Jurnal Hukum Lex Generalis. Vol.7. No.7 (2026)
Tema/Edisi : Hukum Pidana (Bulan Ketujuh)
https://lexgeneralis.co.id/

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA *SKIMMING* DI INDONESIA

LAW ENFORCEMENT AGAINST PERPETRATORS OF SKIMMING CRIMES IN INDONESIA

I Gusti Bagus Agung Kusuma Atmaja

Institut Teknologi dan Bisnis STIKOM Bali, Program Studi Sistem Informasi

Korespondensi Penulis: agungkusumaatmaja85@gmail.com

Citation Structure Recommendation :

Atmaja, I Gusti Bagus Agung Kusuma. *Penegakan Hukum terhadap Pelaku Tindak Pidana Skimming di Indonesia*. Jurnal Hukum Lex Generalis. Vol.7. No.7 (2026).

ABSTRAK

Teknologi pada masa ini bagai pisau bermata dua, di satu sisi dapat memberi kemudahan, di sisi yang lain dapat menjadi masalah. Kasus Tindak *skimming* merupakan kasus yang bukan lagi tergolong kejahatan baru namun sangat menghawatirkan untuk nasabah perbankan. Kejahatan *skimming* bisa dilakukan berbagai macam yaitu pemasangan perangkat skimmer serta pengambilan data nasabah. Kejahatan *skimming* diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, namun masalah pada aturan Undang-Undang ini adalah terdapat kekosongan secara spesifik dan ketidakpastian penerapan pasal karena *skimming* tidak diatur secara eksplisit.

Kata Kunci: Hukum Pidana, Kejahatan Dunia Maya, Skimming

ABSTRACT

Technology today is like a double-edged sword; on the one hand, it provides convenience, while on the other, it can cause problems. The act of skimming is no longer considered a new crime, yet it remains highly alarming for banking customers. Skimming crimes can be committed in various ways, namely through the installation of skimmer devices and the extraction of customer data. The crime of skimming is regulated under Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions. However, the issue with this regulation is the existence of a specific legal vacuum and uncertainty in the application of its articles, as skimming is not explicitly addressed.

Keywords: Criminal Law, Cyber Crime, Skimming

A. PENDAHULUAN

Era globalisasi seperti saat ini, segala macam kegiatan atau pekerjaan dituntut untuk dilakukan secara cepat. Kecepatan dalam mengakses sesuatu sangat diperlukan karena setiap orang menginginkan kemudahan-kemudahan dalam melakukan pekerjaan atau aktivitasnya walau dalam saat yang bersamaan. Dalam kegiatan perbankan juga sangat membutuhkan akses yang cepat guna menunjang kegiatan transaksi menjadi lebih mudah, terutama para nasabah dapat melakukan transasksi perbankan dari mana saja tanpa harus menunggu antrian lagi di bank. Kemudahan-kemudahan ini sudah bisa didapatkan oleh para pengguna jasa perbankan melalui mobile banking, internet banking atau bertransaksi melaui gerai-gerai ATM yang sudah menjamur diseluruh wilayah Indonesia.

Namun dibalik kemudahan akses perbankan ini, ada masalah juga yang dapat dihadapi oleh para nasabah bank. Kejahatan dunia maya (*cyber crime*) menjadi suatu masalah yang harus ditemukan jalan keluarnya. Perlindungan data pribadi awalnya adalah bagian integral dan hak konstitusional warga negara dalam penggunaan teknologi digital.[1] *Cyber crime* secara umum didefinisikan sebagai kejahatan di bidang komputer melalui penggunaan sistem secara ilegal *Cyber crime* merupakan kejahatan berbasis teknologi informasi tanpa batas wilayah yang merekayasa sistem atau data berkeamanan tinggi.[2] Ruang lingkup kejahatan ini mencakup pembajakan, pencurian, penipuan, pencemaran nama baik dan pemalsuan.[3] Tindak kejahatan ini merambat pada berbagai macam tindakan ilegal yang dilaksanakan melalui sistem di ruang digital melalui jaringan, seperti pembobolan data, penipuan *online*, pembajakan, serta penyebaran virus berbahaya.

---

[1] Anas Heryanto, Iksan dan Nurul Izzati Mardiyah, *Perlindungan Hukum terhadap Data Nasabah dalam Transaksi Financial Technology di Indonesia,* Jurnal Lex Generalis, Vol.7, No.4 (April 2026).

[2] Antoni, *Kejahatan Dunia Maya (Cybercrime) dalam Simak Online,* Jurnal Nuraini : Jurnal Kajian Syari'ah dan Masyarakat, Vol.17, No.2 (Desember 2017), p.261-274.

[3] Surya Ari Wibowo, Alvi Syahrin, Mahmud Mulyadi dan Sunarmi, *Pertanggungjawaban Pidana bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan dengan Metode Skimming Ditinjau Menurut Undang-Undang Informasi dan Transaksi Elektronik,* Jurnal Kajian Hukum : Iuris Studia, Vol.2, No.2 (Juni 2021), p.138.

Dampaknya sangat merugikan semua nasabah namun tidak berhenti hanya disitu tetapi juga merugikan bagi skala nasional[4], sehingga diperlukan regulasi untuk mencegah kejahatan tersebut. Perkembangan kejahatan digital seperti *phishing* dan *skimming* menuntut bank untuk menerapkan sistem pengamanan yang lebih canggih, termasuk penggunaan *biometric authentication* guna meminimalisasi risiko kebocoran data.[5]

Merujuk pada laporan TB News mengenai kasus yang terjadi di Bali, aparat dari Direktorat Reserse Kriminal Umum Polda Bali telah melakukan OTT kasus kejahatan *skimming*, yakni Dogan Kimis (45) dan Noldy Wullur (50). Keduanya diringkus petugas saat sedang berupaya mencabut perangkat *deep skimming* pada sebuah mesin ATM di kawasan Kuta Utara, Kabupaten Badung. Dogan Kimis, seorang WNA asal Turki, merupakan residivis kasus serupa yang bebas pada April 2020, sedangkan Noldy Wullur bertugas mengantarnya ke lokasi kejadian. Para pelaku tercatat telah melakukan aksinya sebanyak empat kali.[6]

Kejahatan Skimming diatur dalam Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di pasal 30 ayat (1) yang berbunyi : ” Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun”.[7] Ancaman hukuman dari pelanggaran atas pasal tersebut tertuang dalam peraturan di pasal 46 ayat (1) ini disebutkan:

> ”Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah)”.

Namun terhadap pada kasus ini pasal yang lebih mengkhusus diatur dalam pasal 30 ayat (2), dimana bunyinya :

---

[4] Aulia Mawaddah Matondang dan Andryan, *Kebijakan Hukum Pidana terhadap Kejahatan Cyber Studi Perbandingan Antara Indonesia dan Thailand dalam Perspektif Hukum Internasional,* Jurnal Lex Generalis, Vol. 6, No.1 (Januari 2025).

[5] Yutika Ariani Tungga Dewi, Andika Wijaya, Nuraliah Ali dan Ivans Januardy, *Perlindungan Data Pribadi Nasabah dalam Perspektif Hukum Perbankan Syariah di Palangka Raya,* Jurnal Lex Generalis, Vol.7, No.2 (Februari 2026).

[6] TB News, *Polda Bali Tangkap 2 Pelaku Residivis Kasus Skimming,* diakses dari https://tribratanews.polri.go.id/blog/hukum-4/polda-bali-tangkap-2-pelaku-residivis-kasus-skimming-15625, diakses pada 02 Oktober 2026, jam 08.55 Wita.

[7] Indonesia, *Undang-Undang Republik Indonesia tentang Informasi dan Transaksi Elektronik*, UU No.11 Tahun 2008, LN Tahun 2008 No.58, TLN No.4843.

> "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".

Sedangkan pada ketentuan pidana pada pasal 46 ayat (2) berbunyi:

> "Setiap Orang yang memenuhi unsur sebagaimana yang dimaksud dalam pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah)".

Kehadiran peraturan termuat dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sudah seharusnya dapat menjamin keamanan bagi nasabah pengguna jasa perbankan, namun masih ada saja jalan untuk pelaku kriminal ini untuk menjalankan tindakan kriminalnya tersebut. Selain adanya peraturan perundang-undangan ini, sikap tegas dan tindakan aparat penegak hukum sebagai garda terdepan dalam memerangi tindak pidana dunia maya ini, apalagi saat ini ada tindak pidana perbankan yang disebut dengan *Skimming*. *Skimming* merupakan jenis penipuan yang termasuk ke dalam metode *phising*. Metode *phishing* merupakan kejahatan siber yang bertujuan mencuri data pribadi target, termasuk informasi perbankan seperti nomor rekening dan PIN. Sementara itu, *skimming* sebagai bentuk *cyber theft* atau *identity theft* adalah pencurian data kartu debit atau kredit dengan melakukan penyalinan atau pemindahan informasi kedalam penyimpanan di mesin ATM secara melawan hukum untuk menguasai rekening nasabah.

Di sisi lain, *skimming* dapat diartikan sebagai kasus peretasan data nasabah perbankan mulai dari kartu debit sampai kartu kredit dengan memanfaatkan perangkat tersembunyi di mesin ATM atau EDC. Perangkat yang lazim disebut *skimmer* ini bekerja dengan cara menyalin informasi rahasia dari pita magnetik kartu korban, yang nantinya disalahgunakan untuk keperluan transaksi yang tidak sah.

Adapun di dalam kasus kejahatan *skimming*, terdapat celah atau kesenjangan hukum yang nyata antara hukum yang tertulis (*de jure*) dengan kenyataan yang mana terjadi di lapangan (*de facto*). Secara *de jure*, Indonesia sendiri sudah memiliki instrumen hukum yang kuat untuk menjerat pelaku.

Namun secara *de facto*, penegakan hukum dan perlindungan korban masih menghadapi banyak hambatan teknis. Secara *De Jure*, pelaku *skimming* bisa mendapat sanksi peraturan UU ITE mengenai pengaksesan sistem elektronik secara melawan hukum dan pasal yang berkenaan dengan UU KUHP. Namun menurut *De Facto*, Menangkap tersangka utama sangat sulit. Kejahatan ini kerap dilakukan oleh jaringan internasional *organized crime* yang beroperasi lintas negara. Pelaku yang tertangkap di lapangan biasanya hanyalah "kurir" yang bertugas memasang alat atau menarik uang, sementara aktor intelektualnya (otak kejahatan) sulit dilacak karena bersembunyi di balik enkripsi internet.

Penelitian yang dilakukan oleh Putri Sari Nilam Cayo membahas mengenai sanksi pidana terhadapan pelaku kejahatan skimming yang terjadi di dunia perbankan.[8] Penelitian lain yang dilakukan oleh Adib Yanuar Gunawan dan H. Sutrisno meneitik beratkan pembahasan pada pertanggungjawaban pidana warga negara asing sebagai pelaku tindak pidana *skimming* berdasarkan Undang-Undang ITE.[9] Berikutnya penelitian yang dilakukan oleh Surya Ari Wibowo, dkk., mengkaji mengenai pertanggung jawaban pidana oleh pelaku tindak pidana perbankan dengan cara skimming.[10] Adapun penelitian yang dibahas oleh Andi Tanwir Mappanyukki menganalisa mengenai suatu tindak pidana skimming lewat sudut pandang kepolisian Daerah Sulawesi Selatan.[11] Keempat penelitian tersebut lebih berfokus pada aspek normatif perlindungan korban, pembuktian elektronik, aspek empiris dan pengaturan tindak pidana siber secara umum. Sementara itu, penelitian ini memiliki kebaruan karena tidak hanya menganalisa terkait Undang-Undang Informasi dan Transaksi Elektronik, namun membahas kejahatan *skimming* melalui hukum yang dimuat pada UU KUHP.

---

[8] Putri Sari Nilam Cayo, *Sanksi Pidana Terhadap Pelaku Kejahatan Skimming Pada Perbankan*, Jurnal Justici, Vol.18, No.1 (Januari 2025), p.21.

[9] Adib Yanuar Gunawan dan H. Sutrisno, *Penegakan Hukum Bagi Pelaku Tindak Pidana Skimming Oleh Warga Negara Asing Berdasarkan UU ITE,* Jurnal Kajian Ilmu Hukum dan Politik, Vol.1, No.4 (Oktober 2023), p.130.

[10] Surya Ari Wibowo, Alvi Syahrin, Mahmud Mulyadi dan Sunarmi, *Pertanggungjawaban Pidana bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan dengan Metode Skimming Ditinjau Menurut Undang-Undang Informasi dan Transaksi Elektronik*, p.138.

[11] Andi Tanwir Mappanyukki, *Analisa Tindak Pidana Skimming oleh Kepolisian Daerah Sulawesi Selatan,* IJI Publication, Vol.3, No.1 (November 2022), p.72.

Menurut keterangan pada uraian diatas tersebut, dapat dirumusankah permasalahannya yaitu Bagaimana mekanisme penindakan bagi kejahatan *skimming* di wilayah yurisdiksi Indonesia?.

Penelitian ini memiliki tujuan untuk memberi gambaran kepada masyarakat guna mengetahui mengenai penegakan hukum di Indonesia terhadap kasus *skimming* berdasarkan pada Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP).[12]

B. PEMBAHASAN

1. Pengaturan Hukum Tindak Pidana Skimming di Indonesia

Perihal hukum, sesuatu perlakuan dapat petakan sebagai kejahatan apabila dirumuskan secara tegas dalam suatu delik. Kata lain dari tindak pidana berakar pada bahasa Belanda *strafbaar feit*, yaitu *strafbaar* ("dapat dipidana") dan *feit* ("perbuatan" atau "peristiwa"). Sementara itu, para ahli hukum memberikan definisi tindak pidana sebagai berikut:

a. Hazewinkel Suringa, *strafbaar feit* diartikan tingkah seseorang pada saat tertentu diabaikan dalam sosial di masyarakat dan seharusnya tidak ada hukum mengatur dan tidak memaksa.
b. Berdasarkan pernyataan Pompe, *strafbaar feit* diartikan sebagai langkah-langkah nyata dalam peraturan sehingga bisa dikenakan sanksi pidana.
c. Menurut Simons, *strafbaar feit* dapat diartikan perlakuan bertentangan dengan hukum yang secara sengaja dalam subjek hukum yang bisa bertanggung jawab, serta diancam dengan sanksi pidana berdasarkan undang-undang.[13]

[12] Indonesia, *Undang-Undang Republik Indonesia tentang Kitab Undang-Undang Hukum Pidana*, UU No.1 Tahun 2023, LN Tahun 2023 No.1, TLN No.6842.
[13] P.A.F Lamintang, *Dasar-dasar Hukum Pidana Indonesia,* Citra Aditya Bakti, Bandung, 2007.

Pengakuan secara normatif terhadap regulasi pelindungan data pribadi di Indonesia berawal dari disahkannya UU ITE. Sebagai landasan utama jaminan hak privasi tersebut, Pasal 26 ayat (1) UU ITE eksplisit mengamanatkan identitas seseorang secara pribadi di ranah elektronik harus mengantongi izin dari pemilik data terkait, terkecuali terdapat ketentuan khusus dari undang-undang lain yang mengaturnya.[14]

Tindak pidana ruang siber menjadi sesuatu tindakan dapat menimbulkan keresahan dikalangan pengguna internet, karena kejahatan di dunia maya ini tidak mengenal batas wilayah. Di dalam bukunya, Widodo menyebutkan yaitu "*cybercrime* yang berarti seorang secara berkelompok, individu atau perusahaan yang menggunakan barang elektronik atau digital bertujuan untuk melakukan aksi kejahatan dengan mencari target atau sasaran".

Adapun berbagai macam jenis kasus kriminal yang biasa terjadi pada ruang digital yaitu:

a. *Illegal acces/unauthorized access to computer system and service*

   Perilaku hal tersebut adalah perilaku penyusupan kedalam ruang digital dengan cara illegal.

b. *Illegal contents*

   Merupakan tindak pidana siber berupa penyebaran informasi fiktif dan melanggar hukum ke ruang siber. Konten yang diunggah biasanya bertentangan dengan nilai kesusilaan serta berpotensi mengganggu stabilitas dan ketertiban masyarakat umum.

c. *Data forgery*

   Tindakan manipulasi atau pemalsuan data pada dokumen elektronik krusial. Praktik ini sering ditemukan pada aktivitas niaga elektronik (*e-commerce*), di mana pelaku membuat situs web tiruan guna mengelabui korban agar secara sukarela menyerahkan informasi sensitif seperti rincian kartu kredit dan identitas pribadi.

[14] Muhammad Wildan Ichsandi dan Wilma Silalahi, *Urgensi Perlindungan Data Pribadi dalam Sektor Perbankan di Era Digital,* Jurnal Lex Generalis, Vol.5, No.12 (Desember 2024).

d. *Cyber espionage*

Aktivitas spionase digital yang memanfaatkan koneksi internet untuk menerobos sistem target. Tujuan utama kejahatan ini adalah melakukan pengintaian sekaligus mencuri data rahasia atau informasi berharga secara melawan hukum.

e. *Cyber sabotage and extortion* (sabotase dan kekerasan ruang digital)

Kasus tersebut bertumpu pada upaya perusakan, penghancuran, atau pengacauan suatu program, data, hingga infrastruktur jaringan. Pelaku biasanya menginjeksi perangkat lunak berbahaya seperti virus atau *logic bomb* yang memicu kelumpuhan sistem, sehingga kendali atas sistem tersebut sepenuhnya jatuh ke tangan pelaku.

f. *Offense against intellectual property* (pelanggaran HKI)

Tindakan pidana yang secara khusus menargetkan hak cipta dan kekayaan intelektual (HKI) di ekosistem digital. Contoh nyata dari pelanggaran ini meliputi praktik plagiasi, penggandaan, atau kloning tampilan suatu antarmuka situs web secara sepihak tanpa lisensi dari penciptanya.

g. *Infringements of privacy*

Kejahatan siber yang menyasar data-data privat pada suatu basis data komputer terpusat. Eksploitasi dan kebocoran informasi pribadi ini sangat merugikan korban baik secara materiil maupun imateriil mengingat pelaku dapat menyalahgunakan data krusial seperti nomor PIN ATM serta rekam jejak sensitif lainnya.[15]

Budi Suhariyanto mengemukakan bahwa *skimming* merupakan ruang digital (*cybercrime*). Kejahatan ini beroperasi dengan mengeksploitasi teknologi jaringan komputer, baik pada skala lokal hingga global. Modus utamanya berupa penduplikasian data serat magenetis pada kartu ATM dan melawan hukum, dengan tujuan akhir untuk mengambil alih dana di dalam rekening nasabah. Pita magnetik (*magnetic stripe*) merupakan plat bergaris hitam di belakang kartu ATM berfungsi menyimpan data penting seperti Identitas kartu, masa tenggang, dll.

[15] Widodo, *Aspek Hukum Kejahatan Mayantara,* Yogyakarta, Aswindo, 2011.

Keterampilan teknologis yang tinggi dari pelaku kejahatan siber ini menjadi tantangan tersendiri dalam melacak dan memberantasnya secara tuntas.[16] Kerugian yang terjadi akibat tindak pidana skimming ini juga memiliki nominal yang tidak sedikit, tidak hanya puluhan juta bahkan menyentuh angka miliyaran rupiah. Kejadian-kejadian seperti inilah yang perlu diperhatikan oleh pemerintah maupun pihak bank dengan meningkatkan *cyber security* di dalam kegiatan perbankan di masa kini, hal ini menjadi sangat penting uintuk dapat memberikan rasa aman kepada masyarakat pengguna jasa perbankan.

Perbuatan (*Actus Reus*) yang dilakukan dalam kejahatan *skimming* ATM yaitu "mengakses", niat pelaku (*Mens Rea*) dalam kejahatan *skimming* ATM yaitu "dengan sengaja", objek dari kejahatan *skimming* ialah "Mendapatkan Informasi dan/atau Sistem Digital" dan bertujuan dari kejahatan *skimming* ATM untuk "Mendapatkan sebuah Informasi Digital dan/atau Dokumen Artiannya Digital". Bahwa tersangka bisa dikenakan kurungan menurut aturan pada pasal 30 ayat (2) UU ITE jika pelaku telah mendapatkan akses ke sebuah perangkat elektronik dan/atau ruang digital dengan tujuan mendapatkan suatu data atau informasi dan sebuah sesuatu yang bersifat elektronik serta korban dari kasus ini adalah pemilik Informasi Elektronik tersebut.[17]

Tindak pidana *skimming* ini diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, hal terkait dengan perilaku *skimming* dapat dilihat dari bunyi Pasal 30 ayat (1) yang menyebutkan: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun". Ancaman hukuman dari pelanggaran atas pasal tersebut dapat diperhatikan pada bunyi pasal 46 ayat (1), dimana pada pasal ini disebutkan : " Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah)".

---

[16] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya,* Rajawali Press, Jakarta, 2016.

[17] Dian Ekawati, *Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan,* Unes Law Review, Vol.1, No.2 (Desember 2018).

Sedangkan ada juga aturan yang masih berkaitan dengan tindak pidana skimming yakni pada pasal 30 ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, di mana dalam pasal ini berbunyi :

> "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".[18]

Atas perbuatan tindak pidana *skimming* tersebut, pelaku yang terbukti bersalah dapat dijatuhi hukuman. Pelanggaran pada ketentuan diatas dikenakan hukuman sebagaimana diatur pada Pasal 46 ayat (2) UU ITE, yang berbunyi:

> "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah.)

Pentingnya kehadiran UU Nomor 1 Tahun 2023 bagi hukum peradilan setidaknya dititikberatkan melalui dua dimensi pokok. Pertama, UU KUHP ini menawarkan landasan yuridis dan lebih mendetail serta utuh, yang secara langsung membantu kelancaran aparat berwenang dalam memproses serta menghukum pelaku kejahatan secara terukur. Kedua, regulasi ini dirancang agar lebih responsif dalam menjawab perubahan zaman. Fleksibilitas tersebut tampak dari diakuinya ragam kejahatan baru di sektor teknologi informasi, sekaligus penerapan sanksi pidana yang lebih proporsional guna mewujudkan rasa aman di tengah masyarakat.[19]

Dalam KUHP baru, pasal-pasal yang berkaitan dengan kasus *skimming* ini telah tertuang pada pasal 332 dan 334 KUHP yang berbunyi:

Pasal 332 KUHP :

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem elektronik milik Orang lain dengan cara apa pun, dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V;

---

[18] Indonesia, *Undang-Undang Republik Indonesia tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, UU No.1 Tahun 2024, LN Tahun 2024 No.1, TLN No.6905.

[19] M. Irwan P. Ratu Bangsawan, *Menakar Arti Penting Undang-Undang Nomor 1 Tahun 2023 tentang KUHP*, diakses dari https://kumparan.com/irwan-pachrozi/menakar-arti-penting-undang-undang-nomor1-tahun-2023-tentang-kuhp-1zxgXlDQ1TC/full, diakses pada 10 September 2026, jam 21.42 Wita.

(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, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori V.
(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, dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau pidana denda paling banyak kategori VI.

Pasal 334 KUHP:

Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau pidana denda paling banyak kategori VI, Setiap Orang yang:

(a) tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari bank sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya;
(b) tanpa hak menggunakan data atau mengakses dengan cara apa pun kartu kredit atau kartu pembayaran milik orang lain dalam transaksi elektronik untuk memperoleh keuntungan;

Berdasarkan rumusan Pasal 332 dan Pasal 334 dalam KUHP baru, terminologi subjek hukum yang digunakan adalah "Setiap orang". Penggunaan frasa ini bermakna luas, karena bukan mengarah pada seseorang atau subjek perorangan, namun melingkupi skala perusahaan. Sebagaimana diuraikan oleh Pujiyono (2015), korporasi didefinisikan sebagai suatu himpunan kekayaan maupun orang yang terstruktur, tanpa memandang status entitas tersebut sebagai badan hukum ataupun non-badan hukum. Kehadiran instrumen pidana terbaru ini pada akhirnya memunculkan ekspektasi positif dari masyarakat luas, khususnya dalam menjamin terciptanya ekosistem transaksi perbankan yang lebih aman, nyaman dan terlindungi. Dengan adanya ancaman atas suatu tindak pidana skimming ini juga diharapkan memberikan efek jera yang signifikan terhadap pelaku-pelaku dikemudian hari.

2. Penegakan Hukum terhadap Pelaku Tindak Pidana *Skimming* di Indonesia

Pada pandangan Lawrence M. Friedman, sebuah yang dibentuk oleh tiga pilar utama yang saling terintegrasi, yakni struktur, substansi dan kultur (budaya)

hukum. Elemen ini pada dasarnya merujuk pada kelembagaan pemangku kebijakan atau pihak terkait. Dalam ranah ini, pilar ini direpresentasikan dalam struktur peradilan pidana (*criminal justice system*), mensinergikan berbagai kewenangan mulai dari proses penyidikan, penuntutan, peradilan, hingga eksekusi sanksi. Wujud nyata dari struktur ini adalah institusi Kepolisian, Kejaksaan, serta Pengadilan. Di sisi lain, substansi hukum memuat keseluruhan norma, asas dan regulasi yang saat ini telah diberlakukan. Dalam Negara Indonesia, pijakan utama hukum pidana materil berpusat dengan UU KUHP, kemudian prosedur formilnya berpedoman pada UU KUHAP. Terakhir, tradisi hukum didefinisikan sebagai seperangkat nilai, tingkah laku, serta kebiasaan yang memengaruhi jalannya praktik penegakan hukum di lapangan. Budaya hukum ini melekat ditengah kebiasaan masyarakat dan pihak hukum. Pada dasarnya, budaya hukum suatu bangsa mencerminkan tingkat kemajuan dan kondisi sosial masyarakat yang bersangkutan.[20]

Pada tindak pidana dunia maya (*cyber crime*), *skimming* menjadi model kejahatan yang marak terjadi saat ini. Dimana kejahatan dunia maya (*cyber crime*) dalam hal ini *skimming*, menjadi salah satu kejahatan di dunia maya yang meresahkan bagi para nasabah perbankan. Tindak pidana skimming ini kerap disalahgunakan untuk mendapatkan keuntungan diri sendiri dalam transaksi perbankan secara melawan hukum. Pelaku kejahatan *skimming* melakukan pencurian data, duplikasi pada peralatan transaksi dan melakukan manipulasi terhadap sistem perbankan. Perkembangan teknologi perbankan ini diibaratkan seperti pisau bermata dua, di mana dengan adanya teknologi di dunia perbankan nasabah akan dimudahkan dalam menjalankan aktifitas transaksinya namun disisi yang berbeda adanya kejahatan di dunia perbankan ini membuat resah nasabah pengguna jasa perbankan yang banyak aktifitas perbankannya dilakukan melalui mesin ATM, internet banking maupun layanan perbankan lainnya.

Praktik *skimming* merupakan tindak pidana yang beroperasi melalui ekstraksi atau pencurian informasi elektronik pada kartu ATM. Aksi ini umumnya dijalankan dengan memanfaatkan sebuah perangkat pembaca khusus yang lazim disebut *skimmer*. Alat ini bekerja dengan menyalin data dari pita magnetik

[20] Satjipto Rahardjo, *Pembangunan Hukum dalam Perspektif Politik Hukum Nasional,* CV. Rajawali, Jakarta, 1986, p.27.

(*magnetic stripe*) yang menyimpan informasi pribadi nasabah untuk proses identifikasi transaksi perbankan. Pembobolan perbankan melalui teknik *skimming* ini secara umum terbagi ke dalam tiga tahapan: pertama, perolehan data nasabah; kedua, pemalsuan kartu elektronik dan ketiga, pelaksanaan transaksi menggunakan kartu palsu tersebut. Ada beberapa faktor yang menjadi penyebab kejahatan yang semakin meningkat pada praktik di ruang digital menggunakan kejahatan *skimming* yaitu:[21]

a. Faktor Perbankan

Dalam penyelenggaraan layanan perbankan elektronik (*e-banking*) seperti fasilitas ATM, pihak perbankan masih kurang mengoptimalkan pengendalian serta pengamanan fisik terhadap perangkat dan ruang operasional dari risiko pencurian, perusakan, maupun tindakan ilegal oleh pihak yang tidak berwenang. Selain itu, minimnya pemantauan secara rutin oleh pihak bank berpotensi mengurangi jaminan keamanan dan kenyamanan bagi nasabah.

b. Faktor Hukum

1) Ketentuan yang berlaku

Aturan mengenai perilaku peretasan uang nasabah dengan cara *skimming* secara khusus telah diatur oleh UU ITE. Tetapi, penerapan sanksi oleh apparat hukum dinilai belum maksimal karena dalam beberapa kasus masih menggunakan ketentuan KUHP. Hal ini berdampak pada rendahnya sanksi yang dijatuhkan.

2) Penegakan Hukum

Aparat hukum kerap menjadi kendala utama pada penanganan kejahatan berbasis sistem elektronik. Keterbatasan pemahaman teknis di bidang teknologi informasi menyebabkan penegak hukum mengalami kesulitan dalam proses pengumpulan alat bukti digital, terutama pada kejahatan dengan modus operandi yang kompleks. Hambatan tersebut diperparah oleh keterbatasan sarana di daerah, di mana belum seluruh institusi kepolisian ditunjang oleh akses jaringan internet yang memadai.

[21] Dikdik M. Arief Mansur, *Cyber Law Aspek Hukum Teknologi Informasi,* Refika Aditama, Bandung, 2005, p.89.

c. Faktor Teknologi

Faktor teknologi turut mendorong meningkatnya kejahatan berbasis sistem elektronik. Kelemahan ini antara lain bersumber dari keterbatasan sistem pengamanan pada mesin ATM.

Terdapat persoalan hukum dalam penerapan UU ITE terhadap tindak pidana *skimming*, tetapi perlu dibedakan antara "UU ITE tidak mengatur istilah skimming secara khusus" dan "perbuatan *skimming* sama sekali tidak dapat dipidana." UU ITE yang berlaku saat ini adalah UU No. 11 Tahun 2008 sebagaimana telah diubah terakhir dengan UU No. 1 Tahun 2024. UU No. 1 Tahun 2024 didalam penerapan UU ITE sebelumnya terdapat beberapa persoalan, termasuk perbedaan pemahaman terhadap sejumlah ketentuan yang dapat menimbulkan penerapan kepada subjek yang seharusnya tidak menjadi sasaran. Salah satu hal yang menjadi masalah adalah bahwa UU ITE tidak menggunakan istilah "*skimming*" sebagai suatu tindak pidana tersendiri. Padahal, modus skimming memiliki karakteristik khusus, yaitu memperoleh atau menyalin data pada alat pembayaran secara tidak sah melalui sarana teknologi. Akibatnya, aparat penegak hukum perlu mengkualifikasikan perbuatan konkret pelaku ke dalam ketentuan pidana yang tersedia, berdasarkan bagaimana pelaku memperoleh, mengubah, memindahkan, menggunakan, atau memanfaatkan data elektronik tersebut. Sehingga dapat mengakibatkan persoalan untuk memberikan aturan yang paling sesuai untuk diterapkan, khususnya apabila suatu kasus *skimming* terdiri atas beberapa rangkaian perbuatan.

Dalam tindak pidana tertentu, perbuatan pelaku skimming dapat berkaitan dengan aturan dan tata cara tentang akses dalam perangkat digital dan/atau sistem elektronik secara tanpa hak. Namun, tidak setiap *skimming* otomatis dapat dikategorikan hanya berdasarkan Pasal 30. Hal tersebut bergantung pada fakta perkara, khususnya apakah pelaku melakukan akses terhadap komputer atau sistem elektronik secara melawan hukum dan bagaimana cara memperoleh data korban. Maka, persoalan hukumnya bukan semata-mata "ada atau tidak ada pasal", tetapi apakah unsur pasal tersebut dapat dibuktikan berdasarkan modus *skimming* yang dilakukan.

C. PENUTUP

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah sebagai alat pengatur warga negara Indonesia dalam melakukan apapun kegiatan berkaitan di ruang digital. Saat ini pada dalam peraturan tersebut sudah mengatur larangan yang tidak diperkenankan untuk dipraktikkan. Skimming merupakan suatu tindakan melawan hukum dan sebagai perbuatan yang berakibat dijatuhinya sanski pidana, baik pidana kurungan maupun denda. Peranan dalam aturan tersebut diharapkan bisa memberikan kenyamanan untuk masyarakat dalam hal ini masyarakat adalah pengguna layanan perbankan dalam melakukan segala jenis transaksi perbankannya.



DAFTAR PUSTAKA

Buku

Lamintang, P.A.F. 2007. *Dasar-dasar Hukum Pidana Indonesia*. (Bandung: Citra Aditya Bakti).

Mansur, Dikdik M. Arief. 2005. *Cyber Law Aspek Hukum Teknologi Informasi*. (Bandung: Refika Aditama).

Rahardjo, Satjipto. 1986. *Pembangunan Hukum dalam Perspektif Politik Hukum Nasional*. (Jakarta: CV. Rajawali).

Suhariyanto, Budi. 2016. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. (Jakarta: Rajawali Press).

Widodo. 2011. *Aspek Hukum Kejahatan Mayantara*. (Yogyakarta: Aswindo).

Publikasi

Antoni. *Kejahatan Dunia Maya (Cybercrime) dalam Simak Online*. Jurnal Nurani: Jurnal Kajian Syari'ah dan Masyarakat. Vol.17. No.2 (Desember 2017), p.261–274.

Cayo, Putri Sari Nilam. *Sanksi Pidana Terhadap Pelaku Kejahatan Skimming Pada Perbankan*. Jurnal Justici. Vol.18. No.1 (Januari 2025), p.21.

Dewi, Yutika Ariani Tungga, Andika Wijaya, Nuraliah Ali dan Ivans Januardy. *Perlindungan Data Pribadi Nasabah dalam Perspektif Hukum Perbankan Syariah di Palangka Raya*. Jurnal Lex Generalis. Vol.7. No.2 (Februari 2026).

Ekawati, Dian. *Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan*. Unes Law Review. Vol.1. No.2 (Desember 2018).

Gunawan, Adib Yanuar dan H. Sutrisno. *Penegakan Hukum bagi Pelaku Tindak Pidana Skimming oleh Warga Negara Asing Berdasarkan UU ITE. Jurnal Kajian Ilmu Hukum dan Politik.* Vol.1. No.4 (Oktober 2023), p.130.

Heryanto, Anas, Iksan dan Nurul Izzati Mardiyah. *Perlindungan Hukum terhadap Data Nasabah dalam Transaksi Financial Technology di Indonesia*. Jurnal Lex Generalis. Vol.7. No.4 (April 2026).

Ichsandi, Muhammad Wildan dan Wilma Silalahi. *Urgensi Perlindungan Data Pribadi dalam Sektor Perbankan di Era Digital*. Jurnal Lex Generalis. Vol.5. No.12 (Desember 2024).

Mappanyukki, Andi Tanwir. *Analisa Tindak Pidana Skimming oleh Kepolisian Daerah Sulawesi Selatan*. IJI Publication. Vol.3. No.1 (November 2022), p.72.

Matondang, Aulia Mawaddah dan Andryan. *Kebijakan Hukum Pidana terhadap Kejahatan Cyber Studi Perbandingan Antara Indonesia dan Thailand dalam Perspektif Hukum Internasional*. Jurnal Lex Generalis. Vol.6. No.1 (Januari 2025).

Wibowo, Surya Ari, Alvi Syahrin, Mahmud Mulyadi dan Sunarmi. *Pertanggungjawaban Pidana bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan dengan Metode Skimming Ditinjau Menurut Undang-Undang Informasi dan Transaksi Elektronik*. Jurnal Kajian Hukum: Iuris Studia. Vol.2. No.2 (Juni 2021), p.138.

Website

Bangsawan, M. Irwan P. Ratu. *Menakar Arti Penting Undang-Undang Nomor 1 Tahun 2023 tentang KUHP*, diakses dari https://kumparan.com/irwan-pachrozi/menakar-arti-penting-undang-undang-nomor1-tahun-2023-tentang-kuhp-1zxgXlDQ1TC/full. diakses pada 10 September 2026.

TB News. *Polda Bali Tangkap 2 Pelaku Residivis Kasus Skimming,* diakses dari https://tribratanews.polri.go.id/blog/hukum-4/polda-bali-tangkap-2-pelaku-residivis-kasus-skimming-15625. diakses pada 02 Oktober 2026.

Sumber Hukum

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6842.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6905.