JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.v5i6

Perlindungan Hukum terhadap Nasabah Akibat Pencurian Data Pribadi

Janto Chandra [1], Fajar Rachmad D. M. [2], Dhofirul Yahya[3]
[1] Universitas Maarif Hasyim Latif, Sidoarjo, Indonesia, janto_chandra@student.umaha.ac.id
[2] Universitas Maarif Hasyim Latif, Sidoarjo, Indonesia, janto_chandra@student.umaha.ac.id
[3] Universitas Maarif Hasyim Latif, Sidoarjo, Indonesia, janto_chandra@student.umaha.ac.id

Corresponding Author: janto_chandra@student.umaha.ac.id[1]

Abstract: *This study aims to analyze legal protection for bank customers who become victims of personal data theft through the skimming method within the context of banking law and personal data protection in Indonesia. Using a normative juridical approach, this research examines various relevant regulations, including the Banking Law, the Consumer Protection Law, the ITE Law, and the Personal Data Protection Law. The research findings indicate that although there is a sufficiently comprehensive normative foundation, the implementation of legal protection still faces various challenges, such as weak regulation harmonization, imbalance in the burden of proof, and the limitations of standards for compensation for victims. Legal protection for customers consists of preventive measures, such as the implementation of security technology, and repressive measures, such as compensation. This study recommends the need for regulatory reform and strengthening the roles of regulators and dispute resolution institutions to ensure more fair and effective protection for customers in the face of cybercrime.*

Keyword: *Legal protection, bank customers, personal data theft, banking regulations, ITE law.*

Abstrak: Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap nasabah bank yang menjadi korban pencurian data pribadi melalui modus *skimming* dalam konteks hukum perbankan dan perlindungan data pribadi di Indonesia. Menggunakan metode yuridis normatif, penelitian ini mengkaji berbagai peraturan perundang-undangan yang relevan, termasuk Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, Undang-Undang ITE, dan Undang-Undang Perlindungan Data Pribadi. Hasil penelitian menunjukkan bahwa meskipun terdapat landasan normatif yang cukup komprehensif, implementasi perlindungan hukum masih menghadapi berbagai kendala, seperti lemahnya harmonisasi regulasi, ketidakseimbangan dalam pembuktian, serta keterbatasan standar pemulihan kerugian bagi korban. Perlindungan hukum terhadap nasabah terdiri dari langkah preventif, seperti penerapan teknologi keamanan, dan langkah represif, seperti pemberian ganti rugi. Penelitian ini menyarankan perlunya reformasi regulasi dan penguatan peran regulator serta lembaga penyelesaian sengketa untuk memastikan perlindungan yang lebih adil dan efektif bagi nasabah dalam menghadapi kejahatan siber.

Kata Kunci: Perlindungan hukum, nasabah, pencurian data pribadi, regulasi perbankan, hukum ITE.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah paradigma pelayanan jasa keuangan di Indonesia. Salah satu perubahan signifikan terjadi dalam sektor perbankan, di mana digitalisasi sistem transaksi telah menjadi hal yang tak terpisahkan dari operasional perbankan. Penggunaan layanan seperti *mobile banking*, *internet banking*, dan Anjungan Tunai Mandiri (ATM) memudahkan nasabah dalam mengakses layanan perbankan kapan saja dan di mana saja. Namun, kemajuan teknologi ini juga membuka celah bagi tindak kejahatan siber. Salah satu bentuk kejahatan digital yang kerap terjadi di sektor perbankan adalah *skimming*. *Skimming* merupakan metode pencurian data pada kartu ATM atau kartu kredit dengan menggunakan alat khusus yang mampu menyalin informasi magnetik secara ilegal. Data yang diperoleh kemudian digunakan untuk membobol rekening nasabah (Linggoharjo, 2020).

Kasus *skimming* kerap terjadi tanpa disadari oleh nasabah. Transaksi ilegal yang dilakukan oleh pelaku sering kali baru diketahui setelah dana nasabah telah terkuras. Hal ini menunjukkan lemahnya sistem perlindungan hukum dan teknologi perbankan dalam mengantisipasi kejahatan digital yang semakin canggih dan kompleks. Perlindungan hukum terhadap nasabah yang menjadi korban kejahatan perbankan seperti *skimming* menjadi isu penting dalam kerangka perlindungan konsumen dan hukum perbankan. Bank sebagai lembaga keuangan memiliki kewajiban hukum dan moral untuk menjaga keamanan data pribadi nasabah dan bertanggung jawab atas kerugian yang timbul dari kelalaian sistem keamanannya (Usman, 2001).

Menurut Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, bank wajib menjaga kepercayaan masyarakat dengan menjamin kerahasiaan dan keamanan dana serta data pribadi nasabah. Hal ini juga ditegaskan dalam berbagai regulasi Otoritas Jasa Keuangan (OJK) dan Peraturan Bank Indonesia (PBI) yang mewajibkan setiap penyelenggara sistem pembayaran dan layanan keuangan untuk menerapkan prinsip kehati-hatian dan perlindungan konsumen (PBI No. 16/1/PBI/2014). Dalam konteks perlindungan konsumen, Undang-Undang Nomor 8 Tahun 1999 memberikan perlindungan terhadap hak-hak nasabah sebagai konsumen. Pasal 4 UU tersebut menegaskan hak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa. Jika bank sebagai pelaku usaha gagal memenuhi standar keamanan sistem, maka secara hukum mereka dapat dimintai pertanggungjawaban (Kristiyanti, 2011).

Hartono (2007) menyatakan bahwa setiap pelaku usaha bertanggung jawab atas kerugian konsumen jika kerugian tersebut disebabkan oleh produk atau jasa yang tidak aman. Dalam konteks perbankan, ATM sebagai produk teknologi yang disediakan bank harus memenuhi standar keamanan tertinggi. Kegagalan dalam mencegah terjadinya *skimming* dapat dianggap sebagai kelalaian pihak bank dalam menjamin keamanan sistemnya. Di sisi lain, keberadaan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) turut memperkuat perlindungan hukum terhadap nasabah. UU ini mengatur larangan akses ilegal terhadap sistem elektronik serta pencurian data pribadi secara digital. Namun, penegakan hukum terhadap pelaku cybercrime seperti *skimming* masih menghadapi banyak tantangan, terutama terkait dengan pembuktian teknis dan keberadaan pelaku yang sering berada di luar yurisdiksi hukum nasional (Chazawi, 2015). Dalam ranah perlindungan data pribadi, Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini mewajibkan setiap pengendali data, termasuk bank, untuk menjaga integritas dan kerahasiaan data pribadi nasabah. Namun, Suryanto (2024) menilai bahwa

implementasi UU PDP masih belum optimal dalam konteks industri perbankan, terutama dalam hal pengawasan dan penegakan sanksi.

Beberapa studi sebelumnya telah mengkaji perlindungan hukum terhadap nasabah dalam konteks layanan perbankan digital. Misalnya, Yulianti (2020) menyoroti peran OJK dalam mengawasi lembaga keuangan dan memberikan perlindungan kepada nasabah korban kejahatan *skimming*. Namun, kajian tersebut lebih menekankan aspek kelembagaan dan belum menggali secara mendalam aspek tanggung jawab hukum bank terhadap nasabah dari perspektif hukum pidana dan perdata. Di sisi lain, Astrini (2015) meneliti bentuk perlindungan hukum terhadap pengguna internet banking, dan menekankan pentingnya tanggung jawab bank dalam memastikan keamanan teknologi dan kebijakan privasi. Namun, tanggung jawab bank dalam konteks *skimming* yang lebih spesifik belum banyak dikaji secara mendalam dari sudut pandang hubungan kontraktual dan tanggung gugat hukum.

Studi oleh Tarigan dkk. (2019) menambahkan bahwa perlindungan preventif dan represif terhadap nasabah digital banking memerlukan penguatan regulasi dan pengawasan. Namun, mekanisme pemulihan kerugian bagi nasabah akibat kegagalan sistem keamanan masih menjadi titik lemah yang belum banyak dibahas secara rinci dalam literatur hukum perbankan di Indonesia. Kelemahan dalam perlindungan hukum ini diperparah oleh ketidakseimbangan posisi tawar antara bank dan nasabah. Hubungan antara keduanya yang bersifat kontraktual sering kali merugikan nasabah karena klausul-klausul baku yang dibuat sepihak oleh bank. Hal ini menempatkan nasabah dalam posisi rentan ketika terjadi kegagalan sistem atau kejahatan digital seperti *skimming*. Permasalahan ini menunjukkan perlunya evaluasi terhadap efektivitas hukum yang ada dalam memberikan perlindungan nyata kepada nasabah. Selain itu, bank juga perlu melakukan peningkatan kualitas sistem keamanan serta menerapkan prinsip tanggung gugat yang lebih kuat dan transparan kepada nasabah.

Berdasarkan latar belakang tersebut, artikel ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap nasabah korban pencurian data melalui modus *skimming*, serta mengevaluasi efektivitas dan kecukupan regulasi yang berlaku. Pendekatan yuridis normatif akan digunakan dengan penekanan pada analisis peraturan perundang-undangan, putusan pengadilan, dan literatur hukum. Penelitian ini diharapkan dapat memberikan kontribusi baik secara teoritis dalam pengembangan studi hukum perbankan dan perlindungan data pribadi, maupun secara praktis bagi lembaga perbankan dan regulator dalam menyusun kebijakan perlindungan data yang lebih responsif dan berkeadilan.

METODE

Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan yang bertumpu pada analisis terhadap norma-norma hukum yang berlaku. Pendekatan ini digunakan untuk mengkaji perlindungan hukum terhadap nasabah bank sebagai korban pencurian data pribadi melalui modus *skimming*, berdasarkan peraturan perundang-undangan, doktrin hukum, serta putusan pengadilan yang relevan. Penelitian yuridis normatif bersifat konseptual dan teoritis, dengan tujuan mengidentifikasi dan menafsirkan norma-norma hukum yang mengatur tanggung jawab bank serta hak-hak hukum nasabah.

Pendekatan normatif dalam penelitian ini juga dikombinasikan dengan pendekatan konseptual dan pendekatan perundang-undangan (*statute approach*). Pendekatan konseptual digunakan untuk memahami konsep perlindungan hukum, data pribadi, dan hubungan kontraktual antara bank dan nasabah, sementara pendekatan perundang-undangan digunakan untuk menganalisis berbagai regulasi yang terkait, seperti Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Sumber bahan hukum yang digunakan dalam penelitian ini terdiri atas tiga jenis. Pertama, bahan hukum primer, yaitu peraturan perundang-undangan yang berlaku di Indonesia terkait hukum perbankan dan perlindungan data pribadi. Kedua, bahan hukum sekunder, berupa literatur hukum seperti buku teks, jurnal ilmiah, artikel hukum, dan pendapat para ahli hukum yang mendukung analisis terhadap bahan hukum primer. Ketiga, bahan hukum tersier, seperti kamus hukum, ensiklopedia, dan sumber lain yang membantu menjelaskan istilah-istilah hukum yang digunakan dalam penelitian.

Pengumpulan data dilakukan melalui metode studi kepustakaan (*library research*), yaitu dengan menelaah dokumen-dokumen hukum, peraturan, dan putusan pengadilan yang relevan. Studi pustaka memungkinkan peneliti untuk memperoleh pemahaman yang komprehensif terhadap praktik dan perkembangan perlindungan hukum bagi nasabah di tengah meningkatnya kejahatan siber, khususnya pencurian data melalui *skimming*. Data yang telah dikumpulkan kemudian dianalisis secara kualitatif normatif, yaitu dengan cara mengkaji isi normatif dari peraturan perundang-undangan dan dokumen hukum lainnya, serta menilai kesesuaiannya dengan prinsip-prinsip hukum perlindungan konsumen dan perlindungan data pribadi. Analisis dilakukan dengan sistematika argumentatif, yaitu mengaitkan antara teori, norma, dan praktik hukum yang berlaku.

HASIL DAN PEMBAHASAN

Bentuk Perlindungan Hukum oleh Bank terhadap Nasabah Korban Pencurian Data

Skimming merupakan kejahatan siber yang menargetkan data pribadi nasabah melalui pencurian data dari kartu ATM atau debit menggunakan perangkat tersembunyi. Dalam konteks ini, nasabah sebagai konsumen berhak atas perlindungan hukum berdasarkan Pasal 4 huruf a, b, dan c Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen, yang menegaskan hak atas kenyamanan, keamanan, dan keselamatan dalam mengonsumsi jasa. Sementara Pasal 19 ayat (1) menyebutkan bahwa pelaku usaha wajib bertanggung jawab atas kerugian akibat produk atau jasa yang digunakan. Dalam konteks perjanjian antara bank dan nasabah, Pasal 1320 KUHPerdata menjelaskan syarat sahnya perjanjian, yaitu sepakat, cakap, hal tertentu, dan sebab yang halal, sedangkan Pasal 1338 KUHPerdata menegaskan bahwa setiap perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi para pihak. Artinya, bank wajib memenuhi janjinya termasuk perlindungan data pribadi nasabah.

Undang-Undang No. 10 Tahun 1998 tentang Perbankan dalam Pasal 40 mewajibkan bank menjaga kerahasiaan data nasabah. Pelanggaran atas kewajiban ini dapat dikenai sanksi sebagaimana tercantum dalam Pasal 47 dan 47A. Dalam kasus pencurian data pribadi melalui skimming, jika ditemukan kelalaian sistemik pada sistem keamanan bank, maka bank tetap dapat dimintai pertanggungjawaban. Dalam perspektif perlindungan konsumen, prinsip tanggung jawab objektif (*strict liability*) sebagaimana dikemukakan oleh Hartono (2007) harus diterapkan. Prinsip ini menyatakan bahwa pelaku usaha bertanggung jawab atas kerugian yang dialami konsumen tanpa harus dibuktikan kesalahannya jika produk/jasa yang ditawarkan cacat atau tidak aman. ATM atau sistem perbankan yang gagal melindungi data nasabah dapat dikategorikan sebagai produk yang tidak aman.

Perlindungan hukum terbagi menjadi dua, yaitu preventif dan represif. Perlindungan preventif mencakup penggunaan teknologi keamanan seperti chip EMV, OTP, sistem enkripsi data, serta edukasi kepada nasabah. Menurut Yulianti (2020), penguatan sistem keamanan perlu didukung dengan audit teknologi secara berkala. Pendapat ini mempertegas perlunya kebijakan perlindungan menyeluruh sejak awal. Perlindungan represif melibatkan investigasi internal oleh bank, kerja sama dengan penegak hukum, pemberian ganti rugi kepada nasabah, serta mekanisme pengaduan yang efektif sebagaimana diatur dalam POJK No. 1/POJK.07/2013 dan PBI No. 16/1/PBI/2014. Dalam praktiknya, banyak bank berupaya melepaskan tanggung jawab dengan dalih otorisasi PIN. Namun, pendekatan ini tidak dapat

diterima jika ditemukan bahwa sistem bank memiliki celah keamanan yang disengaja maupun lalai. Konsep keadilan restoratif relevan untuk memberikan perlindungan lebih menyeluruh. Keadilan restoratif adalah pendekatan hukum yang berfokus pada pemulihan korban dan tanggung jawab pelaku secara moral dan sosial, bukan sekadar hukuman pidana. Dalam hal ini, bank perlu berperan aktif dalam memulihkan kerugian nasabah serta mengembalikan kepercayaan publik.

Perlindungan hukum terhadap nasabah bank korban pencurian data pribadi melalui kejahatan *skimming* merupakan bagian dari kewajiban hukum bank dalam menjaga hak-hak nasabah sebagai konsumen jasa keuangan. Dalam sistem hukum Indonesia, nasabah bank berada dalam posisi sebagai konsumen yang menggunakan jasa dari pelaku usaha, dalam hal ini institusi perbankan, sebagaimana didefinisikan dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Oleh karena itu, nasabah berhak atas rasa aman, keadilan, dan kompensasi ketika mengalami kerugian akibat kelalaian penyedia jasa keuangan. Hubungan hukum antara nasabah dan bank merupakan hubungan perdata yang didasarkan pada perjanjian, terutama perjanjian simpanan atau penggunaan layanan elektronik. Dalam hubungan ini, bank berkewajiban untuk melindungi informasi rahasia milik nasabah, termasuk data pribadi dan transaksi keuangan. Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dengan tegas mewajibkan bank untuk merahasiakan informasi terkait nasabah, dan pelanggaran terhadap kewajiban ini dapat dikenakan sanksi hukum. Dalam konteks *skimming*, meskipun data nasabah dicuri oleh pihak ketiga, tanggung jawab bank tidak dapat serta merta dilepaskan apabila terdapat unsur kelalaian sistemik.

Menurut Usman (2001), bank sebagai lembaga kepercayaan masyarakat harus menjamin keamanan informasi dan sistem yang digunakannya. Hal ini menjadi dasar bagi konsep perlindungan hukum preventif, yaitu segala upaya yang dilakukan bank untuk mencegah terjadinya pelanggaran atau kerugian terhadap nasabah. Perlindungan preventif ini mencakup penerapan teknologi keamanan seperti chip EMV, OTP (*One Time Password*), dan sistem enkripsi data yang memadai. Selain itu, penyuluhan kepada nasabah tentang potensi modus kejahatan perbankan juga menjadi bagian dari tanggung jawab preventif. Namun demikian, perlindungan tidak hanya berhenti pada tahap pencegahan. Ketika nasabah telah menjadi korban kejahatan *skimming*, maka perlindungan hukum yang dibutuhkan adalah perlindungan represif. Perlindungan represif merujuk pada tanggung jawab bank untuk menindaklanjuti laporan nasabah, melakukan investigasi internal, bekerja sama dengan aparat penegak hukum, serta memberikan ganti rugi apabila ditemukan bahwa kegagalan sistem keamanan bank berkontribusi terhadap kerugian nasabah (Kristiyanti, 2011). Pelaksanaan perlindungan represif oleh bank masih menghadapi berbagai persoalan. Banyak bank menggunakan alasan bahwa transaksi dilakukan secara sah dengan memasukkan PIN yang hanya diketahui nasabah, sehingga mengalihkan seluruh tanggung jawab kepada korban. Padahal, menurut Hartono (2007), prinsip tanggung jawab objektif (*strict liability*) dalam perlindungan konsumen menuntut pelaku usaha tetap bertanggung jawab meskipun tidak ada unsur kesalahan langsung, apabila produk atau jasa yang digunakannya menimbulkan kerugian.

Pada aspek regulasi teknis, Peraturan OJK No. 1/POJK.07/2013 dan Peraturan Bank Indonesia No. 16/1/PBI/2014 mewajibkan bank menyediakan mekanisme pengaduan dan penyelesaian sengketa secara internal, serta memberikan akses kepada nasabah terhadap mediasi atau lembaga penyelesaian sengketa eksternal. Namun efektivitas aturan ini sangat bergantung pada responsif dan itikad baik bank dalam menanggapi laporan nasabah. Tidak sedikit kasus pengaduan nasabah yang berakhir tanpa penyelesaian yang memuaskan karena proses yang panjang dan minim transparansi. Putusan pengadilan menunjukkan adanya keberagaman pendekatan dalam menentukan tanggung jawab bank. Sebagian hakim menegaskan bahwa bank tetap bertanggung jawab atas kelalaian sistem yang memungkinkan terjadinya pencurian data, meskipun dilakukan oleh pihak ketiga. Namun di sisi lain, ada pula

putusan yang membebaskan bank dari tanggung jawab dengan alasan bahwa nasabah tidak cukup cermat menjaga PIN atau informasi pribadinya. Hal ini menunjukkan adanya celah dalam perlindungan hukum, terutama terkait standar pembuktian dan beban tanggung jawab.

Yulianti (2020) menjelaskan bahwa perlindungan hukum terhadap nasabah melalui pengawasan OJK (Otoritas Jasa Keuangan) masih bersifat normatif dan belum efektif secara substansial. Hal ini menunjukkan bahwa meskipun regulasi yang ada sudah cukup mengatur, implementasinya dalam praktik belum mampu memberikan perlindungan maksimal kepada nasabah, terutama dalam menghadapi ancaman kejahatan siber seperti skimming. Perlindungan hukum yang ideal tidak hanya membutuhkan regulasi yang baik, tetapi juga mekanisme penegakan yang adil, transparan, dan aksesibel bagi nasabah. Dalam konteks ini, pendekatan keadilan restoratif bisa menjadi solusi yang relevan. Dalam pendekatan ini, tidak hanya bank yang berperan dalam melindungi kepentingan kelembagaannya, tetapi juga bertanggung jawab untuk memulihkan kerugian nasabah dan mengembalikan kepercayaan yang hilang akibat kejadian tersebut. Secara normatif, perlindungan hukum terhadap korban kejahatan skimming harus dilihat dalam kerangka yang lebih luas, yakni perlindungan hak-hak konsumen dan hak atas data pribadi. Perlindungan ini mencakup beberapa dimensi, antara lain hak atas keamanan data pribadi nasabah, hak untuk mendapatkan transparansi mengenai penggunaan dan pengelolaan data, serta hak untuk berpartisipasi dalam pengawasan terhadap layanan keuangan digital yang mereka gunakan. Selain itu, hak untuk memperoleh pemulihan yang adil dan efektif juga merupakan bagian yang tak terpisahkan dari perlindungan hukum yang seharusnya diberikan kepada nasabah yang dirugikan.

Selain regulasi yang lebih tegas dan jelas, penguatan sistem keamanan teknologi di sektor perbankan juga menjadi faktor penting dalam upaya perlindungan ini. Implementasi teknologi yang lebih canggih, seperti enkripsi data yang lebih kuat dan penggunaan autentikasi ganda, akan memperkecil peluang terjadinya kejahatan skimming. Tak kalah penting, komitmen etis lembaga keuangan dalam menjaga data pribadi nasabah harus ditingkatkan, di mana bank tidak hanya melihat aspek keuntungan semata, tetapi juga memperhatikan aspek perlindungan hak-hak nasabah. Oleh karena itu, penguatan regulasi, peningkatan sistem keamanan teknologi, serta komitmen etis yang lebih kuat dari lembaga-lembaga keuangan menjadi kunci untuk menciptakan perlindungan hukum yang tidak hanya ada di atas kertas, tetapi juga dapat memberikan perlindungan yang nyata dan efektif bagi nasabah dalam menghadapi ancaman kejahatan siber di era digital ini. Regulasi yang lebih responsif terhadap perkembangan teknologi serta pendekatan yang melibatkan semua pemangku kepentingan dalam ekosistem keuangan digital akan memastikan bahwa nasabah mendapatkan perlindungan yang memadai dan keadilan yang seimbang.

Peraturan Perundang-Undangan dalam Memberikan Perlindungan Hukum terhadap Nasabah Korban Pencurian Data

Peraturan perundang-undangan yang ada saat ini di Indonesia pada prinsipnya telah menyediakan kerangka hukum yang cukup luas dalam upaya melindungi nasabah dari risiko pencurian data pribadi. Regulasi tersebut mencakup aspek perbankan, perlindungan konsumen, transaksi elektronik, dan perlindungan data pribadi. Namun, pertanyaan penting yang muncul adalah apakah peraturan-peraturan tersebut sudah memadai dalam menjamin perlindungan hukum secara nyata, efektif, dan berkeadilan bagi nasabah, khususnya korban *skimming*. Dalam sistem hukum nasional, perlindungan hukum terhadap nasabah didasarkan pada beberapa norma utama. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mewajibkan bank untuk menjaga kerahasiaan data nasabah sebagai bagian dari prinsip kepercayaan dalam hubungan fiduciary. Akan tetapi, undang-undang ini belum memberikan ruang yang cukup luas dalam menjabarkan tanggung jawab bank ketika terjadi kebocoran data atau kejahatan siber yang berdampak pada kerugian finansial nasabah. Perlindungan hukum

dalam undang-undang ini masih berfokus pada tanggung jawab konvensional, bukan pada kompleksitas era digital.

Perlindungan hukum terhadap nasabah korban pencurian data dalam konteks skimming diatur dalam berbagai peraturan perundang-undangan di Indonesia. Undang-Undang No. 10 Tahun 1998 tentang Perbankan memberikan dasar hukum yang kuat melalui Pasal 40 yang mewajibkan bank menjaga kerahasiaan nasabah, dan Pasal 47 serta 47A yang mengatur sanksi atas pelanggaran tersebut. Selain itu, Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen secara eksplisit menjamin hak konsumen melalui Pasal 4, yang mencakup hak atas kenyamanan, keamanan, dan keselamatan dalam mengonsumsi jasa, serta Pasal 19 yang mengatur kewajiban pelaku usaha untuk memberikan ganti rugi atas kerugian yang timbul. KUH Perdata juga memberikan fondasi normatif yang penting, khususnya Pasal 1320 tentang syarat sahnya perjanjian dan Pasal 1338 tentang asas kebebasan berkontrak, yang menjadi dasar hubungan hukum antara bank dan nasabah. Dalam konteks kejahatan digital, Undang-Undang No. 11 Tahun 2008 jo. No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) mengatur perbuatan melawan hukum digital, seperti akses ilegal (Pasal 30) dan manipulasi data elektronik (Pasal 32).

Penguatan perlindungan terhadap data pribadi nasabah semakin relevan dengan diberlakukannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pasal 4 UU PDP menjelaskan hak subjek data, termasuk hak untuk memperoleh informasi, akses, dan pemulihan atas data pribadinya, sedangkan Pasal 67 dan 68 memberikan ancaman sanksi bagi pengendali data yang melanggar ketentuan hukum tersebut. Di sisi lain, POJK No. 1/POJK.07/2013 dan PBI No. 16/1/PBI/2014 menetapkan kewajiban bank dalam menyediakan mekanisme pengaduan dan perlindungan konsumen. Namun demikian, implementasi dari peraturan-peraturan tersebut dalam praktik masih jauh dari ideal. Banyak bank yang menerapkan klausul sepihak dalam perjanjian layanan yang membatasi hak nasabah untuk memperoleh ganti rugi, dan memindahkan seluruh beban tanggung jawab kepada nasabah melalui asumsi validitas PIN. Hal ini bertentangan dengan prinsip keadilan dan asas proporsionalitas dalam perlindungan konsumen. Negara-negara maju seperti Inggris dan Jerman telah menerapkan prinsip "reversed burden of proof," di mana bank diwajibkan membuktikan bahwa sistem keamanannya tidak mengalami kegagalan dalam mencegah skimming.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen mengandung prinsip tanggung gugat pelaku usaha atas kerugian yang diderita konsumen akibat produk atau jasa yang cacat. Dalam kasus *skimming*, kartu ATM atau sistem elektronik bank yang gagal melindungi data nasabah dapat dikategorikan sebagai produk yang tidak aman. Namun, dalam praktiknya, jarang ditemukan kasus di mana bank dimintai pertanggungjawaban perdata secara penuh berdasarkan UU Perlindungan Konsumen, karena dominannya pendekatan kontraktual dan standar baku yang merugikan posisi tawar nasabah (Hartono, 2007). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan perubahannya melalui UU No. 19 Tahun 2016, memang telah mengatur perbuatan pidana seperti akses ilegal, manipulasi data elektronik, dan pencurian identitas digital. Namun, fokus utama undang-undang ini lebih kepada penindakan pidana terhadap pelaku, bukan pada perlindungan dan pemulihan korban. Dalam banyak kasus, nasabah kesulitan menuntut bank melalui kerangka UU ITE, karena kejahatan dilakukan oleh pihak ketiga yang sulit diidentifikasi atau ditangkap, sementara bank kerap lepas dari tanggung jawab karena mengklaim sistemnya telah sesuai prosedur.

Indonesia baru mengadopsi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pada tahun 2022, yang secara khusus mengatur hak subjek data dan kewajiban pengendali data, termasuk lembaga keuangan. UU PDP merupakan tonggak penting karena memberikan dasar hukum atas hak privasi warga negara dalam lingkup

digital, serta menetapkan sanksi administratif dan pidana atas pelanggaran. Namun, implementasi UU ini masih dalam tahap transisi, dengan beberapa ketentuan pelaksanaannya masih menunggu peraturan turunan dan kesiapan institusional, baik dari sisi teknologi maupun sumber daya manusia (Suryanto, 2024). Di samping itu, regulasi sektoral juga telah mencoba mengisi celah perlindungan. Peraturan Bank Indonesia dan Otoritas Jasa Keuangan memberikan pedoman teknis mengenai tata kelola risiko dan perlindungan konsumen. Misalnya, PBI No. 16/1/PBI/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran dan POJK No. 1/POJK.07/2013 tentang Mekanisme Pengaduan Konsumen. Namun, regulasi ini cenderung lebih menekankan aspek administratif dan prosedural, bukan pada aspek substantif seperti hak atas ganti rugi, restitusi, atau perlindungan hukum dalam proses peradilan.

Fakta di lapangan menunjukkan bahwa banyak bank menggunakan ketentuan syarat dan ketentuan penggunaan kartu sebagai dasar untuk membebaskan diri dari tanggung jawab. Misalnya, dengan menyatakan bahwa "transaksi yang menggunakan PIN dianggap sah dilakukan oleh pemilik rekening". Hal ini menyulitkan korban *skimming* untuk menuntut haknya karena sistem hukum dan kontraktual seolah-olah telah membatasi upaya hukum mereka sejak awal. Ketentuan semacam ini memperlihatkan kekosongan hukum dalam menjamin prinsip proporsionalitas dan perlindungan pihak yang lebih lemah secara posisi hukum. Salah satu tantangan besar dalam implementasi perlindungan hukum terhadap nasabah adalah sistem pembuktian. Dalam hukum perdata, beban pembuktian berada pada pihak penggugat, yaitu nasabah. Padahal, dalam kasus *skimming*, nasabah tidak memiliki akses terhadap sistem keamanan internal bank untuk membuktikan adanya kebocoran atau kelemahan sistem. Dalam praktik global, beberapa negara seperti Inggris dan Jerman menerapkan prinsip *reversed burden of proof* dalam konteks perlindungan konsumen digital, dimana bank wajib membuktikan bahwa sistemnya aman dan tidak terjadi pelanggaran (European Union GDPR, 2016).

Sisi kebijakan perlu dikritisi lebih lanjut, terutama terkait dengan belum adanya standar kompensasi nasional yang wajib diikuti oleh semua bank dalam kasus kejahatan digital. Meskipun beberapa bank besar telah memiliki prosedur internal yang lebih cepat dan bersahabat, yang memudahkan proses klaim dan pemulihan bagi nasabah korban kejahatan *skimming* atau pencurian data, kenyataannya tidak semua bank memiliki kebijakan yang serupa. Ketimpangan perlakuan ini menciptakan ketidakadilan yang merugikan nasabah secara struktural, terutama bagi mereka yang berada di wilayah dengan akses terbatas terhadap informasi, layanan digital, dan bantuan hukum. Nasabah di daerah terpencil atau dengan tingkat literasi digital rendah sering kali menghadapi kesulitan dalam mendapatkan perlindungan yang memadai. Hal ini memperburuk ketimpangan sosial dan ekonomi dalam sektor perbankan, yang seharusnya memberikan perlindungan yang adil bagi seluruh lapisan masyarakat. Secara teoritik, pendekatan hukum yang diterapkan saat ini masih berorientasi pada respons pasif. Hukum hadir hanya setelah kejahatan terjadi, yang menunjukkan bahwa regulasi yang ada lebih fokus pada penanganan akibat daripada pencegahan dan upaya preventif. Pendekatan ini tidak cukup untuk mendorong tanggung jawab preventif yang sistematis dari bank, yang seharusnya lebih proaktif dalam menjaga keamanan nasabah dari potensi kejahatan digital. Hukum yang berfokus pada respons pasif tidak mendorong bank untuk melakukan tindakan yang lebih holistik dalam mencegah kejahatan sejak awal. Sebagai contoh, bank sering kali hanya mengimplementasikan sistem keamanan setelah terjadi insiden, bukannya berusaha mengidentifikasi dan mengurangi potensi ancaman sebelum hal tersebut terjadi.

Dalam konteks perlindungan konsumen dan data pribadi, perlu ada perubahan paradigma dalam pendekatan regulasi yang diterapkan. Pendekatan *precautionary* (berhati-hati) dan *responsibility-based regulation* (berbasis tanggung jawab) harus diterapkan secara lebih luas. Dalam pendekatan precautionary, bank dan penyedia layanan digital diwajibkan untuk menilai

dan mengidentifikasi potensi risiko sejak dini serta mengambil langkah-langkah mitigasi untuk mencegah kerugian sebelum terjadi. Misalnya, dalam pengembangan produk dan layanan digital, bank harus mengintegrasikan prinsip *privacy by design*, di mana perlindungan data pribadi sudah dipertimbangkan dan diterapkan sejak tahap perancangan produk. Ini berarti bahwa sistem keamanan dan kebijakan privasi harus menjadi bagian integral dari desain produk, bukan tambahan yang dipikirkan setelah produk tersebut diluncurkan. Dengan menerapkan prinsip *privacy by design*, bank tidak hanya mematuhi regulasi yang ada, tetapi juga bertanggung jawab untuk memastikan bahwa produk dan layanan mereka tidak hanya aman secara teknis, tetapi juga mempertimbangkan aspek perlindungan data pribadi nasabah sejak awal. Hal ini juga mencakup upaya yang lebih besar untuk memastikan bahwa risiko terkait dengan data nasabah selalu dipantau, diidentifikasi, dan dikelola secara berkelanjutan.

Penerapan standar kompensasi yang jelas dan nasional di Indonesia juga menjadi langkah penting untuk memastikan perlindungan yang lebih merata bagi nasabah. Standar ini dapat mencakup prosedur yang jelas dalam hal pemulihan kerugian akibat kejahatan digital, serta batas waktu yang tegas bagi bank untuk menyelesaikan klaim dan memberikan kompensasi. Dengan adanya standar yang mengikat, bank di seluruh Indonesia akan memiliki pedoman yang sama dalam memberikan perlindungan kepada nasabah, mengurangi ketimpangan dalam perlakuan dan memberikan kepastian hukum bagi nasabah yang menjadi korban. Dengan demikian, untuk menciptakan perlindungan hukum yang lebih adil dan efektif bagi nasabah dalam menghadapi kejahatan digital, diperlukan langkah-langkah yang tidak hanya reaktif, tetapi juga proaktif dan sistematis. Penyedia jasa keuangan, khususnya bank, harus lebih bertanggung jawab atas perlindungan data pribadi dan harus memiliki kebijakan yang lebih komprehensif dalam pencegahan dan penanggulangan kejahatan siber.

Meskipun peraturan perundang-undangan yang ada telah mencakup aspek perlindungan nasabah secara luas, kenyataannya peraturan tersebut belum sepenuhnya memadai dalam praktik. Salah satu masalah utama terletak pada aspek harmonisasi regulasi yang masih lemah, yang menyebabkan ketidaksesuaian antar peraturan dan penerapannya yang tidak konsisten. Selain itu, keberanian dalam penegakan hukum juga masih sering terkendala oleh berbagai faktor, seperti keterbatasan sumber daya dan ketidakjelasan dalam penuntutan, yang mengurangi efektivitas perlindungan hukum bagi nasabah (Kristiyanti, 2011; Sidabalok, 2014). Perlindungan korban dalam proses peradilan juga sering kali tidak maksimal, baik dari segi akses yang terbatas maupun proses yang memakan waktu lama, yang pada akhirnya menambah beban psikologis dan finansial bagi korban (Soekanto, 1986).

Minimnya instrumen pemulihan yang tegas dan cepat menjadi salah satu kendala utama dalam memastikan keadilan bagi korban. Proses pemulihan yang lambat dan tidak transparan menambah kesulitan bagi nasabah yang terdampak kejahatan siber, terutama dalam hal penggantian kerugian atau pemulihan data pribadi yang hilang atau disalahgunakan (Djumhana, 1993; Ginting, 2008). Oleh karena itu, untuk menjawab tantangan ini, Indonesia perlu menyusun kebijakan nasional yang berbasis teknologi digital yang lebih integratif dan responsif terhadap kejahatan siber. Kebijakan ini harus mampu mengakomodasi perkembangan pesat dalam dunia teknologi informasi dan transaksi digital, serta memberikan solusi yang cepat dan efisien bagi korban (Usman, 2001). Selain itu, revisi terhadap peraturan kontraktual yang tidak seimbang antara bank dan nasabah juga sangat diperlukan. Banyak perjanjian yang ada saat ini cenderung lebih menguntungkan pihak bank dan memberikan sedikit ruang bagi nasabah untuk memperjuangkan hak-haknya, terutama dalam konteks perlindungan data pribadi dan kejahatan siber. Revisi ini harus mencakup klausul yang lebih mengutamakan keadilan bagi nasabah, memastikan bahwa hak-hak konsumen tetap terlindungi meskipun dalam ketidakseimbangan posisi kontraktual (Usman, 2001; Hartono, 2007).

Penguatan lembaga mediasi dan arbitrase perbankan yang benar-benar independen dan berpihak pada keadilan konsumen juga harus menjadi fokus utama. Lembaga-lembaga ini

harus mampu memberikan ruang bagi penyelesaian sengketa secara adil dan efisien, tanpa adanya keberpihakan pada salah satu pihak, terutama pihak yang memiliki kekuatan lebih besar seperti bank (Andreae, 1977; Sjahdeini, 1993). Mediasi dan arbitrase yang efektif dapat membantu mengurangi beban peradilan yang sering kali lambat dan mahal, serta memberikan solusi yang lebih cepat bagi nasabah yang dirugikan. Dengan demikian, perlindungan hukum yang lebih efektif bagi nasabah, khususnya dalam menghadapi kejahatan siber, membutuhkan pembaruan regulasi yang lebih komprehensif, serta penegakan hukum yang lebih berani dan tegas. Penguatan lembaga penyelesaian sengketa dan penyesuaian terhadap kontrak-kontrak yang tidak adil akan menciptakan iklim yang lebih adil dan memberikan perlindungan yang maksimal bagi nasabah dalam menghadapi ancaman digital di era modern ini.

KESIMPULAN

Perlindungan hukum terhadap nasabah bank yang menjadi korban pencurian data pribadi melalui kejahatan skimming merupakan bagian dari tanggung jawab hukum dan sosial institusi perbankan dalam era digital. Hubungan antara bank dan nasabah bersifat kontraktual, sehingga tunduk pada ketentuan Pasal 1320 dan Pasal 1338 KUHPerdata. Di sisi lain, bank juga memiliki kewajiban fiduciary untuk menjaga kerahasiaan dan keamanan data nasabah sebagaimana diatur dalam Pasal 40 Undang-Undang No. 10 Tahun 1998 tentang Perbankan, dan pengaturannya diperkuat dengan sanksi dalam Pasal 47 dan 47A. Bentuk perlindungan hukum yang diberikan kepada nasabah terbagi menjadi dua, yakni perlindungan preventif dan represif. Perlindungan preventif dilakukan melalui penggunaan teknologi keamanan seperti chip EMV, OTP, dan sistem enkripsi yang kuat, serta penyuluhan kepada nasabah untuk meningkatkan kewaspadaan. Perlindungan represif meliputi investigasi internal, pemberian kompensasi atau ganti rugi, dan penyelesaian sengketa melalui mekanisme pengaduan serta mediasi sebagaimana diatur dalam POJK No. 1/POJK.07/2013 dan PBI No. 16/1/PBI/2014.

Landasan hukum perlindungan nasabah diperkuat oleh Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen (Pasal 4 dan 19), Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (Pasal 4, 67, dan 68), serta Undang-Undang ITE (Pasal 30 dan 32). Namun, efektivitas pelaksanaannya belum optimal karena lemahnya harmonisasi antar regulasi, dominasi posisi kontraktual bank, serta beban pembuktian yang tidak seimbang yang membebani nasabah. Oleh karena itu, perlu dilakukan reformasi regulasi menyeluruh yang mencakup prinsip tanggung jawab objektif (*strict liability*), pembagian beban pembuktian yang adil (*reversed burden of proof*), dan standar kompensasi nasional. Pendekatan keadilan restoratif juga harus diterapkan untuk memulihkan hak-hak korban secara utuh dan mengembalikan keseimbangan hubungan hukum antara bank dan nasabah dalam sistem perbankan digital yang adil dan transparan. perlu adanya reformasi regulasi secara menyeluruh yang mencakup prinsip tanggung jawab objektif (*strict liability*), penerapan prinsip *reversed burden of proof*, dan perumusan standar kompensasi nasional bagi korban kejahatan digital. Pendekatan keadilan restoratif harus dijadikan orientasi dalam perlindungan hukum, di mana fokus tidak hanya pada pelaku, tetapi juga pada pemulihan kerugian korban dan pemulihan hubungan hukum yang adil antara bank dan nasabah. Perlindungan hukum yang efektif harus mampu memberikan kepastian hukum, keadilan, dan keberpihakan terhadap pihak yang lebih rentan dalam transaksi keuangan digital.

REFERENSI

Andreae, S. J. F., dkk. (1977). *Indonesia & Dutch, terjemahan kamus istilah hukum Belanda-Indonesia*. Bina Cipta.

Asikin, Z. (2015). *Pengantar hukum perbankan Indonesia*. PT. RajaGrafindo Persada.

Bank Indonesia. (2017). *Peraturan Bank Indonesia Nomor 19/12/PBI. 2017 tentang penyelenggaraan teknologi finansial*.

Chazawi, A. (2015). *Tindak pidana informasi dan transaksi elektronik*. Media Nusa Creative.
Certo, S. (1996). *Strategic management*. McGraw-Hill.
Djumhana, M. (1993). *Asas-asas hukum perbankan Indonesia*. Citra Aditya Bakti.
Ekawati, D. (2018). Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan *skimming* ditinjau dari perspektif teknologi informasi dan perbankan. *Unnes Law Review, 1*(2), 159.
Fuadi, M. (1999). *Hukum perbankan modern*. PT. Citra Aditya Bakti.
Garner, B. A. (2004). *Black's law dictionary* (8th ed.). Linguaphone Institute Limited.
Ginting, P. (2008). Kebijakan penanggulangan tindak pidana teknologi informasi melalui hukum pidana. (Unpublished master's thesis). Universitas Diponegoro.
Hartono, S. R. (2007). *Penegakan hukum tentang tanggung gugat produsen dalam perwujudan perlindungan konsumen*. Genta Press.
Kasmir. (2002). *Bank dan lembaga keuangan lainnya* (6th ed.). PT. RajaGrafindo Persada.
Kristiyanti, C. T. S. (2011). *Hukum perlindungan konsumen* (3rd ed.). Sinar Grafika.
Linggoharjo, V. (2020). Tanggung jawab kejahatan perbankan melalui modus operandi *skimming*. *Magister Hukum Arumentum, 7*(1), 34.
Mishkin, F. S. (1995). *The economics of money, banking, and financial markets* (4th ed.). Columbia University.
Oughton, D., & Lowry, J. (1997). *Textbook on consumer law*. Blackstone Press Limited.
Poerwodarminta, W. J. S. (1976). *Kamus umum bahasa Indonesia*. Balai Pustaka.
Sidabalok, J. (2014). *Hukum perlindungan konsumen di Indonesia* (3rd ed.). PT. Citra Aditya Bakti.
Simorangkir, O. P. (1998). *Seluk beluk bank komersial*. Aksara Persada Indonesia.
Sjahdeini, S. R. (1993). *Kebebasan berkontrak dan perlindungan yang seimbang bagi para pihak dalam perjanjian kredit bank di Indonesia*. Institut Bankir Indonesia.
Soekanto, S. (1986). *Pengantar penelitian hukum* (3rd ed.). UI-Press.
Suryanto. (2020). Implementasi Undang-Undang Nomor 27 tahun 2022 tentang perlindungan data pribadi dalam industri ritel tinjauan terhadap kepatuhan dan dampaknya pada konsumen. *Veritas, 10*(1), 121–135.
Suyatno, T., dkk. (1993). *Kelembagaan perbankan*. PT. Gramedia Pustaka Utama.
Usman, R. (2001). *Aspek-aspek hukum perbankan di Indonesia* (2nd ed.). PT. Gramedia Pustaka Utama.
Utrecht, E. (1983). *Pengantar dalam hukum Indonesia* (M. S. Djingdang, Trans.). PT. Ichtiar Baru dan Sinar Harapan.