KEBIJAKAN PENCEGAHAN PENCURIAN DATA *ATM* (*SKIMMING*) DALAM MEMBERIKAN PERLINDUNGAN TERHADAP KONSUMEN PERBANKAN DI INDONESIA

Laura Cecilia, Fakultas Hukum Universitas Tarumanagara,
e-mail: lim.lauracecilia @gmail.com
Ade Adhari, Fakultas Hukum Universitas Tarumanagara,
e-mail: adea@fh.untar.ac.id

doi: https://doi.org/10.24843/KS.2023.v11.i09.p09

ABSTRAK

Skimming dapat diartikan sebagai pencurian data pada kartu debet atau kartu kredit konsumen perbankan yang kemudian data tersebut disalin ke dalam kartu palsu yang masih kosong. Tujuan penelitian ini adalah untuk memahami dan menganalisa bagaimana kebijakan pencegahan skimming yang dilakukan oleh Bank Indonesia bersama dengan pemerintah dalam memberikan perlindungan terhadap konsumen perbankan. Penelitian ini menggunakan metode yuridis empiris dengan pendekatan perundang-undangan dan pendekatan konsep. Hasil penelitian ini menunjukkan bahwa kebijakan pencegahan skimming yang dilakukan oleh Bank Indonesia adalah dengan mengenalkan teknologi chip dan personal identification number (PIN) pada setiap kartu yang dikeluarkan oleh lembaga penerbit. Selain itu, pemerintah juga mengeluarkan dan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi baru-baru ini guna mencegah terjadinya skimming di Indonesia.

Keywords: *Skimming, Chip, Personal Identification Number, Perlindungan Data Pribadi, Pencegahan Skimming*

ABSTRACT

Skimming can be defined as stealing debit or credit card information from banking customers, which is then transferred onto a counterfeit blank card. The purpose of this study is to comprehend and analyze how Bank Indonesia and the government skimming prevention policies to safeguard banking customers. This study employs the juridical-empirical legal method with a statutory and concept approach. The findings of this study indicate that Bank Indonesia's skimming prevention policies are implement chip technology and a personal identification number (PIN) on each card issued by the issuing institution. To prevent skimming in Indonesia, the government recently issued and passed Law Number 27 of 2022 on Personal Data Protection.

Keywords: *Skimming, Chip, Personal Identification Number, Personal Data Protection, Skimming Prevention*

1. PENDAHULUAN

1.1. Latar Belakang Masalah

Dewasa ini, pola kehidupan masyarakat telah mengalami banyak perubahan. Hal tersebut tidak terlepas dari adanya perkembangan dalam bidang teknologi dan informasi yang telah menyebar. Tentunya perkembangan dalam bidang teknologi dan informasi akan memberikan kemudahan dalam berbagai bidang sosial, politik, ekonomi, budaya, hukum dan keamanan. Namun, apabila dilihat lebih dalam lagi ternyata perkembangan dalam bidang teknologi dan informasi ini juga dapat memunculkan suatu jenis kejahatan baru seperti kejahatan siber atau yang biasa dikenal sebagai *cybercrime.*[1]

Muladi dan Agus Raharjo berpendapat bahwa hingga saat ini belum ada keseragaman pendapat mengenai definisi *cybercrime*[2], namun ada yang menyamakan *cybercrime* dengan *computer crime*. Hal tersebut dikarenakan dalam melancarkan aksinya pelaku menggunakan sarana komputer, internet maupun perangkat keras lainnya secara ilegal yang menimbulkan kerugian bagi orang dan/atau pihak lain.[3] Perlu kita ketahui pelaku *cybercrime* adalah mereka yang memiliki keahlian khusus dalam ilmu komputer serta menguasai algoritma dan pemograman komputer. Pelaku *cybercrime* tersebut biasanya akan menganalisa bagaimana cara kerja sistem dan jaringan komputer lalu mencari celah atau kelemahan untuk dapat masuk ke dalamnya untuk melakukan kejahatan seperti misalnya pencurian data.[4] Sektor yang selalu menjadi bulan-bulanan para pelaku *cybercrime* yakni sektor perbankan, dengan kejahatan yang paling sering dilakukan ialah *skimming.*

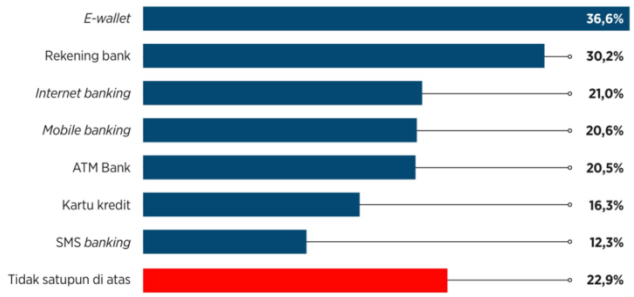
Skimming sendiri dapat diartikan sebagai pencurian data pada kartu debet maupun kartu kredit konsumen perbankan dengan cara membobol *Automatic Teller Machine* (ATM). Modus operandi yang biasanya dilakukan oleh pelaku *skimming* tersebut adalah dengan memasang alat *skimmer* di lubang mulut mesin ATM dan memasang kamera tersembunyi untuk mendapatkan kata sandi dari kartu debet maupun

[1] Laksana, Andri Winjaya. "Pemidanaan Cybercrime dalam Perspektif Hukum Pidana Positif". *Jurnal Hukum Unissula* 35, No. 1 (2019) : 52.
[2] Edrisy, Ibrahim Fikma. *Pengantar Hukum Siber* (Lampung, Sai Wawai Publishing, 2019), 37-38.
[3] Situmeang, Sahat Maruli T. *Cyber Law* (Bandung, Cakra, 2020), 23-24.
[4] *Ibid., 24.*

kartu kredit yang berbasis *magnetic stripe*.[5] Kemudian kata sandi dan data-data yang telah diperoleh tersebut akan diduplikatkan ke dalam kartu palsu yang masih kosong. *Magnetic stripe* sendiri merupakan teknologi berupa pita magnetik hitam yang berada di belakang kartu debet maupun kartu kredit. Fungsi dari *magnetic stripe* tersebut kurang lebih sama seperti pita kaset yang material feromagnetiknya dapat digunakan untuk menyimpan data.[6]

Merujuk kepada Pasal 4 Ayat (1) Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) menyatakan bahwa setiap konsumen berhak atas keamanan, kenyamanan serta keselamatan dalam menggunakan barang dan/atau jasa. Hal ini berlaku juga bagi setiap konsumen perbankan untuk mendapatkan perlindungan hukum dalam melakukan transaksi agar terhindar dari risiko kerugian yang akan ditimbulkan.[7] Kemudian berdasarkan survei nasional yang dilakukan pada tahun 2021, dari sejumlah produk perbankan atau lembaga keuangan, para responden menilai *e-wallet* dan rekening bank sebagai produk yang dianggap rentan mengalami kebocoran data. Di sisi lain, sebanyak 20,5% responden mempercayai bahwa produk perbankan belum memiliki perlindungan data yang memadai sehingga kemungkinan besar sangat rentan mengalami kebocoran data melalui *skimming ATM*.[8]

Grafik 1.1 Lembaga atau Produk Keuangan yang Rentan Mengalami Kebocoran Data



Sumber : *Katadata Insight Centre 2021*

Berkaitan dengan upaya pencegahan *skimming* yang dilakukan oleh Bank Indonesia selaku regulator sistem pembayaran adalah dengan mengeluarkan Surat Edaran Bank Indonesia Nomor 17/52/DKSP tentang Implementasi Standar Nasional Teknologi *Chip* dan Penggunaan *Personal Identification Number Online* 6 (Enam) Digit untuk Kartu ATM dan/atau Kartu Debet yang Diterbitkan di Indonesia (SEBI 2015). Penekanan pada SEBI 2015 ini adalah penggunaan *chip* dengan *National Standard Indonesian Chip Card Specification (NSICCS)* dan penggunaan *Personal Identification Number* (PIN) pada setiap kartu yang dikeluarkan oleh lembaga penerbit. Ketentuan tersebut kemudian diperkuat dengan adanya Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran (PBI 2021) yang mewajibkan setiap lembaga penerbit untuk melakukan migrasi dari kartu yang berbasis *magnetic stripe* ke kartu yang berbasis *chip*. Kemudian upaya yang dilakukan oleh pemerintah Republik Indonesia dalam mencegah terjadinya kejahatan *skimming* adalah dengan mengeluarkan dan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) baru-baru ini. Berdasarkan hal tersebut, penting untuk dilakukan penelitian lebih lanjut mengenai bagaimana kebijakan pencegahan *skimming ATM* yang dilakukan oleh Bank Indonesia bersama pemerintah dalam memberikan perlindungan terhadap konsumen perbankan di Indonesia.

Penelitian terdahulu dilakukan oleh Dian Eka Kusuma Wardani dan Maskun pada tahun 2019 yang berjudul "Kejahatan *Skimming* Sebagai Salah Satu Bentuk *Cyber Crime*". Penelitian terdahulu dan penelitian ini memiliki kesamaan yakni sama-sama mengkaji tentang kejahatan *skimming* yang merupakan bagian dari *cybercrime.* Namun, perbedaannya terdapat pada objek penelitian dan tinjauan undang-undang yang digunakan. Penelitian terdahulu tersebut lebih memfokuskan kepada pengaturan *skimming* dalam sebuah regulasi undang-undang. Sedangkan penelitian ini lebih memfokuskan kepada kebijakan pencegahan *skimming* di Indonesia. Penelitian lainnya juga dilakukan oleh Mugiatno Sumbodo dan Jafar Octo Fernas pada tahun 2019 yang berjudul "Skimming, Cara Kerja dan Pencegahan pada ATM". Walaupun sama-sama mengkaji tentang pencegahan *skimming,* namun penelitian tersebut ditujukan kepada upaya pencegahan *skimming* yang dapat dilakukan oleh diri sendiri atau masyarakat. Sedangkan fokus pada penelitian ini

[5] Enrick, Michael. "Pembobolan ATM Menggunakan Teknik Skimming Kaitannya Dengan Pengajuan Restitusi". *Jurist-Diction* 2, No. 2 (2019) : 557-558.

[6] Wardani, Dian Eka Kusuma dan Maskun. "Kejahatan Skimming sebagai Salah Satu Bentuk Cyber Crime". *Jurisprudentie* 6, No. 1 (2019) : 168-169.

[7] Sugistiyoko, Bambang Slamet Eko. "Tinjauan Yuridis Perlindungan Hukum Terhadap Nasabah Asuransi". *Yustitiabelen : Jurnal Fakultas Hukum Universitas Tulungagung* 6, No. 1 (2020) : 3.

[8] Delphia, Risanti dan K, Harjono Maykada. *Persepsi Masyarakat atas Perlindungan Data Pribadi : Survei Nasional Tahun 2021* (Jakarta, Katadata Insight Centre, 2021), 36.

adalah upaya pencegahan *skimming* yang dilakukan oleh Bank Indonesia bersama dengan pemerintah dalam memberikan perlindungan terhadap konsumen perbankan.

1.2. Rumusan Masalah

Berangkat dari pemaparan di atas, penulis ingin mengetahui lebih dalam mengenai kebijakan pencegahan *skimming* yang dilakukan di Indonesia. Oleh sebab itu, diangkatlah permasalahan dalam penelitian ini yakni bagaimana kebijakan pencegahan pencurian data *ATM* (*skimming*) yang dilakukan oleh Bank Indonesia bersama dengan Pemerintah dalam memberikan perlindungan terhadap konsumen perbankan di Indonesia?

1.3. Tujuan Penulisan

Penelitian ini dilakukan dengan sebuah tujuan untuk memahami dan menganalisa bagaimana kebijakan pencegahan pencurian data ATM (*skimming*) yang dilakukan oleh Bank Indonesia bersama dengan Pemerintah dalam memberikan perlindungan terhadap konsumen perbankan di Indonesia.

2. METODE PENELITIAN

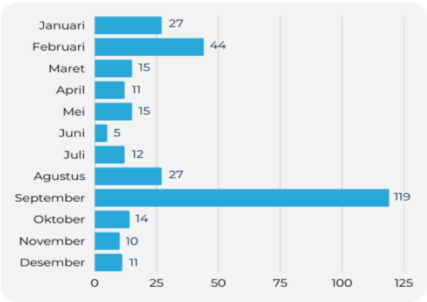
Dalam penelitian ini, metode penelitiannya terbagi menjadi 5 (lima) yakni sebagai berikut : Pertama, jenis penelitian yang digunakan adalah yuridis empiris. Penelitian ini merupakan penelitian lapangan yang data primernya didapatkan melalui regulasi hukum kemudian nantinya akan digabungkan dengan perilaku yang terjadi di dalam masyarakat. Kedua, sifat penelitian ini bersifat *descriptive research* dimana penulis akan menguraikan variabel dengan penjelasan kemudian fakta yang didapatkan akan disusun secara sistematis. Ketiga, sumber data dalam penelitian ini adalah data primer yang didapatkan melalui penelitian lapangan atau wawancara dengan responden dari Bank Indonesia dan data sekunder didapatkan melalui penelusuran bahan hukum primer, sekunder maupun tersier. Keempat, penelitian ini menggunakan pendekatan perundang-undangan dan pendekatan konsep. Kelima, teknik analisa data yang digunakan dalam penelitian ini adalah normatif kualitatif. Dimana gambaran singkat terhadap permasalahan *skimming* dan pencegahannya dilandaskan kepada UU PDP, SEBI 2015 dan PBI 2021. Kemudian nantinya akan ditarik suatu kesimpulan dengan menggunakan metode deduktif.

3. HASIL DAN PEMBAHASAN

3.1. Kebijakan Pencegahan Pencurian Data ATM (*Skimming*) dalam Memberikan Perlindungan Terhadap Konsumen Perbankan di Indonesia

Berdasarkan data yang diperoleh dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa sepanjang tahun 2022 di Indonesia telah terjadi 311 dugaan insiden kebocoran data (*data breach*) termasuk didalamnya terdapat kejahatan *skimming* pada 248 *stakeholder*.[9]

Grafik 3.1 Jumlah Insiden Kebocoran Data pada Tahun 2022



Sumber : Lanskap Keamanan Siber Indonesia 2022

Melihat banyaknya kejahatan *skimming* yang masih terjadi di Indonesia, diperlukan suatu kebijakan penanggulangan kejahatan serta sanksi pidana agar pelaku *skimming* tersebut mendapatkan efek jera terhadap perbuatannya.[10] Kebijakan penanggulangan kejahatan tersebut biasa dikenal dengan istilah kebijakan kriminal (*criminal policy*). Berkaitan dengan hal tersebut, kebijakan kriminal dalam rangka penanggulangan kejahatan di Indonesia umumnya menggunakan teori yang dikemukakan oleh G.P. Hoefnagels yang teorinya merupakan perumusan kembali dari teori yang dikemukakan oleh Marc Ancel yang menyatakan bahwa kebijakan kriminal adalah upaya rasional yang dilakukan oleh masyarakat dalam menanggulangi suatu kejahatan. Kemudian G.P Hoefnagels merumuskan kebijakan kriminal secara lebih terperinci dalam bukunya yang berjudul *The Other Side of Criminology* bahwa kebijakan kriminal tersebut merupakan bagian dari kebijakan yang lebih luas yakni kebijakan sosial (*social policy*). Dengan demikian

[9] Negara, Badan Siber dan Sandi. "Lanskap Keamanan Siber Indonesia 2022". *Dokumen Badan Siber dan Sandi Negara* (2023) : 33

[10] Hoefnagels, G. Peter. *The Other Side of Criminology (an Inversion of the Concept of Crime)* (Deventer, Kluwer, 1969), 57-59.

dapat disimpulkan bahwa kebijakan kriminal merupakan bagian dari sistem penegakan hukum, dan sistem penegakan hukum itu sendiri merupakan bagian dari kebijakan sosial.[11] Kemudian Muladi dan Barda Nawawi Arief berpendapat bahwa kebijakan kriminal atau kebijakan penanggulangan kejahatan merupakan bagian untuk mencapai suatu kesejahteraan sosial. Upaya penanggulangan kejahatan tersebut dapat dilakukan dengan 2 (dua) cara yakni secara represif melalui sistem peradilan pidana (*penal policy*) dan secara preventif diluar hukum pidana (*non-penal policy*).[12]

Upaya penanggulangan kejahatan yang dilakukan secara penal melalui sistem peradilan pidana merupakan upaya yang paling tua, setua peradaban manusia sendiri. Namun kelemahannya adalah upaya secara penal ini tidak dapat menanggulangi sebab permasalahan *skimming* yang ada di Indonesia.[13] Sudarto memberikan penjelasan lebih mendalam bahwa upaya penanggulangan kejahatan melalui sarana penal ini lebih menitikberatkan kepada penindasan, pemberantasan serta penumpasan setelah terjadinya kejahatan. Namun dalam pelaksanaannya, diperlukan suatu pertimbangan perbuatan apa saja yang seharusnya diberikan sanksi pidana dengan memperhatikan asas *ultimum remedium*. Asas ini memandang bahwa sistem peradilan pidana merupakan jalan terakhir apabila sanksi dari bidang hukum lainnya dipandang tidak cukup untuk mengatasi pencegahan serta penanggulangan kejahatan. Hal ini sesuai dengan pemikiran aliran modern yang dipelopori oleh Lambroso, Lacasagne dan Ferri yang kemudian diteruskan oleh Von Liszt, Prins dan Van Hamel dengan mendirikan *International Association for Criminology* dengan landasannya bahwa pidana adalah alat yang paling ampuh dimiliki oleh negara dengan fungsi utamanya adalah untuk memerangi kejahatan sebagai suatu gejala sosial. Namun pidana bukan merupakan satu-satunya alat, sehingga pidana tidak bisa dipisahkan dari tindakan sosial lainnya dengan memperhatikan penelitian antropologis serta penelitian sosiologis.[14]

Bila dikaitkan dengan penelitian ini, seluruh rangkaian kejahatan *skimming* telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Yuridiksi dari regulasi ini berlaku bagi setiap orang yang berada di wilayah Indonesia, baik itu warga negara Indonesia maupun warga negara asing yang menyebabkan kerugian bagi dalam negeri (Indonesia) dan/atau kerugian di negara lain. Hal tersebut sesuai dengan ketentuan dalam Pasal 2 UU ITE, mengingat kejahatan *skimming* memanfaatkan teknologi informasi dan komunikasi seperti transaksi elektronik yang sifatnya universal atau lintas teritorial. Dengan kata lain, pelaku *skimming* yang memiliki kewarganegaraan asing akan tetap dijerat dan diadili dengan ketentuan pidana dalam UU ITE yang berlaku.[15]

Ketentuan pidana bagi pelaku *skimming* tersebut telah diatur dalam Pasal 30 UU ITE yang melarang "setiap orang dengan sengaja, tanpa hak atau melawan hukum untuk mengakses komputer dan/atau sistem elektronik orang lain untuk memperoleh infomasi atau dokumen elektronik dengan cara menerobos, melanggar, melampaui maupun menjebol sistem pengamanan sehingga menyebabkan kerugian bagi orang lain". Apabila pelanggaran terhadap Pasal 30 UU ITE tersebut mengakibatkan kerugian terhadap orang lain, maka sanksi yang dikenakan dapat berupa pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp 12.000.000.000,- (dua belas miliar rupiah) sesuai dengan ketentuan dalam Pasal 46 UU ITE.

Selain itu, dalam ranah perlindungan konsumen beban pembuktian dari kejahatan *skimming* sebagaimana tertulis dalam Pasal 28 UUPK merupakan tanggung jawab pelaku usaha yakni lembaga keuangan. Apabila konsumen perbankan mengalami kerugian berupa pencurian uang yang disebabkan oleh orang tidak bertanggung jawab maka berdasarkan Pasal 4 UUPK konsumen perbankan itu berhak mendapatkan kompensasi, ganti rugi dan/atau penggantian atas hilangnya uang tersebut.[16]

Dikatakan demikian karena hubungan hukum yang terjadi antara lembaga keuangan dengan konsumen perbankan didasarkan kepada perjanjian penyimpanan. Dimana lembaga keuangan berkedudukan sebagai penerima simpanan dan konsumen perbankan sebagai nasabah yang mempercayakan dananya untuk disimpan kepada lembaga perbankan. Hubungan hukum antara lembaga keuangan dan konsumen perbankan itu didasarkan kepada hukum, kepercayaan, kerahasiaan serta prinsip kehati-hatian. Sehingga lembaga keuangan hanya dapat mengembangkan kegiatan usahanya ketika

[11] Ravena, Dey dan Kristian. *Kebijakan Kriminal (Criminal Policy)* (Jakarta, Kencana, 2017), 3.
[12] Muladi. *Demokratisasi, Hak Asasi Manusia dan Reformasi Hukum di Indonesia* (Jakarta, The Habibie Centre, 2002), 182.
[13] Kenedi, John. *Kebijakan Hukum Pidana (Penal Policy) dalam Sistem Penegakan Hukum di Indonesia* (Yogyakarta, Pustaka Pelajar, 2017), 51.
[14] Muladi dan Arief, Barda Nawawi. *Teori-Teori dan Kebijakan Pidana* (Bandung, Alumni, 1992), 33.
[15] Utomo, Renaldy Putro et al. *Upaya Perbankan dalam Penyelesaian Card Skimming* (Pekalongan, Nasya Expanding Management, 2023), 33.
[16] *Ibid*, 60.

konsumen perbankan tersebut memberikan kepercayaan untuk menempatkan dananya.[17] Dalam hal ini, lembaga keuangan yang wanprestasi menerapkan prinsip kehati-hatian dalam menjalankan usahanya sebagaimana telah diatur dalam Pasal 2 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (UU Perbankan) maka dapat dikenakan sanksi administratif berupa teguran tertulis, denda uang, penurunan tingkat kesehatan bank, larangan untuk turut serta dalam kegiatan kliring, pembekuan kegiatan usaha bahkan sampai dengan pemberhentian pengurus bank.[18] Berkaitan dengan hal ini, OJK juga mewajibkan lembaga keuangan untuk mengganti kerugian konsumen perbankan sesuai dengan Pasal 29 Peraturan Otoritas Jasa Keuangan Nomor 1/PJOK.07/2013 yang menyatakan bahwa pelaku usaha jasa keuangan wajib bertanggung jawab akibat dari kesalahan dan/atau kelalaian, pengurus, pegawai pelaku usaha jasa keuangan, dan/atau pihak ketiga yang bekerja.[19]

Ketentuan pidana kejahatan *skimming* lainnya terkait dengan perlindungan data pribadi seseorang telah diatur dalam Pasal 65 dan Pasal 66 UU PDP yang melarang "setiap orang secara melawan hukum mengumpulkan, mengungkapkan, menggunakan, dan/atau membuat data pribadi yang bukan miliknya dengan tujuan menguntungkan diri sendiri maupun orang lain yang dapat mengakibatkan kerugian bagi subjek data pribadi tersebut". Sanksi terhadap pelanggaran tersebut telah dinyatakan dalam Pasal 67 dan Pasal 68 UU PDP dengan pidana penjara paling lama 6 (enam) tahun dan denda paling banyak Rp 6.000.000.000,- (enam miliar rupiah).

Selanjutnya, Barda Nawawi Arief dalam bukunya yang berjudul "Bunga Rampai Kebijakan Hukum Pidana : Perkembangan, Penyusunan, Konsep KUHP Baru" menyatakan bahwa kejahatan juga dapat dikatakan sebagai suatu fenomena sosial dinamis yang tumbuh dan berkembang berkaitan dengan fenomena dan struktur kemasyarakatan lainnya yang kompleks, sehingga sering disebut juga sebagai *socio political problem*.[20] Oleh karenanya, upaya penanggulangan kejahatan tidak hanya dilakukan dengan sarana penal tetapi juga dilakukan dengan sarana non penal.

Berdasarkan hal tersebut, kebijakan penanggulangan kejahatan melalui sarana non penal dinilai tidak kalah penting dalam memberantas kejahatan *skimming* yang terjadi di Indonesia saat ini. Upaya penanggulangan kejahatan melalui sistem preventif ini lebih menitikberatkan kepada pencegahan terjadinya suatu kejahatan sehingga yang menjadi sasaran utamanya adalah penanganan terhadap faktor-faktor sosial yang dapat menimbulkan suatu kejahatan.[21] Upaya ini sering disebut juga sebagai *prevention without punishment* yakni upaya yang berkaitan dengan langkah teknis pencegahan yang menerapkan pedoman-pedoman tertentu seperti misalnya *code of conduct, code of ethics* dan *code of practice*.[22] Pada dasarnya, pencegahan kejahatan tidak memiliki definisi yang baku antara satu dengan yang lain. Namun, inti dari pencegahan kejahatan tersebut adalah suatu rancangan untuk mengupayakan pengurangan jumlah dan kesempatan terjadinya kejahatan dalam masyarakat.[23] Hal ini ditekankan dalam berbagai Kongres PBB antara lain dalam Kongres PBB ke-VI di Caracas, Venezuela tahun 1980 tentang *Crime Trends and Crime Prevention Strategies.* Selanjutnya ditekankan lagi dalam Kongres PBB ke-VII di Milan pada tahun 1985 dan dalam Kongres PBB ke-VIII di Havana tahun 1990 berkaitan dengan masalah "*Social Aspects of Crime Prevention and Criminal Justice in the Context of Development*".

Dalam perkembangannya, upaya pencegahan kejahatan dapat dilakukan dengan beberapa pendekatan :

1. Pendekatan sosial (*social crime prevention*), yang menekankan kepada bagaimana akar dari kejahatan dapat ditumpas sehingga pola kehidupan sosial masyarakat berubah;
2. Pendekatan situasional (*situational crime prevention*), yang menekankan pada bagaimana caranya mengurangi kesempatan bagi pelaku melakukan tindak pidana; dan
3. Pendekatan komunitas/masyarakat (*community based crime prevention*), yang melibatkan masyarakat secara aktif bekerja sama dengan lembaga pemerintah untuk mengurangi terjadinya kejahatan dalam masyarakat.

Upaya pencegahan ini dipandang sebagai upaya penanggulangan kejahatan yang paling strategis, memegang peranan penting dan dianggap lebih menjanjikan keberhasilannya daripada penerapan dengan sarana penal melalui sistem pemidanaan. Sejalan dengan hal tersebut, nyatanya kebijakan kriminal yang

[17] Prasetio, Ary. "Perlindungan Hukum terhadap Nasabah Bank yang menjadi Korban Skimming", *Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara* (2019) : 33-34.
[18] Djumhana, Muhammad. *Hukum Perbankan di Indonesia* (Bandung, PT. Citra Aditya Bakti, 2012), 278.
[19] Utomo, Renaldy Putro et al., *Op. Cit*., 58.
[20] Ravena, Dey dan Kristian. *Op.Cit.,* 17.
[21] Kenedi, John. *Op. Cit.,* 57.
[22] Ravena, Dey dan Kristian. *Op. Cit*, 18.
[23] Lab, Steven P. *Crime Prevention : Approaches, Practices and Evaluations* (USA, Anderson Pub Co, 2010), 26.

dilakukan dengan sarana penal melalui jalur pemidanaan tidak dapat mengurangi atau bahkan menghilangkan kejahatan *skimming* yang masih marak terjadi di Indonesia.

Bila dikaitkan dengan penelitian ini, beberapa faktor pendukung yang menyebabkan kejahatan *skimming* di Indonesia terus meningkat setiap tahunnya yakni layanan komunikasi yang mudah didapatkan, bahkan jumlah *provider* internet di Indonesia sangat beragam sehingga membuat sistem pengawasan menjadi sangat sulit. Lembaga keamanan siber *Communication and Information System Security Research Center* (CISSReC) menyatakan bahwa kejahatan *skimming* yang terjadi di Indonesia belakangan ini mudah ditebak dikarenakan lemahnya sistem pengawasan dan pengamanan perbankan serta kurangnya pengamanan data konsumen perbankan yang membuat pelaku *skimming* mengeksploitasi korban.[24] Berkaitan dengan hal tersebut, Denny Sugiri seorang *Auditor Information Security Management System* juga menyatakan pendapatnya yang dikutip dari Liputan 6 bahwa salah satu faktor yang menyebabkan kejahatan *skimming* terus meningkat adalah kurangnya penerapan analisa risiko dari lembaga perbankan. Dalam hal ini, lembaga perbankan harus melakukan analisa terhadap permasalahan pada *update system* serta kontrol keamanan dan informasi agar kejahatan *skimming* tidak terjadi lagi.[25] Penggunaan mesin ATM di Indonesia juga perlu dikritisi, lantaran sebagian besar perbankan yang ada di Indonesia masih menggunakan sistem operasi *Windows XP* yang sama sekali tidak mendapatkan dukungan keamanan dari *Microsoft* sejak tahun 2014. Kemudian bila melihat dari segi teknologi keamanan perbankan di Indonesia masih sangat kurang terjamin. Hal tersebut dapat terbukti dari sekian banyak perbankan di tanah air tidak ada yang masuk ke dalam kategori bank paling aman di Asia versi *Global Magazine*.[26]

Dalam mengumpulkan informasi mengenai kebijakan pencegahan *skimming* yang dilakukan oleh Bank Indonesia, penulis melakukan wawancara dengan seorang informan yang bekerja di Departemen Hukum Bank Indonesia. Beberapa kebijakan yang telah dilakukan oleh Bank Indonesia dalam mencegah terjadinya *skimming*, diantaranya adalah melalui pengenalan *chip* dan *PIN* pada setiap kartu yang diterbitkan oleh lembaga penerbit dan regulasinya telah diatur dalam SEBI 2015. Kebijakan tersebut dilatarbelakangi oleh maraknya kejahatan *skimming* yang terjadi di Indonesia dilakukan dengan cara menyalin data kartu yang berbasis *magnetic stripe* ke dalam kartu yang masih kosong. Kemudian SEBI 2015 tersebut diperkuat lagi dengan adanya kebijakan PBI 2021 yang mewajibkan seluruh lembaga penerbit kartu untuk melakukan migrasi dari kartu yang berbasis *magnetic stripe* menjadi kartu yang berbasis *chip.* Kartu yang menggunakan *chip* dengan *NSICCS* dinilai lebih sulit untuk digandakan atau dicuri datanya dikarenakan pada kartu yang berbasis *chip* tersebut sudah memiliki kriptografi.[27] Pengertian kriptografi sendiri adalah sebuah seni untuk menjaga keamanan pesan dengan cara mengubahnya menjadi kode yang sulit dimengerti.[28] Dalam kriptografi juga dikenal istilah enkripsi yang dapat diartikan sebagai suatu proses penyamaran untuk mengamankan pesan asli (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*) agar tidak dapat dibaca dengan mudah.[29]

Berkaitan dengan hal tersebut, Bank Indonesia mengelaborasikan lebih lanjut bahwa setiap lembaga penerbit kartu telah membuat kriptografi pada setiap kartu berbasis *chip* yang akan dikeluarkan sehingga tidak mudah digandakan atau dicuri datanya. Sehingga apabila terjadi suatu permintaan transaksi, maka *Electronic Data Capture* (terminal *EDC*) akan mengirimkan proses validasi kriptografi ke lembaga penerbit kartu untuk dilakukan verifikasi lanjutan. Hal tersebut dilakukan guna mengurangi *skimming* yang terjadi di Indonesia.[30]

Pada implementasinya memang saat ini migrasi dari kartu yang berbasis *magnetic stripe* menjadi kartu yang berbasis *chip* sudah 100% dilaksanakan namun terdapat pengecualian untuk penerbitan dan penggunaan kartu yang masih berbasis *magnetic stripe*. Berdasarkan ketentuan dalam Bab 1 Huruf (A) Angka (2) SEBI 2015 menyatakan bahwa kartu yang berbasis *magnetic stripe* masih diperbolehkan terbit untuk keperluan menabung dengan saldo yang ditetapkan hanya Rp 5.000.000,- (lima juta rupiah). Selain itu, lembaga penerbit kartu juga harus memiliki prosedur pencegahan dan penanganan *skimming*, memastikan keamanan yang memadai, serta melakukan edukasi kepada setiap pemegang kartu berbasis *magnetic stripe* untuk melindungi kartu yang dimilikinya.

---

[24] Utomo, Renaldy Putro et al. *Op. Cit.,* 38.

[25] Iskandar. "Ini Penyebab Terjadinya Pembobolan Mesin ATM", https://www.liputan6.com/tekno/read/2049837/ini-penyebab-terjadinya-pembobolan-mesin-atm, 1 Juli 2023, 1.

[26] *Ibid,* 1.

[27] Penulis. "Wawancara *Online* dengan Departemen Hukum Bank Indonesia" pada 10 Januari 2023.

[28] Amin, M. Miftakul. "Implementasi Kriptografi Klasik pada Komunikasi Berbasis Teks". *Jurnal Pseudocode* III, No. 2 (2016) : 130.

[29] Wiharto, Yudi dan Irawan, Ari. "Enkripsi Data Menggunakan Advanced Encryption Standard 256". *Jurnal Kilat* 7, No. 2 (2018) : 92.

[30] Penulis, *Op.Cit.*

Bank Indonesia dalam hal ini juga melakukan kerjasama dengan lembaga penerbit kartu dalam rangka pelaksanaan *NSICCS* serta melakukan berbagai upaya guna mencegah terjadinya kejahatan *skimming* di Indonesia, antara lain sebagai berikut:

A. Bank Indonesia meminta laporan berkala terkait sejauh mana proses migrasi kartu berbasis *magnetic stripe* menjadi kartu yang berbasis *chip* telah dilakukan;
B. Bank Indonesia melakukan pengawasan apakah frekuensi kejahatan *skimming* semakin berkurang atau malah semakin bertambah setelah proses migrasi kartu dilakukan;
C. Bank Indonesia yang memiliki otoritas melakukan pemeriksaan dan kliring terkait dengan pemrosesan transaksi pembayaran yang menggunakan kartu wajib berlandaskan kepada *NSICCS*;
D. Bank Indonesia juga akan mengenakan sanksi apabila terjadi pelanggaran kewajiban dalam SEBI 2015 dan PBI 2021 yang dilakukan oleh lembaga penerbit kartu.[31]

Selain itu, Bank Indonesia juga melakukan kerjasama dengan Asosiasi Sistem Pembayaran Indonesia (ASPI) dalam menciptakan sistem pembayaran yang aman dan efisien guna mencegah terjadinya *skimming* di Indonesia. ASPI inilah yang nantinya akan bekerjasama dengan lembaga penerbit kartu untuk membantu proses migrasi dari kartu yang berbasis *magnetic stripe* ke kartu yang berbasis *chip*.[32] Lembaga penerbit kartu akan memeriksa secara berkala apakah di setiap terminal *EDC* atau mesin *ATM* dipasang alat *skimmer*. Lembaga penerbit kartu juga melakukan edukasi kepada konsumen perbankan khususnya yang berada pada *remote area* untuk tidak menyerahkan kartu yang dimilikinya kepada sembarang orang termasuk kepada *teller* atau kasir tanpa pengawasan. Edukasi tersebut dapat dilakukan dengan cara datang langsung kepada masyarakat, melalui seminar dan webinar atau bisa juga dilakukan edukasi langsung saat terjadi kasus skimming.[33]

Berdasarkan hasil pengawasan pada tahun 2022, Bank Indonesia menemukan 7 (tujuh) kasus skimming kartu ATM/kartu debet pada penyedia jasa pembayaran. Dalam pengawasan itu, ditemukan 5 (lima) kelemahan dalam penerapan kebijakan pencegahan skimming yang terjadi, yakni sebagai berikut :

1) Logic host ATM yang masih dapat memproses kartu berbasis *magnetic stripe* tidak melakukan penolakan terhadap transaksi fallback;
2) Keamanan fisik dari terminal EDC maupun mesin ATM belum cukup memadai sehingga seringkali bisa dimodifikasi oleh pelaku *skimming* ATM;
3) Host ATM tidak membatasi saldo kartu yang berbasis *magnetic stripe* maksimal Rp 5.000.000.000,- (lima juta rupiah);
4) Host ATM tidak menolak hasil modifikasi data *service code* pada track 2 data magnetic stripe; dan
5) *Fraud Detection System* (FDS) tidak dapat mengidentifikasi transaksi abnormal dari nasabah yang berdampak pada kasus *skimming* ATM.

Sehingga untuk langkah kedepannya, Bank Indonesia akan mengupayakan berbagai hal untuk memitigasi kejahatan skimming antara lain sebagai berikut :

a) Meningkatkan pemahaman serta melakukan review kembali logic dalam host ATM agar dapat sesuai dengan ketentuan NSICCS, yaitu melakukan penolakan terhadap transaksi fallback serta membatasi saldo maksimal untuk rekening yang masih menggunakan kartu berbasis magnetic stripe;
b) Meningkatkan upaya monitoring terhadap status mesin ATM, melakukan review berkala atas penempatan ATM serta memeriksa perangkat keamanan ATM seperti CCTV, keypad dan slot kartu secara berkala;
c) Menyusun upaya mitigasi risiko skimming terhadap kartu khusus (seperti kartu bantuan sosial, kartu kredit co-branding, affinity card, dll) yang masih menggunakan kartu berbasis magnetic stripe; dan
d) Melakukan upaya edukasi secara masif dan berkala kepada konsumen mengenai modus-modus kejahatan skimming di berbagai kanal Bank.

Selain Bank Indonesia, OJK dalam hal ini juga bertanggung jawab dalam memberikan perlindungan hukum kepada konsumen perbankan. Upaya pencegahan kerugian konsumen perbankan yang dilakukan oleh OJK telah diatur dalam Pasal 28 Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (UU OJK) yang meliputi pembekalan edukasi kepada konsumen perbankan terkait dengan karakteristik, layanan dan produk sektor jasa keuangan; penghentian kegiatan lembaga keuangan yang dapat membahayakan dan merugikan masyarakat; serta melakukan upaya lainnya yang dianggap tepat sesuai dengan ketentuan perundang-undangan yang berlaku. Selain upaya pencegahan yang dilakukan tersebut, berdasarkan Pasal 29 UU OJK yang menyatakan bahwa OJK juga menyiapkan perangkat yang

[31] *Ibid*.
[32] *Ibid*.
[33] *Ibid*.

memadai, membuat mekanisme serta memfasilitasi penyelesaian pengaduan apabila konsumen perbankan merasa dirugikan oleh lembaga jasa keuangan. Kemudian merujuk kepada Pasal 30 UU OJK yang menyatakan bahwa OJK memiliki kewenangan untuk melakukan pembelaan hukum bagi konsumen perbankan dengan cara melakukan tindakan tertentu dan mengajukan gugatan untuk menyelesaikan pengaduan konsumen serta memperoleh kembali harta kekayaan dan ganti kerugian dari pihak yang dirugikan.

Selanjutnya pencegahan *skimming* yang dilakukan oleh pemerintah adalah dengan mengesahkan UU PDP baru-baru ini. Berdasarkan ketentuan dalam Pasal 35 dan Pasal 60 UU PDP menyatakan bahwa upaya yang dilakukan oleh pemerintah dalam mencegah terjadinya *skimming ATM* adalah sebagai berikut :

(1) Menyusun kebijakan mengenai pemrosesan data pribadi yang bertentangan dengan undang-undang;
(2) Memperhatikan dan melindungi risiko keamanan data pribadi;
(3) Melakukan pemeriksaan terhadap dugaan terjadinya pelanggaran data pribadi; serta
(4) Menjatuhkan sanksi administratif kepada pengendali data pribadi maupun pemroses data pribadi terhadap pelanggaran perlindungan data.

Kemudian berdasarkan ketentuan dalam Pasal 63 UU PDP peran serta dari masyarakat juga sangat diperlukan baik secara langsung maupun tidak langsung dalam mendukung terselenggaranya perlindungan data pribadi. Peran serta dari masyarakat tersebut dapat dilakukan melalui berbagai cara seperti pendidikan, pelatihan, sosialisasi, advokasi dan/atau pengawasan berdasarkan peraturan perundang-undangan yang berlaku. Upaya lainnya yang dapat dilakukan oleh masyarakat dalam mencegah terjadinya *skimming* adalah sebagai berikut :

(a) Menutup tangan saat memasukkan PIN di mesin ATM maupun terminal EDC. Hal ini dilakukan untuk mencegah pelaku *skimming* mengetahui PIN ATM pemilik kartu tersebut melalui kamera tersembunyi yang telah dipasang sebelumnya;
(b) Menjaga kerahasiaan PIN dan tidak membagikannya kepada siapapun juga;
(c) Mengganti PIN secara berkala guna menghindari kejahatan *skimming* melalui pembobolan ATM. Dalam hal ini, jangan menggunakan PIN dengan angka yang mudah ditebak seperti tanggal lahir melainkan gunakanlah nomor acak yang sulit ditebak;
(d) Selalu periksa mesin ATM dan terminal EDC yang akan digunakan apakah terdapat alat *skimmer* yang dipasang atau tidak. Apabila masyarakat melihat adanya alat yang mencurigakan dipasang pada mesin ATM maupun terminal EDC, segeralah melapor ke pihak yang bersangkutan. Kemudian perhatikan juga lokasi mesin ATM dikarenakan biasanya pelaku hanya mengincar mesin ATM yang berada di *remote area* atau di wilayah yang penjagaannya tidak diawasi dengan ketat; dan
(e) Segera blokir kartu ATM atau melaporkan kepada lembaga keuangan apabila menemukan kejanggalan atau telah terjadi transaksi abnormal pada kartu debet maupun kartu kredit.[34]

4. KESIMPULAN

Kejahatan *skimming* merupakan salah satu bentuk *cybercrime* dikarenakan dalam melancarkan aksinya pelaku menggunakan komputer, internet atau perangkat keras lainnya secara ilegal. Kebijakan pencegahan *skimming* yang dilakukan oleh Bank Indonesia dalam memberikan perlindungan terhadap konsumen perbankan dilakukan dengan cara mengenalkan teknologi *chip* dan PIN pada setiap kartu yang diterbitkan oleh lembaga penerbit kartu. Selain itu, dilakukan juga migrasi dari kartu yang berbasis *magnetic stripe* ke kartu yang berbasis *chip*. Kedua kebijakan tersebut telah diatur dalam SEBI 2015 dan PBI 2021. Dalam mendukung kebijakan tersebut, Bank Indonesia melakukan kerjasama dengan berbagai lembaga penerbit kartu, ASPI dan OJK. Kemudian, pemerintah juga memiliki peranan yang besar dalam mencegah terjadinya *skimming* yakni dengan melindungi data pribadi setiap konsumen perbankan yang telah direalisasikan melalui pengesahan UU PDP baru-baru ini.

DAFTAR PUSTAKA

Buku

Delphia, Risanti dan K, Harjono Maykada. *Persepsi Masyarakat atas Perlindungan Data Pribadi : Survei Nasional Tahun* 2021 (Jakarta : Katadata Insight Centre, 2021).

Djumhana, Muhammad. *Hukum Perbankan di Indonesia* (Bandung, PT. Citra Aditya Bakti, 2012).

Edrisy, Ibrahim Fikma. *Pengantar Hukum Siber.* (Lampung : Sai Wawai Publishing, 2019).

[34] Renaldy Putro Utomo et al., *Op. Cit*., hal. 81-82.

Hoefnagels, G. Peter. *The Other Side of Criminology (an Inversion of the Concept of Crime)* (Deventer, Kluwer, 1969).

Kenedi, John. *Kebijakan Hukum Pidana (Penal Policy) dalam Sistem Penegakan Hukum di Indonesia* (Yogyakarta, Pustaka Pelajar, 2017).

Lab, Steven P. *Crime Prevention : Approaches, Practices and Evaluations* (USA, Anderson Pub Co, 2010).

Muladi. *Demokratisasi, Hak Asasi Manusia dan Reformasi Hukum di Indonesia* (Jakarta, The Habibie Centre, 2002).

Muladi dan Arief, Barda Nawawi. *Teori-Teori dan Kebijakan Pidana* (Bandung, Alumni, 1992).

Ravena, Dey dan Kristian. *Kebijakan Kriminal (Criminal Policy)* (Jakarta, Kencana, 2017).

Situmeang, Sahat Maruli T. *Cyber Law* (Bandung : Cakra, 2020).

Utomo, Renaldy Putro et al. *Upaya Perbankan dalam Penyelesaian Card Skimming* (Pekalongan, Nasya Expanding Management, 2023).

Jurnal

Amin, M. Miftakul. "Implementasi Kriptografi Klasik pada Komunikasi Berbasis Teks". *Jurnal Pseudocode* III, No. 2 (2016).

Enrick, Michael. "Pembobolan ATM Menggunakan Teknik Skimming Kaitannya Dengan Pengajuan Restitusi". *Jurist*-Diction 2, No. 2 (2019).

Laksana, Andri Winjaya. "Pemidanaan Cybercrime dalam Perspektif Hukum Pidana Positif". *Jurnal Hukum Unissula* 35, No. 1 (2019).

Sugistiyoko, Bambang Slamet Eko. "Tinjauan Yuridis Perlindungan Hukum Terhadap Nasabah Asuransi". *Yustitiabelen : Jurnal Fakultas Hukum Universitas Tulungagung* 6, No. 1 (2020).

Wardani, Dian Eka Kusuma dan Maskun. "Kejahatan Skimming sebagai Salah Satu Bentuk Cyber Crime". *Jurisprudentie* 6, No. 1 (2019).

Wiharto, Yudi dan Irawan, Ari. "Enkripsi Data Menggunakan Advanced Encryption Standard 256". *Jurnal Kilat* 7, No. 2 (2018).

Peraturan Perundang-Undangan

Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 118, Tambahan Lembaran Negara Republik Indonesia Nomor 5431).

Surat Edaran Bank Indonesia Nomor 17/52/DKSP tentang Implementasi Standar Nasional Teknologi Chip dan Penggunaan Personal Identification Number Online 6 (Enam) Digit untuk Kartu ATM dan/atau Kartu Debet yang Diterbitkan di Indonesia.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790).

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 22, Tambahan Lembaran Negara Republik Indonesia Nomor 3821).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).

Sumber Lainnya

Iskandar. "Ini Penyebab Terjadinya Pembobolan Mesin ATM", https://www.liputan6.com/tekno/read/2049837/ini-penyebab-terjadinya-pembobolan-mesin-atm, 1 Juli 2023.

Penulis. "Wawancara *Online* dengan Departemen Hukum Bank Indonesia" pada 10 Januari 2023.

Prasetio, Ary. "Perlindungan Hukum terhadap Nasabah Bank yang menjadi Korban Skimming", *Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara* (2019).