Indonesian Journal of Law

Vol. 3, No. 7, Juli 2026
Hal 217-225

E-ISSN: 3032-3622
P-ISSN: 3032-3614

Site: https://jurnal.intekom.id/index.php/inlaw

Urgensi Pengaturan Standar Keamanan Siber Perbankan Sebagai Bentuk Perlindungan Konsumen Dari Kejahatan *Phising* Dan *Skimming*

Erma Zahro Noor[1], Muhammad Amiruddin Widodo[2]
[1,2] Fakultas Hukum, Universitas Narotama, Surabaya, Indonesia

Article Info

Article history:

Received Juli 7, 2026
Revised Juli 7, 2026
Accepted Juli 8, 2026

Kata Kunci:

Cybersecurity,
Kejahatan Siber,
Keamanan Siber Perbankan,
Phishing dan *Skimming*

Keywords:

Cybersecurity,
Cybercrime,
Banking Cybersecurity,
Phishing and Skimming

ABSTRAK

Transformasi digital sektor perbankan Indonesia menghadirkan ancaman kejahatan siber berupa *phishing* dan *skimming* yang terus meningkat intensitasnya, sementara kerangka regulasi yang ada masih bersifat sektoral dan belum membentuk standar keamanan siber yang komprehensif, terukur, dan adaptif sebagai instrumen perlindungan konsumen perbankan. Penelitian ini menggunakan metode hukum normatif dengan pendekatan *statute approach*, *conceptual approach*, dan *comparative approach* melalui studi kepustakaan terhadap peraturan perundang-undangan, doktrin, dan literatur hukum yang relevan. Hasil penelitian menunjukkan bahwa regulasi perbankan Indonesia mencakup UU P2SK, UU PDP, UU ITE, dan POJK terkait belum menetapkan *minimum cybersecurity standard* yang seragam, serta mekanisme pertanggungjawaban bank terhadap kerugian nasabah akibat kegagalan siber masih menempatkan nasabah pada posisi yang secara struktural dirugikan akibat beban pembuktian yang tidak proporsional. Diperlukan reformasi regulasi melalui pembentukan *lex specialis* keamanan siber perbankan, penerapan prinsip *strict liability* dan *pembuktian terbalik*, kewajiban *cyber insurance*, serta penguatan kapasitas LAPS-SJK guna mewujudkan perlindungan konsumen yang substantif dan berkeadilan
.

ABSTRACT

The digital transformation of the Indonesian banking sector presents a growing threat of cybercrime in the form of phishing and skimming, while the existing regulatory framework remains sectoral and has not yet established comprehensive, measurable, and adaptive cybersecurity standards as an instrument for protecting banking consumers. This study uses a normative legal method with a statute approach, a conceptual approach, and a comparative approach through a literature review of relevant laws, doctrines, and legal literature. The results show that Indonesian banking regulations, including the P2SK Law, the PDP Law, the ITE Law, and related POJK, have not established uniform minimum cybersecurity standards, and the bank's accountability mechanism for customer losses due to cyber failures still places customers at a structural disadvantage due to a disproportionate burden of proof. Regulatory reform is needed through the establishment of a banking cybersecurity lex specialis, the implementation of strict liability and reverse burden of proof principles, mandatory cyber insurance, and strengthening the capacity of the LAPS-SJK to realize substantive and equitable consumer protection.

Corresponding Author:

Erma Zahro Noor
Fakultas Hukum, Universitas Narotama,
Surabaya, Indonesia
Email: erma.zahro@narotama.ac.id

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong transformasi digital sektor perbankan secara masif, sehingga layanan *digital banking* menjadi tulang punggung transaksi keuangan modern di Indonesia. Namun, di balik kemudahan tersebut, ancaman *cybercrime* dalam bentuk *phishing* dan *skimming* terus meningkat secara signifikan dan mengancam keamanan data serta aset nasabah [1] Data Otoritas Jasa Keuangan (OJK) menunjukkan bahwa kerugian akibat kejahatan siber perbankan mencapai angka yang mengkhawatirkan setiap tahunnya, mencerminkan lemahnya sistem perlindungan konsumen di sektor ini [2]. Ketidakmampuan regulasi yang ada dalam mengantisipasi perkembangan modus kejahatan siber secara adaptif menjadi persoalan mendasar yang perlu segera diselesaikan melalui pendekatan hukum yang komprehensif [3]. Urgensi pengaturan standar keamanan siber perbankan pun semakin nyata sebagai bentuk tanggung jawab negara dalam melindungi konsumen dari praktik kejahatan digital yang kian canggih [4].

Kerangka hukum yang mengatur keamanan siber di Indonesia saat ini masih bersifat sektoral dan belum terintegrasi secara menyeluruh, sehingga menimbulkan celah (*gap*) regulasi yang dimanfaatkan oleh pelaku kejahatan siber. Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (P2SK), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Peraturan OJK terkait tata kelola teknologi informasi perbankan belum secara eksplisit menetapkan *minimum cybersecurity standard* yang wajib dipenuhi oleh seluruh lembaga perbankan. Fragmentasi regulasi ini menyebabkan inkonsistensi implementasi keamanan siber antara bank besar dan bank kecil, yang pada akhirnya merugikan nasabah sebagai konsumen jasa keuangan [5]. Prinsip *due diligence* yang seharusnya menjadi kewajiban lembaga perbankan dalam melindungi data nasabah belum dijalankan secara optimal akibat ketiadaan standar yang jelas dan terukur. Kondisi ini menuntut adanya reformasi regulasi yang sistematis guna menciptakan ekosistem perbankan digital yang aman dan terpercaya bagi seluruh lapisan masyarakat [6] Permasalahan hukum yang muncul dari kondisi tersebut berpusat pada dua isu krusial, yakni pertama, belum adanya standar keamanan siber yang komprehensif dan adaptif dalam regulasi perbankan Indonesia, dan kedua, ketidakjelasan mekanisme pertanggungjawaban lembaga perbankan atas kerugian nasabah akibat kegagalan sistem keamanan siber. Konsep *strict liability* dan *vicarious liability* relevan untuk dikaji dalam konteks pertanggungjawaban bank ketika terjadi insiden siber yang mengakibatkan kerugian nasabah. Perlindungan konsumen sebagaimana diamanatkan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen seharusnya menjadi landasan utama dalam membangun kerangka hukum keamanan siber perbankan yang berkeadilan [7]. Oleh karena itu, penelitian ini hadir untuk menganalisis dan memberikan rekomendasi konstruktif bagi pembaruan regulasi keamanan siber perbankan di Indonesia demi terwujudnya perlindungan konsumen yang optimal [8].

2. METODE

2.1 Tipe Penelitian

Penelitian ini merupakan penelitian hukum *normatif* (*normative legal research*) yang mengkaji permasalahan hukum berdasarkan analisis terhadap norma, asas, dan sistem hukum yang berlaku terkait keamanan siber perbankan dan perlindungan konsumen.

2.2 Pendekatan Masalah

Penelitian ini menggunakan pendekatan *perundang-undangan* (*statute approach*) dengan menganalisis seluruh regulasi yang berkaitan dengan keamanan siber, perbankan, dan perlindungan konsumen, serta pendekatan *konseptual* (*conceptual approach*) yang mengkaji konsep, teori, dan doktrin hukum relevan seperti *strict liability* dan *due diligence* sebagai kerangka analisis. Mengingat kompleksitas isu yang dikaji, penelitian ini juga menerapkan pendekatan *perbandingan* (*comparative approach*) untuk menelaah regulasi keamanan siber perbankan di negara lain sebagai bahan pembanding dalam merumuskan rekomendasi kebijakan yang tepat [9].

2.3 Sumber Bahan Hukum

Sumber bahan hukum terdiri atas bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa doktrin, jurnal ilmiah, dan literatur hukum relevan, serta bahan hukum tersier berupa kamus hukum dan ensiklopedia.

2.3.1 Bahan Hukum Primer

1. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP);
   Menetapkan kewajiban bank sebagai pengendali data untuk menjamin keamanan data nasabah dari kebocoran.
2. UU No. 1 Tahun 2024 tentang perubahan Kedua atas UU ITE;
   Dasar hukum pemindanaan materil terhadap tindakan phising.

2.3.2 Bahan Hukum Sekunder

1. Buku tentang *Hukum Perlindungan Konsumen.*
2. Buku Tentang *Hukum Siber dan Kejahatan Komputer.*

2.3.3 Bahan Hukum Tersier

1. Black Law Dictionary atau Kamus Hukum Indonesia
2. Glosarium Resmi dari Badan Siber dan Sandi Negara (BSSN)

2.3.4 Prosedur Pengumpulan Bahan Hukum

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan inventarisasi dan klasifikasi seluruh sumber hukum yang relevan secara sistematis.

2.3.5 Analisis Bahan Hukum

Analisis dilakukan secara *preskriptif* dengan menggunakan metode interpretasi hukum dan konstruksi hukum untuk menghasilkan argumentasi dan rekomendasi normatif yang koheren.

3. HASIL DAN PEMBAHASAN

3.1 Kecukupan Regulasi Perbankan Indonesia dalam Menetapkan Standar Keamanan Siber yang Komprehensif dan Adaptif guna Memitigasi Risiko Kejahatan *Phishing* dan *Skimming*

3.1.1 Pemetaan Regulasi Keamanan Siber Perbankan yang Berlaku

Kerangka hukum yang mengatur keamanan siber di sektor perbankan Indonesia pada dasarnya telah terbentuk melalui sejumlah instrumen regulasi, namun keberadaannya masih bersifat sektoral dan belum membentuk satu kesatuan sistem yang kohesif. Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (P2SK), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Peraturan Otoritas Jasa Keuangan (OJK) Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh

Bank Umum, secara kolektif membentuk arsitektur regulasi yang dimaksudkan untuk melindungi ekosistem digital perbankan. Meskipun demikian, regulasi-regulasi tersebut pada tataran implementasinya masih menghadapi persoalan mendasar, yakni tidak adanya *minimum cybersecurity standard* yang ditetapkan secara eksplisit, terukur, dan berlaku seragam bagi seluruh lembaga perbankan tanpa membedakan skala usahanya. Kondisi ini sejalan dengan temuan [10] yang menyatakan bahwa ”ketertinggalan regulasi, keterbatasan teknologi, dan kurangnya edukasi nasabah menjadi hambatan nyata dalam penerapan strategi perlindungan perbankan digital,” sehingga kerja sama antara bank, regulator, dan penegak hukum menjadi kebutuhan yang tidak dapat ditunda.

Lebih lanjut, apabila ditelaah secara kritis, UU PDP dan UU ITE yang menjadi dua pilar utama perlindungan digital belum mampu menjawab tantangan keamanan siber perbankan secara spesifik dan memadai. UU PDP memang mengatur kewajiban pelindungan data pribadi, namun ruang lingkupnya bersifat umum dan tidak secara khusus menyentuh dimensi teknis keamanan sistem perbankan seperti persyaratan enkripsi, autentikasi berlapis, atau protokol penanganan insiden siber. Begitu pula UU ITE yang lebih berorientasi pada penindakan pidana *post-factum* daripada pencegahan berbasis standar teknis [11]. Dalam kajiannya atas kasus serangan *ransomware* terhadap Bank Syariah Indonesia menemukan bahwa meskipun regulasi nasional secara tekstual mengatur perlindungan data, penerapannya dalam praktik masih menghadapi hambatan serius, termasuk keterlambatan pelaporan insiden dan rendahnya kesiapan kelembagaan bank dalam menghadapi ancaman siber, yang mengindikasikan adanya jurang (*gap*) yang signifikan antara norma hukum tertulis dan realitas implementasi di lapangan.

3.1.2 Analisis Kesenjangan (*Gap Analysis*) Regulasi terhadap Ancaman *Phishing* dan *Skimming*

Kesenjangan regulasi yang paling mencolok dalam konteks perlindungan nasabah dari ancaman *phishing* dan *skimming* terletak pada tidak adanya definisi operasional yang jelas dan spesifik mengenai kedua modus kejahatan tersebut dalam regulasi perbankan Indonesia. Ketiadaan definisi yang presisi ini berdampak langsung pada sulitnya penegakan hukum, sebab aparat penegak hukum maupun lembaga perbankan tidak memiliki acuan normatif yang konkret untuk mengidentifikasi, mengklasifikasikan, dan merespons insiden *phishing* maupun *skimming* secara cepat dan tepat [12]. Secara tegas mengungkapkan bahwa UU ITE dan UU PDP belum secara spesifik dan komprehensif mengatur unsur-unsur tindak pidana *phishing*, khususnya dalam modus yang semakin berkembang melalui *file* aplikasi (*APK*), sehingga kekosongan norma ini menciptakan ruang abu-abu hukum yang menguntungkan pelaku kejahatan dan merugikan nasabah sebagai korban. Lebih jauh, tidak adanya kewajiban *mandatory cybersecurity audit* secara berkala yang berlaku seragam bagi seluruh bank menyebabkan tingkat keamanan sistem antarinstitusi perbankan bervariasi secara signifikan, dan disparitas ini pada akhirnya menciptakan celah yang dapat dieksploitasi oleh pelaku *phishing* maupun *skimming* untuk menyasar institusi dengan tingkat keamanan yang lebih rendah.

Persoalan kesenjangan regulasi ini semakin diperparah oleh absennya mekanisme *breach notification* yang tegas dan terstandarisasi, yakni kewajiban bagi bank untuk segera memberitahukan nasabah apabila terjadi kebocoran data atau insiden keamanan siber yang berpotensi merugikan mereka. Dalam konteks ini [13], mengingatkan bahwa serangan *cybercrime* di industri keuangan tidak hanya dipicu oleh faktor eksternal seperti modus serangan yang kian canggih, tetapi juga oleh faktor internal berupa lemahnya sistem keamanan, kurangnya pembaruan sistem secara berkala, dan keterbatasan kompetensi sumber daya manusia di bidang keamanan siber, yang keseluruhannya mencerminkan perlunya regulasi yang tidak hanya mengatur larangan, tetapi juga mewajibkan standar teknis minimum yang konkret dan dapat diaudit secara independen. Apabila dibandingkan dengan standar internasional seperti *Basel Committee on Banking Supervision (BCBS) Principles for Operational Resilience* atau *MAS Technology Risk Management Guidelines* Singapura yang mewajibkan *penetration testing* berkala, pelaporan insiden dalam waktu 24 jam, dan sertifikasi keamanan sistem yang terverifikasi, maka

regulasi perbankan Indonesia masih tertinggal cukup jauh dalam hal ketegasan, terukurnya standar, dan mekanisme pengawasannya.

3.1.3 Evaluasi Sifat Adaptivitas Regulasi terhadap Perkembangan Modus Kejahatan Siber

Salah satu kelemahan struktural yang paling kritis dari kerangka regulasi keamanan siber perbankan Indonesia adalah sifatnya yang cenderung reaktif (*reactive*) dan tidak *future-proof*, sehingga regulasi yang ada selalu tertinggal dari perkembangan modus kejahatan siber yang berevolusi dengan kecepatan yang jauh melampaui ritme pembentukan peraturan perundang-undangan. Modus *phishing* kontemporer telah jauh berkembang melampaui sekadar pembuatan situs web palsu, kini mencakup *spear phishing* yang ditargetkan secara personal menggunakan data pribadi korban, *vishing* berbasis rekayasa suara, hingga *smishing* yang memanfaatkan pesan singkat, sementara teknologi *artificial intelligence* dan *deepfake* semakin digunakan untuk mempercanggih serangan peniruan identitas yang menyasar nasabah perbankan [14], menegaskan bahwa meskipun UU ITE dan sejumlah peraturan pelaksana telah diterbitkan, masih ditemukan kelemahan substansial dalam aspek kepastian hukum dan kapasitas teknis aparat penegak hukum, sehingga reformasi hukum yang tidak hanya berfokus pada pemidanaan tetapi juga pada penguatan infrastruktur digital dan kerja sama internasional menjadi sebuah keniscayaan yang tidak dapat lagi ditunda.

Kondisi ketidakadaptifan regulasi ini pada praktiknya menempatkan lembaga perbankan pada posisi yang rentan, karena tanpa adanya kewajiban regulatif untuk memperbarui sistem keamanan secara dinamis mengikuti perkembangan ancaman, banyak bank terutama bank kecil dan *Bank Perkreditan Rakyat* (BPR) beroperasi dengan sistem keamanan yang sudah usang dan tidak mampu mendeteksi modus serangan siber terkini [15]. Dalam kajian rekonstruksi hukum pidana terhadap *cybercrime* menekankan bahwa diperlukan pembaruan paradigma hukum yang tidak hanya bersifat represif, tetapi juga preventif dan restoratif, dengan mengintegrasikan prinsip-prinsip hak asasi manusia dalam tata kelola keamanan siber nasional, sekaligus mendorong adopsi *risk-based approach* yang dinamis sebagai basis regulasi, agar hukum tidak sekadar mengejar kejahatan yang telah terjadi, melainkan mampu mengantisipasi dan mencegah kejahatan siber sebelum menimbulkan kerugian bagi nasabah perbankan. Oleh sebab itu, rekonstruksi regulasi keamanan siber perbankan menuju pendekatan berbasis risiko yang adaptif, terukur, dan berorientasi pada perlindungan konsumen merupakan agenda legislasi yang sudah tidak dapat ditangguhkan lagi.

3.2 Mekanisme Pertanggungjawaban Hukum Lembaga Perbankan terhadap Kerugian Nasabah Akibat Kegagalan Keamanan Siber

3.2.1 Konstruksi Pertanggungjawaban Hukum Bank dalam Perspektif Hukum Perdata dan Hukum Perbankan

Hubungan hukum antara bank dan nasabah pada hakikatnya merupakan hubungan kontraktual yang bersumber dari perjanjian penyimpanan dana dan penggunaan layanan perbankan, yang secara inheren melahirkan kewajiban hukum (*duty of care*) bagi bank untuk melindungi aset, data, dan kepentingan finansial nasabah dari segala bentuk ancaman, termasuk kejahatan siber. Landasan normatif kewajiban ini dapat ditemukan dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan yang secara tegas mengamanatkan bank untuk menjaga kerahasiaan data nasabah, serta Pasal 1338 Kitab Undang-Undang Hukum Perdata (*KUH Perdata*) yang menegaskan bahwa setiap perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi para pihak yang membuatnya, sehingga kelalaian bank dalam memenuhi standar keamanan yang diperjanjikan baik secara eksplisit maupun implisit dapat dikonstruksikan sebagai *wanprestasi* yang melahirkan kewajiban ganti rugi [16]. Selanjutnya dapat dinyatakan bahwa meskipun Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan telah memberikan perlindungan terhadap dana nasabah, perlindungan data nasabah masih memerlukan perhatian lebih, dan bank harus memastikan keamanan sistem elektronik serta bertanggung jawab penuh

atas keamanan data nasabah sebagai prioritas utama dalam memelihara kepercayaan masyarakat terhadap lembaga perbankan. Konstruksi *wanprestasi* ini menjadi relevan ketika bank terbukti tidak mengimplementasikan sistem keamanan yang memadai sesuai dengan standar yang berlaku, sehingga memberikan ruang bagi pelaku kejahatan *phishing* maupun *skimming* untuk mengeksploitasi kelemahan sistem dan merugikan nasabah.

Di sisi lain, apabila kegagalan keamanan siber bank tidak dapat dikaitkan langsung dengan hubungan kontraktual, maka nasabah dapat menempuh jalur *perbuatan melawan hukum* (*onrechtmatige daad*) sebagaimana diatur dalam Pasal 1365 *KUH Perdata*, yang mensyaratkan pembuktian adanya perbuatan melawan hukum, kesalahan, kerugian, dan hubungan kausalitas antara perbuatan dan kerugian yang diderita. Namun, dalam konteks kejahatan siber perbankan, beban pembuktian ini secara struktural sangat memberatkan nasabah mengingat kompleksitas teknis yang melekat pada insiden siber dan keterbatasan akses nasabah terhadap data sistem internal bank [17] dalam analisisnya mengenai pembuktian dalam sengketa *wanprestasi* menegaskan bahwa penggugat memikul kewajiban untuk membuktikan kelalaian tergugat, dan pengadilan menilai keabsahan serta kekuatan alat bukti guna mencapai kebenaran materiil dan keadilan substantif, suatu mekanisme yang dalam sengketa kejahatan siber perbankan menjadi sangat tidak seimbang mengingat nasabah hampir tidak memiliki akses terhadap log sistem, data forensik digital, atau dokumentasi teknis yang menjadi bukti krusial untuk membuktikan kelalaian bank, sehingga diperlukan reformasi normatif berupa penerapan prinsip *pembuktian terbalik* (*reversal of burden of proof*) demi mewujudkan keadilan substantif bagi nasabah sebagai pihak yang secara struktural lebih lemah.

3.2.2 Analisis Mekanisme Ganti Rugi dan Perlindungan Hukum Nasabah yang Berlaku

Mekanisme perlindungan hukum bagi nasabah korban kejahatan siber perbankan di Indonesia pada dasarnya dapat ditempuh melalui dua jalur utama, yakni jalur non-litigasi melalui mekanisme pengaduan internal bank (*internal dispute resolution*) dan Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS-SJK), serta jalur litigasi melalui gugatan perdata di pengadilan. Pada tataran regulasi, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan hak kepada nasabah sebagai konsumen untuk mendapatkan kompensasi atas kerugian yang dideritanya, sementara POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan mewajibkan setiap lembaga jasa keuangan untuk memiliki mekanisme penanganan pengaduan yang efektif dan terstandarisasi [18]. dalam penelitiannya secara kritis mengungkapkan bahwa meskipun kerangka hukum perlindungan nasabah telah tersedia, implementasinya kerap belum efektif dalam praktik nasabah sering mengalami kerugian finansial yang signifikan dan menghadapi berbagai hambatan dalam proses penyelesaian sengketa dengan bank, baik melalui jalur litigasi maupun non-litigasi, yang mencerminkan adanya jurang yang lebar antara norma perlindungan konsumen yang tertulis dan realitas pemenuhan hak nasabah di lapangan. Kondisi ini diperparah oleh kenyataan bahwa proses pembuktian dalam gugatan perdata mensyaratkan nasabah untuk membuktikan secara teknis bahwa kerugian yang dialaminya disebabkan oleh kelalaian bank dalam menjaga keamanan sistem, suatu beban yang secara praktis hampir mustahil dipenuhi oleh nasabah awam tanpa bantuan ahli forensik digital.

Dalam konteks LAPS-SJK sebagai mekanisme alternatif penyelesaian sengketa, regulasi yang menjadi dasar operasionalnya adalah POJK Nomor 61/POJK.07/2020, yang memberikan kewenangan kepada LAPS-SJK untuk memfasilitasi penyelesaian sengketa melalui mediasi dan arbitrase [19] menjelaskan bahwa LAPS-SJK menyediakan dua layanan utama yakni mediasi dan arbitrase yang dapat dipilih oleh para pihak guna menyelesaikan sengketa di sektor jasa keuangan di luar jalur pengadilan, namun dalam konteks sengketa kejahatan siber perbankan, efektivitas LAPS-SJK masih dihadapkan pada keterbatasan kapasitas teknis dalam menilai bukti-bukti digital yang bersifat sangat spesifik dan kompleks, sehingga penguatan kapasitas kelembagaan LAPS-SJK dalam menangani sengketa yang

melibatkan dimensi teknis keamanan siber menjadi kebutuhan mendesak yang harus segera diakomodasi dalam pembaruan regulasi. Selain itu [20] menyoroti bahwa ancaman *cybercrime* di sektor perbankan termasuk *phishing*, *malware*, dan kebocoran data menyebabkan tidak hanya kerugian finansial tetapi juga penurunan reputasi institusi, dan peningkatan keamanan siber serta kerja sama antar lembaga merupakan keniscayaan dalam menghadapi ancaman tersebut, yang secara implisit mengandung makna bahwa mekanisme pertanggungjawaban hukum harus didesain bukan hanya sebagai instrumen kompensasi pasca-insiden, melainkan juga sebagai insentif bagi bank untuk secara proaktif memperkuat sistem keamanannya.

3.2.3 Rekomendasi Kerangka Pertanggungjawaban yang Komprehensif

Mencermati keseluruhan kelemahan dalam konstruksi pertanggungjawaban dan mekanisme perlindungan nasabah yang ada, diperlukan reformasi normatif yang sistematis dan berorientasi pada perlindungan konsumen secara substantif. Pertama, perlu diatur secara eksplisit dalam regulasi OJK mengenai penerapan prinsip *strict liability* bagi lembaga perbankan dalam konteks kegagalan keamanan siber, yakni bahwa bank dapat dimintai pertanggungjawaban dan diwajibkan membayar ganti rugi kepada nasabah yang dirugikan akibat insiden *phishing* atau *skimming* tanpa mensyaratkan nasabah untuk membuktikan adanya unsur kesalahan bank, sepanjang insiden tersebut terjadi dalam lingkup sistem atau kanal layanan yang dioperasikan oleh bank [21]. dalam analisisnya atas perlindungan nasabah Bank Syariah Indonesia menegaskan bahwa perlindungan konsumen dalam *digital banking* diatur oleh Undang-Undang Nomor 8 Tahun 1999, namun implementasinya dalam menghadapi risiko *phishing*, *malware*, dan gangguan layanan masih memerlukan penguatan infrastruktur teknologi informasi yang andal serta peningkatan ketangguhan sistem keamanan secara menyeluruh, yang berarti bahwa kewajiban hukum bank tidak boleh berhenti pada pemenuhan persyaratan administratif semata, tetapi harus mencakup tanggung jawab substantif atas keamanan seluruh ekosistem layanan digital yang dioperasikannya.

Kedua, perlu dipertimbangkan pembentukan mekanisme perlindungan nasabah yang bersifat *ex ante*, yakni sebelum terjadinya insiden siber, melalui kewajiban *cyber insurance* bagi seluruh lembaga perbankan dan pembentukan *Dana Penjaminan Kerugian Siber Nasabah* sebagai instrumen kompensasi yang lebih aksesibel [22]. dalam kajiannya tentang perlindungan hukum nasabah pengguna *mobile banking* menyimpulkan bahwa seiring pesatnya perkembangan teknologi dan informasi, kejahatan terhadap teknologi dan informasi pun berkembang secara paralel, sehingga peraturan dan pelaksanaan perlindungan hukum bagi nasabah pengguna *mobile banking* perlu ditinjau kembali secara menyeluruh agar tetap relevan dan efektif, suatu rekomendasi yang hingga kini belum mendapatkan tindak lanjut legislatif yang memadai dan semakin mendesak untuk diwujudkan mengingat eskalasi ancaman siber yang terus terjadi. Dengan mengintegrasikan prinsip *strict liability*, mekanisme *pembuktian terbalik*, kewajiban *cyber insurance*, dan penguatan kapasitas LAPS-SJK dalam satu kerangka regulasi yang kohesif, Indonesia akan memiliki fondasi hukum yang jauh lebih kuat dalam memastikan bahwa setiap kerugian nasabah akibat kegagalan keamanan siber perbankan dapat diselesaikan secara adil, efisien, dan bermartabat.

4. KESIMPULAN

Peraturan perbankan saat ini, seperti POJK No. 11/POJK.03/2022, POJK No. 22 Tahun 2023, UU PDP, dan peraturan terbaru OJK dan Bank Indonesia di tahun 2025/2026, telah menetapkan peraturan yang komprehensif tentang keamanan siber. Perlindungan data pribadi, kewajiban audit forensik digital, dan rencana pemulihan bencana siber adalah contoh dari peraturan hulu ke hilir. Namun, karena hukum tertinggal dari teknologi, regulasi masih menghadapi banyak masalah dalam hal adaptif. Regulasi sering kali tidak responsif ketika modus operandi kejahatan siber berubah, yang berkembang jauh lebih cepat daripada birokrasi pembaharuan hukum.

Tanggung jawab bank terhadap kerugian nasabah akibat kegagalan siber telah berubah dari pertanggungjawaban konvensional berbasis kesalahan ke tanggung jawab mutlak dan kewajiban penjaga amanah. Berdasarkan UU Perlindungan Konsumen dan POJK terbaru, bank bertanggung jawab penuh untuk mengganti kerugian materiil nasabah sebesar 100% melalui mekanisme beban pembuktian terbalik jika kerugian nasabah murni disebabkan oleh kebocoran server, kegagalan sistem autentikasi, atau kekurangan alat pengaman skimming pada ATM. Bank yang gagal mengurangi risiko siber juga dikenai pertanggungjawaban administratif oleh Otoritas Jasa Keuangan (OJK), yang dapat mengakibatkan denda miliaran rupiah hingga penurunan tingkat kesehatan bank, selain ganti rugi finansial langsung kepada nasabah. Bank hanya dapat menolak pertanggungjawaban jika mereka dapat membuktikan secara forensik digital bahwa nasabah benar-benar lalai (contributory negligence), seperti menyerahkan kode OTP secara sukarela kepada pelaku.

REFERENSI

[1] Putra Abadi Langkat and Pembangunan Panca Budi, "Implikasi Hukum Perlindungan Konsumen Dalam Transaksi Keuangan Digital Dan Peninjauan Peraturan Perbankan" 03, no. 02 (2025): 106–17.
[2] Fadia Adzani, "Perbandingan Perlindungan Hukum Nasabah Perbankan Terkait Hilangnya Saldo Di Spanyol Dan Indonesia" 3, no. 1 (2025): 1–21.
[3] Nafis Dwi Kartiko, "Perlindungan Konsumen Sektor Keuangan: Peran OJK Dalam Menghadapi Ancaman Phising Dan Skimming" 5, no. 2 (2024): 347–63.
[4] Komang Rama Agastya, "Analisis Pembuktian Dalam Sengketa Perdata Mengenai Wanprestasi Dalam Perjanjian" 6 (2024): 340–49.
[5] Subaidah Ratna Juita, Dhian Indah Astanti, and Dian Septiandani, "Perlindungan Hukum Terhadap Nasabah Bank Korban Kejahatan Skimming" 6, no. 19 (2023): 407–19.
[6] Hanafi Dwi Laksono, Ilham Hendra Prabowo, and Aditya Sulistyo Budhi, "Optimalisasi Perlindungan Konsumen Perbankan Bedasarkan UU NO 8 TAHUN 1999," no. 8 (2021): 636–41.
[7] Muhamad Naufal and Aulia Azmi, "Analisa Kasus Kebocoran Data Pada Bank Indonesia Dalam Sistem Perbankan" 1, no. 6 (2024): 448–58.
[8] Ditmar Hadi, "Perlindungan Hukum Nasabah Sebagai Konsumen Perbankan Terhadap Kejahatan Skimming" 8, no. 10 (2023).
[9] Budiarto, Agung. "*Perlindungan Hukum Nasabah Pengguna Mobile Banking*" 9 (2021): 300–308.
[10] Revalina Gita Ananda and Davina Nurfadilah, "Peran Hukum Serta Kendala Dalam Menjalankan Strategi Bank Melindungi Nasabah Di Era Digital Untuk Keamanan Transaksi Online" 2, no. 6 (2024): 148–56.
[11] Ilman Maulana Kholis, "Perlindungan Data Pribadi Dan Keamanan Siber Di Sektor Perbankan : Studi Kritis Atas Penerapan UU PDP Dan UU ITE Di Indonesia" 4, no. 2 (2024).
[12] Devi Anjheli, "Privasi Digital Dan Kejahatan Phishing Di Indonesia : Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP Berdasarkan Laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) Tahun 2023 , Lebih Dari 215 Juta Penduduk Telah Terhubung" 4, no. 1 (2024).
[13] Shofie Azizah et al., "Keamanan Siber Sebagai Fondasi Pengembangan Aplikasi Keuangan Mobile: Studi Literatur Mengenai Cybercrime Dan Mitigasinya" 17, no. September (2024): 221–37.
[14] Bunga Anggreini, "Penguatan Hukum Pidana Indonesia Dalam Menghadapi Kejahatan Siber Era Digital" 3 (2025): 8–20.
[15] Soetardi Tri Cahyono, "Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia" 1, no. 1 (2025): 111–33.
[16] Alfred Yetno, "Tanggung Jawab Bank Dalam Menjaga Keamanan Dan Kerahasiaan Data Nasabah Perbankan Di Indonesia" 10, no. 1 (2024): 67–76.

[17] Agastya, "Analisis Pembuktian Dalam Sengketa Perdata Mengenai Wanprestasi Dalam Perjanjian."
[18] Almira Qurrotul Aini, "Perlindungan Hukum Nasabah Dalam Kasus Pembobolan Rekening Bank Di Indonesia" 1, no. 6 (2024): 165–72.
[19] Dewi Fatmala Putri et al., "Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking" 1, no. 4 (2023): 173–81.
[20] Nasywa Shafa Azzahra, "Tinjauan Literatur Tentang Ancaman Cybercrime Dan Implementasi Keamanan Siber Di Industri Perbankan" 2, no. 7 (2024): 692–700.
[21] Putri et al., "Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking."
[22] Agung Budiarto, "Perlindungan Hukum Nasabah Pengguna Mobile Banking" 9 (2021): 300–308.