

REGULASI PERLINDUNGAN NASABAH TERHADAP RISIKO SKIMMING DAN CYBER CRIMENajwa Rizkiana Hanum¹, Isditta Chaula Liani², Eka Gusnetta Putri Wahyudi³

Prodi Ilmu Hukum, Fakultas Hukum, Universitas Negeri Semarang

njwrizkianahanum@unnes.students.ac.idisditta9@students.unnes.ac.idekagusnetta@unnes.students.ac.id**Abstrak**

Dalam era digital yang semakin berkembang, perlindungan nasabah terhadap risiko *skimming* dan *cyber crime* menjadi isu yang krusial bagi industri keuangan. Penelitian ini bertujuan untuk menganalisis regulasi yang ada dalam rangka melindungi nasabah dari ancaman tersebut. Metode yang digunakan meliputi kajian literatur dan analisis kebijakan yang relevan, dengan fokus pada peran otoritas keuangan dalam mengimplementasikan regulasi yang efektif. Hasil penelitian menunjukkan bahwa meskipun berbagai regulasi telah diterapkan, masih terdapat tantangan dalam penegakan dan kesadaran nasabah. Disarankan agar otoritas keuangan meningkatkan edukasi nasabah dan memperkuat kolaborasi dengan lembaga keuangan untuk menciptakan lingkungan yang lebih aman. Penelitian ini diharapkan dapat memberikan wawasan bagi pembuat kebijakan dan industri keuangan dalam upaya meningkatkan perlindungan nasabah di era digital.

Kata Kunci : Perlindungan Nasabah, *Skimming*, *Cyber Crime*.

Abstract

In the increasingly evolving digital era, customer protection against the risk of skimming and cyber crime has become a crucial issue for the financial industry. This study aims to analyze existing regulations in order to protect customers from these threats. The methods used include literature review and relevant policy analysis, with a focus on the role of financial authorities in implementing effective regulation. The results of the study show that although various regulations have been implemented, there are still challenges in enforcement and customer awareness. It is recommended that financial authorities improve customer education and strengthen collaboration with financial institutions to create a safer environment. This research is expected to provide insights for policymakers and the financial industry in an effort to improve customer protection in the digital era.

Keywords : customer protection, Skimming, Cyber Crime.

Article History

Received: November 2024

Reviewed: November 2024

Published: November 2024

Plagiarism Checker No 234

Prefix DOI : Prefix DOI :

10.8734/CAUSA.v1i2.365

Copyright : Author**Publish by : CAUSA**

This work is licensed under

a [Creative Commons](https://creativecommons.org/licenses/by-nc/4.0/)[Attribution-](https://creativecommons.org/licenses/by-nc/4.0/)[NonCommercial 4.0](https://creativecommons.org/licenses/by-nc/4.0/)[International License.](https://creativecommons.org/licenses/by-nc/4.0/)**PENDAHULUAN**

Teknologi saat ini merupakan peran utama dalam memfasilitasi berbagai kegiatan manusia, terutama dalam hal bertransaksi. Dengan kemajuan teknologi yang semakin cepat, membuat setiap orang yang ingin melakukan transaksi, dapat melakukannya dengan sangat cepat dan juga efisien sehingga mempermudah interaksi ekonomi dan aktivitas lainnya dalam masyarakat modern. Begitupun dengan pihak perbankan yang ada di Indonesia maupun luar negeri, rata-rata sudah menggunakan kecanggihan dari teknologi tersebut dengan melakukan inovasi teknologi industri jasa perbankan dengan melahirkan produk-produk seperti ATM,

*Electronic Bill Payment, Phone Banking, Debet Card, Cash Management, Corporate Internet Banking, Individual Internet Banking Services dan EFT Post.*¹

Di era digital yang semakin maju, sektor perbankan menghadapi risiko yang terus berkembang, terutama dalam bentuk kejahatan *skimming* dan *cyber crime*. *Skimming* adalah metode pencurian data kartu debit atau kredit nasabah dengan menggunakan alat pemindai yang ditempelkan pada mesin ATM atau EDC, sedangkan *cyber crime* mencakup berbagai jenis serangan siber yang bertujuan mencuri informasi sensitif atau mengakses rekening nasabah secara ilegal. Kejahatan-kejahatan ini tidak hanya menimbulkan kerugian finansial bagi nasabah, tetapi juga dapat merusak reputasi lembaga keuangan serta mempengaruhi kepercayaan masyarakat terhadap industri perbankan.²

Pemerintah Indonesia, melalui berbagai regulasi, telah berupaya melindungi nasabah dari risiko ini. Di antaranya adalah Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diperbarui menjadi UU No. 19 Tahun 2016, yang memberikan dasar hukum bagi perlindungan terhadap informasi dan data pribadi nasabah dari penyalahgunaan. Selain itu, Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) juga menerbitkan berbagai aturan terkait keamanan siber dan perlindungan konsumen, seperti Peraturan Bank Indonesia No. 14/2/PBI/2012 tentang Tata Kelola Teknologi Informasi oleh Bank Umum serta ketentuan OJK tentang perlindungan konsumen sektor jasa keuangan. Melalui regulasi ini, diharapkan lembaga keuangan dapat menerapkan sistem keamanan yang lebih baik serta menjalankan edukasi bagi nasabah terkait ancaman *skimming* dan kejahatan siber lainnya.

Pembuatan regulasi yang sudah disebutkan di atas diharapkan dapat menjadi perlindungan hukum kepada para korban. Namun, meskipun regulasi telah diterapkan, kejahatan *skimming* dan *cyber crime* masih sering terjadi. Hal tersebut dapat terjadi karena masih belum ada sebuah regulasi yang secara khusus mengatur mengenai perlindungan data pribadi yang menyebabkan kejahatan dalam penyalahgunaan sistem informasi dan pencurian terhadap data pribadi masih banyak terjadi. Ini mengindikasikan bahwa penerapan regulasi perlindungan nasabah belum sepenuhnya efektif dalam menangani ancaman kejahatan siber di Indonesia. Kecepatan perkembangan teknologi serta minimnya edukasi nasabah menjadi tantangan besar dalam mengatasi permasalahan ini. Selain itu, keterbatasan sumber daya, baik pada lembaga keuangan maupun pada aparat penegak hukum, juga menghambat pelaksanaan regulasi dengan optimal.³

Untuk memahami permasalahan ini lebih mendalam, artikel ini akan mengulas tiga rumusan masalah utama sebagai berikut:

1. Bagaimana efektivitas regulasi perlindungan nasabah dalam menangani kasus *skimming* dan *cyber crime* di Indonesia?
2. Apa saja kendala yang dihadapi dalam penerapan regulasi untuk melindungi nasabah dari risiko *skimming* dan *cyber crime*?
3. Bagaimana peran otoritas keuangan dalam meningkatkan kesadaran dan edukasi nasabah terhadap risiko *skimming* dan *cyber crime*?

Dengan membahas ketiga rumusan masalah ini, diharapkan artikel ini dapat memberikan gambaran yang komprehensif mengenai tantangan yang dihadapi dalam melindungi nasabah dari kejahatan siber di Indonesia serta menawarkan rekomendasi yang konstruktif untuk mengatasi kendala-kendala tersebut.

PEMBAHASAN

¹Triansyah, R. Anadi, Y. & Faisol. (2024). Perlindungan Hukum Terhadap Nasabah Korban *Skimming* (Studi Kasus di Bank Rakyat Indonesia KCP Malinau Kalimantan Utara). *Jurnal DINAMIKA*. Volume 30 Nomor 2 Bulan Juli 2024.

² Juita, S. Astanti, D. & Septiandani D. (2023). Perlindungan Hukum Terhadap Nasabah Bank Korban Kejahatan *Skimming*. *Jurnal USM Law Review* Vol. 6, No. 1, Tahun 2023.

³ Rumlus, M. & Hanif, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik. *Jurnal HAM*. Vol. 11, No. 2, Agustus 2020.

1.1. Efektivitas Regulasi Perlindungan Nasabah Dalam Menangani Kasus Skimming Dan Cyber Crime Di Indonesia

Nasabah di Indonesia memiliki hak yang setara untuk memperoleh kepastian dan kedudukan yang adil di dalam hukum, sesuai dengan Pasal 28D ayat (1) UUD 1945 yang menjamin hak setiap orang atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil, serta perlakuan yang sama di hadapan hukum. Menurut Mochtar Kusumaatmadja, hukum seharusnya berperan dalam melindungi masyarakat guna mencapai ketertiban dan kepastian hukum. Selain itu, sebagai bagian dari perlindungan konsumen, nasabah juga memiliki hak untuk memperoleh informasi yang transparan terkait keamanan sistem perbankan dan tindakan yang diambil oleh lembaga keuangan dalam menghadapi risiko kejahatan siber. Dalam menghadapi semakin kompleksnya ancaman digital, pemerintah dan otoritas perbankan diharapkan meningkatkan regulasi dan pengawasan guna melindungi kepentingan nasabah. Upaya ini penting agar setiap individu merasa aman dan terlindungi dalam menggunakan layanan perbankan, sehingga kepercayaan masyarakat terhadap sistem perbankan dapat terus terjaga.⁴

Dalam melindungi kepentingan nasabah, terdapat sejumlah regulasi yang dirancang untuk melindungi nasabah dari berbagai risiko, termasuk skimming dan kejahatan siber. Pertama, Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen menyediakan dasar hukum bagi perlindungan konsumen, termasuk hak untuk menerima informasi yang transparan mengenai produk dan layanan keuangan yang mereka gunakan. Selanjutnya, Undang-Undang No. 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK) memberikan kewenangan kepada OJK untuk mengawasi dan melindungi kepentingan nasabah di sektor jasa keuangan, termasuk merancang regulasi yang memastikan keamanan transaksi elektronik. Terakhir, Undang-Undang No. 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (P2SK) bertujuan memperkuat perlindungan konsumen di sektor keuangan, termasuk dalam konteks e-commerce dan fintech, dengan menetapkan sanksi bagi pelanggaran yang merugikan nasabah. Melalui peraturan-peraturan ini, pemerintah berupaya membangun ekosistem keuangan yang aman dan andal, sehingga nasabah terlindungi dari berbagai ancaman dan dapat bertransaksi dengan rasa aman.⁵

Efektivitas regulasi perlindungan nasabah dalam menangani kasus skimming dan cyber crime di Indonesia dapat dinilai dari beberapa sudut pandang. Salah satunya adalah implementasi aturan yang telah ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta berbagai peraturan yang dikeluarkan oleh Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI). Peraturan-peraturan ini bertujuan untuk melindungi nasabah dari kejahatan berbasis teknologi, namun efektivitasnya sangat bergantung pada bagaimana aturan tersebut diterapkan di lapangan. Jika bank dan lembaga keuangan konsisten memenuhi standar keamanan yang diatur, maka risiko kejahatan seperti skimming dan serangan siber bisa diminimalisir. Namun, di sisi lain, banyaknya kasus yang terjadi menimbulkan pertanyaan mengenai sejauh mana lembaga keuangan benar-benar mematuhi peraturan tersebut.

Peran OJK dan BI sebagai lembaga pengawas sektor keuangan sangat penting dalam memastikan kepatuhan industri terhadap regulasi perlindungan nasabah. Kedua lembaga ini tidak hanya mengeluarkan peraturan, tetapi juga harus melakukan pengawasan dan audit secara berkala untuk mengidentifikasi potensi kelemahan keamanan di institusi keuangan. Dalam beberapa kasus, ketegasan dalam memberikan sanksi kepada bank atau lembaga yang gagal melindungi data nasabah menjadi sangat penting agar memberikan efek jera. Namun, sejauh mana pengawasan ini berjalan efektif juga perlu dievaluasi, mengingat bahwa teknologi terus berkembang dan pola kejahatan siber semakin kompleks.

⁴ Hardinata, M. Shanty, Sitohang, Y. Rahma, I. Utomo, S & Ramadoni, S. (2024). Sosialisasi Kebijakan Bank Digital Perlindungan Hukum Terhadap Data Nasabah Dari Risiko Serangan Siber. *RENATA : Jurnal Pengabdian Masyarakat Kita Semua*. Vol. 2 No. 2 Agustus 2024.

⁵Saly, J. & Nainggolan, J. (2023). Efektivitas Perlindungan Hukum Konsumen Berdasarkan Undang Undang Nomor 4 Tahun 2023 Tentang Pengembangan dan Penguatan Sektor Keuangan. *Jurnal Kewarganegaraan*. Vol. 7 No. 2 Desember 2023.

Selain itu, perlindungan terhadap data nasabah menjadi inti dari pencegahan skimming dan cyber crime. Bank dan lembaga keuangan harus menggunakan teknologi terbaru dan standar keamanan tinggi untuk melindungi data nasabah dari akses tidak sah. Regulasi di Indonesia menekankan pentingnya enkripsi data dan teknologi anti-skimming pada mesin ATM serta perangkat pembayaran lainnya. Meski demikian, tidak semua lembaga keuangan memiliki kemampuan teknologi yang memadai, terutama bank-bank kecil yang mungkin kesulitan mengadopsi teknologi mutakhir ini.

Penting juga untuk melihat bagaimana kasus-kasus skimming dan cyber crime ditangani ketika terjadi. Respons dari bank dan aparat hukum dalam menangani pengaduan nasabah dan proses penyelesaian kasus dapat menjadi indikator seberapa serius regulasi ini diterapkan. Di beberapa negara, regulasi mengharuskan bank memberikan kompensasi atau ganti rugi kepada nasabah yang menjadi korban. Namun, apakah hal ini sudah diterapkan di Indonesia dan sejauh mana nasabah dapat mengakses hak tersebut masih perlu dipastikan.

Efektivitas regulasi tidak hanya bergantung pada tindakan lembaga keuangan dan pengawasan pemerintah, tetapi juga pada kesadaran nasabah. Bank diharapkan aktif melakukan edukasi kepada nasabah terkait bahaya skimming dan cyber crime, termasuk tips untuk menjaga keamanan data pribadi. Jika nasabah lebih waspada terhadap ancaman ini, risiko kejahatan dapat diminimalisir. Namun, jika kesadaran ini masih rendah, perlindungan dari regulasi akan menjadi kurang efektif.

Upaya pencegahan kejahatan skimming dan cyber crime menuntut kolaborasi antara lembaga keuangan, penegak hukum, dan ahli keamanan siber. Karena teknologi terus berkembang, kerja sama ini menjadi krusial dalam mengimbangi pola ancaman baru. Dengan sinergi ini, deteksi dan penanggulangan kejahatan siber diharapkan lebih cepat, sehingga nasabah dapat merasa lebih aman. Namun, sejauh mana kolaborasi ini berjalan efektif di Indonesia dan seberapa cepat respons dari pihak terkait dalam menangani kasus-kasus skimming dan cyber crime adalah hal-hal yang perlu diteliti lebih lanjut.

2.1. Kendala Yang Dihadapi Dalam Penerapan Regulasi Untuk Melindungi Nasabah Dari Risiko Skimming Dan Cyber Crime

Penerapan regulasi untuk melindungi nasabah dari risiko skimming dan cyber crime di Indonesia, masih menunjukkan adanya sejumlah kendala yang sangat signifikan dan menghambat efektivitas kebijakan tersebut. Salah satu tantangan utama adalah lemahnya sistem pengawasan dan keamanan di sektor perbankan. Banyak bank yang masih menggunakan teknologi lama, seperti kartu berbasis magnetic stripe, yang lebih rentan terhadap skimming dibandingkan dengan kartu berbasis chip yang lebih aman. Meskipun Bank Indonesia telah mengeluarkan regulasi untuk mendorong penggunaan teknologi chip dan Personal Identification Number (PIN), implementasinya masih belum merata di seluruh lembaga keuangan. Selain itu, banyak mesin ATM yang tidak dilengkapi dengan perangkat keamanan tambahan, seperti kamera pengawas atau alarm, yang dapat membantu mendeteksi tindakan mencurigakan. Di samping itu, kurangnya edukasi dan kesadaran nasabah mengenai risiko skimming dan cyber crime juga berkontribusi pada masalah ini. Banyak pengguna layanan perbankan tidak menyadari pentingnya menjaga kerahasiaan informasi pribadi dan cara bertransaksi yang aman. Upaya edukasi yang dilakukan oleh bank sering kali tidak cukup untuk meningkatkan kesadaran nasabah tentang modus operandi pelaku skimming; banyak nasabah yang masih menggunakan PIN yang mudah ditebak atau tidak mengganti PIN secara berkala, sehingga mereka menjadi sasaran empuk bagi pelaku kejahatan.⁶

Masalah penegakan hukum juga merupakan kendala penting dalam perlindungan nasabah. Penegak hukum seringkali kurang memiliki pemahaman yang mendalam tentang teknologi informasi dan kesulitan dalam mengumpulkan bukti yang diperlukan untuk menuntut pelaku kejahatan siber. Proses investigasi terhadap kasus-kasus skimming bisa sangat rumit, terutama ketika pelaku beroperasi secara internasional atau menggunakan metode yang canggih untuk menyembunyikan jejak digital mereka. Kurangnya koordinasi

⁶Cecilia, L. & Adhari, A. (2023). Kebijakan Pencegahan Pencurian Data ATM (*Skimming*) Dalam Memberikan Perlindungan Terhadap Konsumen Perbankan di Indonesia. *Jurnal Kertha Semaya*. Vol. 11 No. 9 Tahun 2023.

antara lembaga penegak hukum dan sektor perbankan dalam menangani kasus-kasus *skimming* juga menghambat upaya penegakan hukum, membuat banyak kasus tidak terungkap atau tidak ditindaklanjuti dengan serius. Selain itu, ketidakcukupan regulasi itu sendiri menjadi tantangan besar dalam melindungi nasabah dari risiko *skimming* dan *cyber crime*. Meskipun ada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, implementasinya masih menghadapi berbagai hambatan. Regulasi yang ada sering kali tidak cukup komprehensif untuk mengatasi semua aspek kejahatan siber yang terus berkembang, sehingga menciptakan celah bagi pelaku kejahatan untuk melakukan aksinya. Banyak regulasi juga belum sepenuhnya diadaptasi untuk mencakup inovasi baru dalam teknologi finansial, seperti *fintech* dan bank digital, sehingga perlindungan terhadap nasabah menjadi kurang efektif.⁷

Keterbatasan sumber daya manusia di lembaga perbankan juga menjadi kendala signifikan dalam penerapan regulasi anti-*skimming*. Banyak bank tidak memiliki tim keamanan siber yang memadai atau kurangnya pelatihan bagi karyawan mengenai cara mendeteksi dan mencegah *skimming* serta *cyber crime* lainnya. Hal ini membuat bank kurang siap dalam menghadapi ancaman-ancaman baru yang muncul seiring dengan perkembangan teknologi. Selain itu, kurangnya investasi dalam teknologi keamanan canggih di sektor perbankan juga berkontribusi pada kerentanan sistem terhadap serangan siber. Secara keseluruhan, kendala-kendala ini menunjukkan bahwa meskipun ada regulasi yang ditetapkan untuk melindungi nasabah, implementasinya masih menghadapi banyak tantangan yang perlu diatasi agar perlindungan terhadap nasabah dari risiko *skimming* dan *cyber crime* dapat ditingkatkan secara efektif. Untuk mengatasi masalah ini, diperlukan kerjasama antara berbagai pihak terkait—termasuk pemerintah, lembaga penegak hukum, industri perbankan, dan masyarakat—dalam meningkatkan kesadaran akan risiko keamanan siber serta memperkuat regulasi dan sistem pengawasan. Dengan langkah-langkah tersebut, diharapkan perlindungan terhadap nasabah dapat ditingkatkan secara signifikan, menciptakan lingkungan perbankan yang lebih aman dan terpercaya bagi semua pihak.

3.1. Peran Otoritas Keuangan Dalam Meningkatkan Kesadaran Dan Edukasi Nasabah Terhadap Risiko *Skimming* Dan *Cyber Crime*

Otoritas Keuangan adalah lembaga independen yang bertugas mengatur dan mengawasi seluruh sektor jasa keuangan di Indonesia. Otoritas keuangan memiliki peran yang krusial dalam meningkatkan kesadaran dan edukasi nasabah terhadap risiko *skimming* dan kejahatan *cyber crime*. Lembaga ini, yang dikenal sebagai Otoritas Jasa Keuangan (OJK), didirikan berdasarkan Undang-Undang Nomor 21 Tahun 2011 dan mulai beroperasi pada 21 Juni 2011. OJK memiliki fungsi utama untuk memastikan bahwa kegiatan di sektor keuangan berlangsung secara teratur, adil, transparan, dan akuntabel, serta melindungi kepentingan konsumen di sektor jasa keuangan di Indonesia, termasuk perbankan, pasar modal, dan lembaga jasa keuangan non-bank. Berikut adalah beberapa langkah dan inisiatif yang diambil oleh otoritas keuangan, khususnya Otoritas Jasa Keuangan (OJK) antara lain :

a) Edukasi Nasabah

OJK berupaya meningkatkan pemahaman nasabah tentang risiko *skimming* dan *cyber crime* melalui berbagai program edukasi. Ini termasuk penyuluhan mengenai cara mengenali modus operandi *skimming* dan langkah-langkah pencegahan yang dapat diambil oleh nasabah untuk melindungi diri mereka. Misalnya, OJK mendorong penggunaan kartu ATM berbasis chip yang lebih aman dibandingkan dengan kartu magnetik.

b) Pengawasan dan Penegakan Hukum

OJK juga bertanggung jawab untuk melakukan pengawasan terhadap bank-bank dalam hal manajemen risiko keamanan sistem. Mereka meminta bank untuk secara rutin memeriksa mesin ATM dan memastikan tidak ada perangkat *skimmer* yang terpasang.

⁷Sari, D. Apriyani, R. & Damanik, A. (2024). Penegakan Hukum Pidana Terhadap Tindak Pidana *Skimming*. *Journal of Law and Nation (JOLN)*. Vol.3 No.1 Februari 2024.

Dalam kasus terjadinya kejahatan *skimming*, OJK mengharuskan bank untuk mengganti dana nasabah yang hilang akibat tindakan tersebut, sehingga memberikan perlindungan hukum bagi nasabah.

c) Kerjasama dengan Lembaga Penegak Hukum

OJK bekerja sama dengan aparat penegak hukum untuk menindaklanjuti kasus-kasus *skimming*. Ini termasuk penyelidikan terhadap pelaku kejahatan dan penerapan sanksi sesuai dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tentang kejahatan *cyber crime*. Dengan adanya kerjasama ini, diharapkan dapat menciptakan efek jera bagi pelaku kejahatan.

d) Peningkatan Keamanan Teknologi

OJK mendorong bank untuk mengadopsi teknologi keamanan yang lebih canggih, seperti sistem otentikasi dua faktor dan enkripsi data, untuk melindungi informasi nasabah dari pencurian. Selain itu, mereka juga memberikan panduan kepada nasabah tentang cara menjaga keamanan data pribadi saat bertransaksi secara online.

e) Penyuluhan tentang *E-Skimming*

Dengan munculnya *e-skimming*, OJK juga menyebarluaskan informasi mengenai metode baru ini kepada publik. *E-skimming* melibatkan pencurian data kartu kredit atau debit secara online melalui *malware* atau infeksi virus pada perangkat pengguna. OJK memberikan tips keamanan, seperti penggunaan antivirus dan pembaruan sistem secara berkala untuk melindungi perangkat dari serangan tersebut.

Melalui langkah-langkah ini, otoritas keuangan tidak hanya berperan dalam pengawasan dan penegakan hukum tetapi juga dalam menciptakan kesadaran di kalangan nasabah mengenai pentingnya keamanan finansial di era digital ini.⁸

KESIMPULAN

Perlindungan hukum bagi nasabah di Indonesia terhadap ancaman *skimming* dan kejahatan siber didukung oleh sejumlah regulasi seperti UUD 1945, UU Perlindungan Konsumen, UU OJK, dan UU P2SK. Meski regulasi ini menjamin hak nasabah, implementasinya masih menghadapi tantangan di lapangan. Banyak lembaga keuangan belum sepenuhnya menerapkan standar keamanan yang memadai, sementara penegakan hukum dan pengawasan oleh OJK dan BI perlu ditingkatkan. Kesadaran dan edukasi nasabah juga menjadi faktor penting dalam meningkatkan kewaspadaan terhadap ancaman ini.

Hambatan utama dalam penerapan regulasi mencakup lemahnya pengawasan, teknologi yang usang, dan kurangnya edukasi nasabah. Selain itu, keterbatasan sumber daya dan teknologi di bank memperburuk kondisi, ditambah dengan kurangnya pemahaman teknologi di kalangan penegak hukum. OJK memainkan peran penting dengan mengedukasi nasabah, mengawasi keamanan, dan bekerja sama dengan penegak hukum untuk menciptakan lingkungan keuangan yang aman. Kolaborasi antara pemerintah, bank, dan masyarakat sangat penting untuk meningkatkan efektivitas regulasi dan keamanan siber bagi nasabah.

DAFTAR PUSTAKA

- Cecilia, L. & Adhari, A. (2023). Kebijakan Pencegahan Pencurian Data ATM (*Skimming*) Dalam Memberikan Perlindungan Terhadap Konsumen Perbankan di Indonesia. *Jurnal Kertha Semaya*. Vol. 11 No. 9 Tahun 2023.
- Hardinata, M. Shanty. Sitohang, Y. Rahma, I. Utomo, S & Ramadoni, S. (2024). Sosialisasi Kebijakan Bank Digital Perlindungan Hukum Terhadap Data Nasabah Dari Risiko Serangan Siber. *RENATA : Jurnal Pengabdian Masyarakat Kita Semua*. Vol. 2 No. 2 Agustus 2024.
- Juita, S. Astanti, D. & Septiandani D. (2023). Perlindungan Hukum Terhadap Nasabah Bank Korban Kejahatan *Skimming*. *Jurnal USM Law Review* Vol. 6, No. 1, Tahun 2023.

⁸ Kartiko, N. D., Soegiono, S. P., Siswanto, C. A., & Indradewi, A. A. (2024). Perlindungan Konsumen Sektor Keuangan: Peran OJK dalam Menghadapi Ancaman Phising dan Skimming. *Iuris Studia: Jurnal Kajian Hukum*, 5(2), 347-363.

- Kartiko, N. D., Soegiono, S. P., Siswanto, C. A., & Indradewi, A. A. (2024). Perlindungan Konsumen Sektor Keuangan: Peran OJK dalam Menghadapi Ancaman Phising dan Skimming. *Iuris Studia: Jurnal Kajian Hukum*, 5(2), 347-363.
- Rumlus, M. & Hanif, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik. *Jurnal HAM*. Vol. 11, No. 2, Agustus 2020.
- Saly, J. & Nainggolan, J. (2023). Efektivitas Perlindungan Hukum Konsumen Berdasarkan Undang Undang Nomor 4 Tahun 2023 Tentang Pengembangan dan Penguatan Sektor Keuangan. *Jurnal Kewarganegaraan*. Vol. 7 No. 2 Desember 2023.
- Sari, D. Apriyani, R. & Damanik, A. (2024). Penegakan Hukum Pidana Terhadap Tindak Pidana Skimming. *Journal of Law and Nation (JOLN)*. Vol.3 No.1 Februari 2024
- Triansyah, R. Anadi, Y. & Faisol. (2024). Perlindungan Hukum Terhadap Nasabah Korban Skimming (Studi Kasus di Bank Rakyat Indonesia KCP Malinau Kalimantan Utara). *Jurnal DINAMIKA*. Volume 30 Nomor 2 Bulan Juli 2024.