- 1) Kebijakan, standar, dan prosedur KKS sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf b mencakup aspek manusia, proses, dan teknologi yang paling sedikit terdiri atas:
 - a. pengamanan data, sistem aplikasi, dan infrastruktur teknologi informasi;
 - b. pengamanan pihak ketiga; dan
 - c. perlindungan konsumen dan manajemen fraud.
- 2) Penyelenggara melakukan evaluasi secara berkala terhadap kebijakan, standar, dan prosedur KKS sebagaimana dimaksud pada ayat (1) untuk memastikan kecukupan dan efektivitas kebijakan, standar, dan prosedur KKS sesuai perkembangan terkini.
- 3) Ketentuan lebih lanjut mengenai kebijakan, standar, dan prosedur KKS sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

Kewajiban lembaga jasa keuangan untuk menjamin keamanan sistem dan memberikan perlindungan kepada konsumen diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Ketentuan tersebut tercantum dalam Pasal 29 yang menyatakan bahwa

“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.” Ketentuan tersebut menegaskan bahwa bank sebagai pelaku usaha jasa keuangan memiliki tanggung jawab hukum untuk memberikan perlindungan kepada nasabah, termasuk melalui penyelenggaraan sistem layanan yang aman dan andal.

Berdasarkan ketentuan tersebut, peneliti mengajukan pertanyaan kepada pihak Bank Negara Indonesia (BNI) Cabang Medan mengenai pemahaman dan penerapan regulasi yang mengatur pencegahan kejahatan *skimming* di Indonesia. Berdasarkan hasil wawancara, pihak BNI menyatakan bahwa bank telah memahami dan melaksanakan berbagai ketentuan yang ditetapkan oleh regulator, baik Bank Indonesia maupun Otoritas Jasa Keuangan. Implementasi tersebut dilakukan melalui langkah-langkah preventif, seperti edukasi kepada nasabah mengenai keamanan transaksi elektronik, penerapan standar keamanan mesin ATM sesuai dengan ketentuan regulator, serta migrasi kartu berbasis *magnetic stripe* menjadi kartu berbasis *chip* guna meminimalkan risiko terjadinya kejahatan *skimming*.

Selain mematuhi ketentuan peraturan perundang-undangan, Bank BNI juga menerapkan berbagai kebijakan internal sebagai bentuk implementasi prinsip kehati-hatian (*prudential banking principle*) dalam mencegah terjadinya kejahatan *skimming*. Kebijakan-kebijakan tersebut meliputi sebagai berikut:

- 1) Secara sistem, yaitu dengan mengubah fitur magnetic strip menjadi chip.
- 2) Melakukan edukasi
- 3) Melakukan patrol petugas (ditujukan untuk mengecek ATM itu sendiri).

Pihak Bank Negara Indonesia (BNI) Cabang Medan menyatakan bahwa dalam penerapan upaya pencegahan kejahatan *skimming* tidak ditemukan kendala yang bersifat signifikan. Hal tersebut karena bank secara berkelanjutan menyesuaikan diri dengan perkembangan teknologi dan berbagai modus kejahatan siber melalui peningkatan sistem keamanan, penguatan sumber daya manusia, penyediaan saluran pengaduan nasabah, serta pengembangan sistem deteksi dini terhadap transaksi yang mencurigakan. Dengan demikian, berbagai perubahan yang dilakukan bukan dipandang sebagai kendala, melainkan sebagai bentuk adaptasi yang diperlukan agar bank mampu menghadapi perkembangan kejahatan berbasis teknologi secara lebih efektif.

Apabila kejahatan *skimming* tetap terjadi meskipun berbagai upaya preventif telah diterapkan, Bank BNI memberikan pertanggungjawaban kepada nasabah sesuai dengan ketentuan yang berlaku. Berdasarkan hasil wawancara, bentuk pertanggungjawaban tersebut berupa penggantian kerugian (*ganti rugi*) secara penuh sepanjang hasil investigasi membuktikan bahwa kerugian timbul akibat kelemahan sistem atau kelalaian dari pihak bank, bukan karena kelalaian nasabah. Selain itu, dalam menangani kasus *skimming*, BNI senantiasa berkoordinasi dengan pihak-pihak terkait, khususnya aparat kepolisian, melalui mekanisme pelaporan dan pemenuhan persyaratan administrasi yang diperlukan guna mendukung proses penyelidikan dan penegakan hukum terhadap pelaku kejahatan.

4.2 Bentuk Kewajiban Hukum Bank Dalam Menerapkan Perlindungan Preventif Guna Mencegah Terjadinya Skimming Pada Layanan Anjungan Tunai Mandiri

Kewajiban hukum merupakan keharusan yang dibebankan oleh norma hukum kepada setiap subjek hukum, baik orang maupun badan hukum, untuk melakukan atau tidak melakukan suatu perbuatan tertentu.²⁶ Pelanggaran terhadap kewajiban tersebut menimbulkan konsekuensi yuridis berupa sanksi sesuai dengan ketentuan peraturan perundang-undangan. Dalam konteks perbankan, kewajiban hukum bank didasarkan pada prinsip kehati-hatian (*prudential banking principle*), yang mengharuskan bank menjalankan kegiatan usahanya secara hati-hati, aman, dan bertanggung jawab guna menjaga stabilitas sistem perbankan serta melindungi dana dan kepentingan nasabah.²⁷

Untuk menjawab rumusan masalah kedua, peneliti melakukan wawancara dengan Bapak Teuku Muhammas Yovan selaku E-Channel and Digital Region 01 Section Head Bank Negara Indonesia (BNI) Cabang Medan mengenai bentuk kewajiban hukum bank dalam menerapkan perlindungan hukum preventif guna mencegah terjadinya kejahatan *skimming* pada layanan ATM. Berdasarkan hasil wawancara, BNI telah menerapkan berbagai langkah preventif sebagai bentuk pelaksanaan kewajiban hukumnya dalam melindungi nasabah dari risiko kejahatan *skimming*, yaitu sebagai berikut:

- 1) Pengamanan fisik, yaitu melakukan penambahan pemasangan alat anti-skimming ke semua perangkat Anjungan Tunai Mandiri.
- 2) Monitoring, Monitoring bank adalah proses pemantauan, pengawasan, dan evaluasi rutin yang dilakukan pihak bank. Pada bank BNI monitoring secara rutin dilakukan oleh beberapa layer baik dari pegawai sendiri atau pihak vendor yang bekerja sama dengan ATM BNI.
- 3) Migrasi ATM, Yaitu pergantian kartu atau perpindahan sistem rekening sebagai bentuk pencegahan terhadap kejahatan *skimming*.
- 4) Melakukan transaksi melalui magnetik
- 5) Prospin, Yaitu meriset nomor PIN dalam jangka waktu tertentu, hal ini dilakukan karena banyaknya nasabah yang nyaman dengan PIN lamanya sehingga Bank memaksa untuk mengganti PIN nasabah melalui layar device ATM dengan tujuan mencegah terjadinya kejahatan *skimming*.
- 6) Penggantian beberapa mesin ATM yang absolet diganti dengan mesin baru.

Langkah-langkah tersebut ditujukan sebagai langkah preventif dalam mencegah terjadinya kejahatan *skimming* dalam layanan Anjungan Tunai Mandiri. Selain itu terdapat juga standar operasional bank BNI yang bertujuan untuk mencegah terjadinya kejahatan *skimming*, yaitu:

- 1) Daily monitoring yaitu pemantauan rutin di beberapa titik yang menjadi target *skimming*.
- 2) Pemasangan perangkat tambahan seperti hidden kamera
- 3) Pengawasan CCTV
- 4) Pengecekan device oleh petugas kebersihan atau security

²⁶ Berteau, "What Is a Legal Obligation?"

²⁷ Plato-Shinar, "Banking Regulation in Israel: Balancing Systemic Stability and Consumer Protection."

Dalam pencegahan *skimming* bank juga bertanggungjawab dalam menyediakan teknologi keamanan, bentuk tanggungjawab bank dalam penyediaan teknologi keamanan berupa.

- 1) Mandotoring kartu chip yang sudah diintegrasikan oleh bank BNI dan sudah di implementasikan.
- 2) Enskripsi data security yang sudah ditingkatkan.
- 3) Penyediaan Frospin
- 4) Pengupdatean Anti-*Skimming*

Selain memperkuat aspek keamanan sistem, Bank Negara Indonesia (BNI) juga melaksanakan kewajiban memberikan edukasi dan sosialisasi kepada nasabah sebagai bagian dari upaya perlindungan hukum preventif. Berdasarkan hasil wawancara, setiap petugas *frontliner* diwajibkan memberikan edukasi kepada nasabah mengenai pentingnya menjaga keamanan transaksi serta meningkatkan kewaspadaan terhadap berbagai modus penipuan di sektor perbankan. Edukasi tersebut juga dilakukan melalui media digital dan elektronik, seperti penyampaian informasi pada layar mesin ATM, publikasi melalui media sosial resmi BNI, serta pemasangan stiker dan imbauan mengenai kejahatan elektronik di area ATM. Upaya tersebut bertujuan meningkatkan literasi dan kesadaran nasabah agar terhindar dari risiko kejahatan *skimming*.

Di samping itu, BNI secara rutin melakukan evaluasi melalui Satuan Pengawas Internal sebagai bentuk pengawasan preventif terhadap penerapan sistem keamanan perbankan. Pengawasan tersebut meliputi pemeriksaan terhadap operasional mesin ATM, termasuk efektivitas pemasangan perangkat *anti-skimming* dan sarana pengamanan lainnya. Meskipun berbagai langkah preventif telah diterapkan, pihak BNI mengakui bahwa risiko terjadinya kejahatan *skimming* tidak dapat dihilangkan sepenuhnya seiring dengan berkembangnya modus kejahatan siber. Oleh karena itu, apabila kejahatan *skimming* tetap terjadi, BNI akan melakukan investigasi terhadap setiap laporan nasabah untuk menentukan penyebab terjadinya kerugian. Apabila hasil investigasi membuktikan bahwa kerugian tersebut disebabkan oleh kelemahan sistem atau kelalaian dari pihak bank dan bukan akibat kelalaian nasabah, maka BNI memberikan pertanggungjawaban berupa penggantian kerugian (*ganti rugi*) kepada nasabah sesuai dengan ketentuan yang berlaku.

5. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan mengenai perlindungan hukum preventif terhadap kejahatan *skimming* dalam layanan Anjungan Tunai Mandiri, dapat disimpulkan bahwa pengaturan hukum terhadap kejahatan *skimming* di Indonesia pada dasarnya telah diakomodasi dalam berbagai peraturan perundang-undangan yang bersifat komprehensif, baik dalam ranah hukum pidana, hukum perbankan, maupun perlindungan konsumen. Ketentuan tersebut tercermin dalam Undang-Undang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, Undang-Undang Perlindungan Konsumen, Undang-Undang Perbankan, serta regulasi Bank Indonesia dan Otoritas Jasa Keuangan. Pengaturan tersebut menunjukkan bahwa secara normatif negara telah

menyediakan landasan hukum yang memadai untuk menanggulangi kejahatan skimming melalui pendekatan preventif maupun represif.

Kewajiban hukum bank dalam menerapkan perlindungan preventif merupakan perwujudan prinsip kehati-hatian (*prudential banking principle*) yang mengharuskan bank menjamin keamanan sistem dan perlindungan dana nasabah. Dalam praktiknya, Bank Negara Indonesia telah melaksanakan berbagai upaya preventif melalui peningkatan sistem keamanan teknologi, seperti migrasi kartu berbasis chip dan penggunaan perangkat anti-skimming, pengawasan operasional ATM secara berkala, penerapan sistem deteksi fraud, serta pemberian edukasi kepada nasabah. Langkah-langkah tersebut menunjukkan adanya kesesuaian antara kewajiban normatif dan implementasi di lapangan.

Efektivitas perlindungan hukum preventif terhadap kejahatan skimming pada dasarnya telah menunjukkan hasil yang cukup baik, khususnya dalam menurunkan risiko kejahatan melalui penguatan sistem keamanan dan pengawasan internal bank. Namun demikian, efektivitas tersebut masih menghadapi berbagai tantangan, antara lain perkembangan modus kejahatan yang semakin canggih, keterbatasan pengawasan di lapangan, serta rendahnya tingkat kesadaran dan kewaspadaan nasabah. Oleh karena itu, diperlukan sinergi yang berkelanjutan antara bank, otoritas pengawas, dan masyarakat dalam meningkatkan sistem keamanan, pengawasan, serta literasi hukum dan digital guna meminimalkan terjadinya kejahatan skimming di masa mendatang.

Dengan demikian, perlindungan hukum preventif terhadap kejahatan skimming tidak hanya bergantung pada keberadaan regulasi, tetapi juga pada efektivitas implementasi, pengawasan yang berkesinambungan, serta partisipasi aktif seluruh pihak terkait dalam menciptakan sistem perbankan yang aman dan terpercaya. Hasil penelitian ini memberikan kontribusi bagi pengembangan kajian hukum perbankan, khususnya mengenai pentingnya pendekatan non-penal melalui perlindungan hukum preventif dalam menanggulangi kejahatan skimming. Penelitian ini memiliki keterbatasan karena hanya berfokus pada penerapan perlindungan hukum preventif terhadap kejahatan skimming pada Bank Negara Indonesia (BNI) Cabang Medan, sehingga hasil penelitian belum dapat menggambarkan secara menyeluruh penerapan kebijakan yang dilakukan oleh seluruh lembaga perbankan di Indonesia. Oleh karena itu, penelitian selanjutnya disarankan untuk melakukan kajian yang lebih luas dengan melibatkan beberapa bank, membandingkan efektivitas sistem perlindungan keamanan antarbank, serta mengkaji perkembangan bentuk-bentuk kejahatan siber terbaru di sektor perbankan seiring dengan perkembangan teknologi informasi.

Ucapan Terima Kasih

Penulis menyampaikan terima kasih kepada Universitas Islam Negeri Sumatera Utara atas dukungan akademik selama pelaksanaan penelitian ini. Penghargaan yang sebesar-besarnya disampaikan kepada Ibu Rasina Padeni Nasution selaku dosen pembimbing atas bimbingan, arahan, kritik, dan saran yang konstruktif selama proses penyusunan penelitian. Penulis juga mengucapkan terima kasih kepada Bank Negara Indonesia (BNI)

Cabang Medan, khususnya Bapak Teuku Muhammas Yovan, atas kesediaannya menjadi narasumber dan memberikan informasi yang diperlukan dalam penelitian ini. Ucapan terima kasih turut disampaikan kepada keluarga dan rekan-rekan yang telah memberikan doa, dukungan, serta motivasi selama proses penyelesaian penelitian.

Konflik Kepentingan

Penulis menyatakan bahwa tidak terdapat benturan kepentingan, baik yang bersifat finansial, pribadi, maupun profesional yang dapat memengaruhi objektivitas, proses penelitian, analisis data, maupun penyusunan artikel ini.

Kontribusi Penulis

Penulis memberikan kontribusi besar terhadap konsepsi dan desain penelitian. Penulis bertanggung jawab dalam proses pengumpulan dan analisis data, interpretasi data, serta penyusunan dan pembahasan hasil penelitian. Para penulis telah membaca, menelaah, dan menyetujui naskah akhir untuk dipublikasikan.

Referensi

- Alfan, Mohammad. "Politik Hukum Pidana Dalam Penanggulangan Kejahatan Siber di Indonesia: Analisis Kriminologis Terhadap Efektivitas Kebijakan Penal dan Non-Penal." *Jaksa : Jurnal Kajian Ilmu Hukum dan Politik* 3, no. 4 (October 10, 2025): 80–92. <https://doi.org/10.51903/wx2hk609>.
- Arief, Barda Nawawi. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*. Jakarta : PT Raja Grafindo Persada, 2006.
- Banirostan, Hamid, Touraj Banirostan, Mir Mohsen Pedram, and Amir Masoud Rahmani. "Analysis and Evaluation of Various Fraud Detection Methods for Electronic Payment Cards Transactions in Big Data." *Journal of Signal Processing Systems* 96, no. 12 (December 18, 2024): 849–70. <https://doi.org/10.1007/s11265-025-01947-w>.
- Bertea, Stefano. "What Is a Legal Obligation?," 27–57. Springer Nature (Netherlands), 2024. https://doi.org/10.1007/978-3-031-54067-7_3.
- Damanik, Debora. "Prudential Banking Principles dalam Pemberian Kredit Kepada Nasabah." *Notarius* 12, no. 2 (2019): 718–30. <https://doi.org/10.14710/nts.v12i2.29011>.
- Dinh, Van, Dao-Van Le, Duy Duong, and Dung Pham. "Determinants Affecting Digital Financial Consumer Protection: Evidence from 135 Countries." *The Journal of Economic Asymmetries* 27 (June 2023): e00301. <https://doi.org/10.1016/j.jeca.2023.e00301>.
- Ekawati, Dian. "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan." *Unes Law Review* 1, no. 2 (2018). <http://garuda.ristekbrin.go.id/documents/detail/895120>.
- Hadi, Sutrisno. *Metodologi Research Jilid 1*. Yogyakarta: Andi Offset, 1993.
- Hadjon, Philipus M. *Perlindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi*. Jakarta: Bina Ilmu, 2007.

- Ichsan, La Ode Muhammad, Herman, and Oheo Kaimuddin Haris. "Upaya Non Penal Dalam Penanggulangan Tindak Pidana Skimming." *Halu Oleo Legal Research* 6, no. 1 (2024). <https://doi.org/https://doi.org/10.33772/holresch.v6i1.815>.
- Kaur, Paramjit, Kewal Krishan, Suresh K. Sharma, and Tanuj Kanchan. "ATM Card Cloning and Ethical Considerations." *Science and Engineering Ethics* 25, no. 5 (October 1, 2019): 1311–20. <https://doi.org/10.1007/s11948-018-0049-x>.
- Lutskyi, Roman, and Petro Havrylyshyn. "Positive Law as a Manifestation of the Rational Correlation of the Will of the State and Its Citizens: Political and Legal Aspect." *Naukovo-Informacijnij Visnik İvano-Frankivs'kogo Universitetu Prava İmeni Korolâ Danila Galits'kogo*, no. 14(26) (2022): 39–45. <https://doi.org/10.33098/2078-6670.2022.14.26.39-45>.
- Marzuki, Peter. *Penelitian Hukum*. 4th ed. Jakarta: Kencana, 2014.
- Muhammad, Abdul Kadir. *Hukum Dan Penelitian Hukum*. Bandung: PT.Citra AdityaBakti, 2004.
- Muladi, H. *Kapita Selektta Sistem Peradilan Pidana*. Semarang: Badan penerbit Universitas Diponegoro, 1995.
- Plato-Shinar, Ruth. "Banking Regulation in Israel: Balancing Systemic Stability and Consumer Protection," 27–48. Palgrave Macmillan, Cham, 2021. https://doi.org/10.1007/978-3-030-56247-2_2.
- Shidarta. *Hukum Perlindungan Konsumen Indonesia*. Jakarta: PT. Gramedia Widiasarana, 2006.
- Siregar, Wahyudi Aulia. "239 Nasabah Bank Sumut Jadi Korban Skimming, Total Kerugian Rp5,5 Miliar," 2022. <https://www.idxchannel.com/playlists/239-nasabah-bank-sumut-jjadi-korban-skimming-total-kerugian-rp55-miliar>.
- Sulistiyandari, Sulistiyandari, Ulil Afwa, Putri Ayu Sutrisno, and Rohaida Nordin. "Implementation of Prudential Banking Principles: State Responsibility in Combating Banking Crimes in Indonesia." *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, November 28, 2024, 341–59. <https://doi.org/10.24090/volksgeist.v7i2.12132>.
- Tribatanews.polri.go.id. "Polda Sumut Dan Koordinasi Ungkap Kasus Hilangnya Uang Nasabah Bank," 2022. <https://tribatanews.polri.go.id/blog/hukum-4/polda-sumut-dan-koordinasi-ungkap-kasus-hilangnya-uang-nasabah-bank-48959>.
- Wang, Shuang, Muhammad Asif, Muhammad Farrukh Shahzad, and Muhammad Ashfaq. "Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector." *Computers & Security* 147 (December 2024): 104051. <https://doi.org/10.1016/j.cose.2024.104051>.
- Wuisman, J.J.J.M. *Penelitian Ilmu-Ilmu Sosial : Jld 1 Asas-Asas*. Cet 1. Vol. 1. Jakarta: Fakultas Ekonomi Universitas Indonesia, 1996.