PETITUM LAW JOURNAL

PetitumLawJournal

Volume 2 Nomor 2, Mei 2025
E-ISSN: 3030-9409

ANALISIS PERLINDUNGAN HUKUM TERHADAP NASABAH PENGGUNA INTERNET BANKING PADA BANK BRI

Samson Ratuloli[1*], Orpa J. Nubatonis [2], Husni Kusuma Dinata[3]

[1*] *Faculty of Law, Nusa Cendana University, Indonesia. E-mail: samsonbatulicin@gmail.com*
[2] *Faculty of Law, Nusa Cendana University, Indonesia. E-mail: orpajnubatonis@gmail.com*
[3]*Faculty of Law, Nusa Cendana University, Indonesia. E-mail: hkusumad@gmail.com*
**Corresponding Author*

Abstract: *This research aims to analyze the legal protection for customers using internet banking services at Bank BRI in Indonesia. This topic is important because, to date, there are no specific regulations that explicitly govern the rights of internet banking users. This research focuses on two main questions: how legal protection is provided to internet banking customers at Bank BRI, and what challenges are encountered in the implementation of such legal protection. The research method used is normative, with a legislative approach to relevant laws and regulations, such as Law No. 10 of 1998 on Banking, Law No. 8 of 1999 on Consumer Protection, as well as regulations from the Financial Services Authority (OJK) and Bank Indonesia, which govern customer data security and digital banking services. The research results show that Bank BRI has implemented preventive legal protection measures, such as security policies, customer education, and security technologies like Secure Socket Layer (SSL). However, significant challenges in providing legal protection to customers include the complexity of regulations related to cybercrime and the lack of law enforcement that adapts to new technological developments, such as artificial intelligence (AI) and blockchain. Cross-border jurisdiction also becomes an obstacle in handling cybercrime cases. Additionally, the lack of customer education on cybersecurity increases the risk of attacks, while cyber threats continue to evolve with increasingly sophisticated methods. This research is expected to contribute to the development of more effective legal protection regulations for internet banking customers.*

Keywords : *Legal Protection; Internet Banking.*

1. Pendahuluan

Perkembangan teknologi dan internet yang pesat telah memudahkan berbagai aspek kehidupan, termasuk sektor perbankan yang berfungsi memobilisasi dana dari masyarakat. Di Indonesia masalah yang terkait dengan bank diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.Inovasi dalam teknologi informasi dan komunikasi telah meningkatkan efisiensi dan efektivitas perbankan melalui produk dan layanan baru, yang tetap harus sesuai dengan ketentuan yang berlaku. Menurut Kamus Hukum, perjanjian adalah kesepakatan antara dua pihak atau lebih untuk mematuhi isi kesepakatan, dan Pasal 1313 KUHPerdata menjelaskan bahwa persetujuan adalah perbuatan di mana satu atau lebih pihak mengikatkan diri kepada pihak lain.[1] Internet banking adalah layanan *e-banking* yang memungkinkan nasabah mengakses informasi, berkomunikasi, dan melakukan transaksi perbankan melalui internet, tanpa perlu mengunjungi kantor bank. Layanan ini tidak hanya memperluas cara bank beroperasi,

[1] Sudarsono. Kamus Hukum, Jakarta: Rineka Cipta, 2007, 363.

tetapi juga meningkatkan kualitas pelayanan dengan menawarkan akses 24 jam sehari, 7 hari seminggu. Dengan internet banking, nasabah tidak perlu antre untuk melakukan pembayaran atau transaksi lainnya, yang membuatnya lebih menarik untuk membuka rekening. Selain itu, nasabah dapat melakukan transaksi secara mandiri dan efisien dari berbagai lokasi, memberikan fleksibilitas dalam mengelola keuangan mereka. Sejak diluncurkan, internet banking telah memberikan lebih banyak pilihan dan kemudahan bagi nasabah dalam menjalankan aktivitas perbankan.[2] Dalam hal fitur keamanan yang disediakan oleh bank, diperlukan regulasi hukum yang mengatur penerapannya. Ini penting mengingat dampak yang mungkin timbul terkait penerapan manajemen risiko. Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, khususnya Pasal 36–38, mengatur perlindungan hukum terkait. Pelanggaran terhadap beberapa pasal ini dapat dikenakan sanksi sesuai ketentuan.[3] Manajemen risiko adalah proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang mungkin menghambat pencapaian tujuan organisasi. Dalam dunia bisnis, risiko dapat berasal dari berbagai sumber, seperti operasional, finansial, hukum, hingga reputasi. Tanpa pengelolaan yang baik, risiko-risiko ini bisa berubah menjadi masalah besar yang mengancam keberlangsungan bisnis. Namun, dengan manajemen risiko yang tepat, Anda bisa memitigasi dampak negatif dan bahkan mengubah beberapa risiko menjadi peluang. Proses manajemen risiko adalah suatu proses yang bersifat berkesinambungan, sistematis, logik, dan terukur yang digunakan untuk mengelola risiko. Proses manajemen risiko meliputi penerapan kebijakan, prosedur, dan praktek untuk melaksanakan penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, penanganan risiko, monitoring dan reviu, dan komunikasi dan konsultasi.

Proses manajemen risiko dimulai dengan identifikasi risiko, di mana Anda mengidentifikasi segala sesuatu yang bisa salah. Langkah berikutnya adalah menganalisis risiko untuk memahami seberapa besar dampaknya dan seberapa sering kemungkinan itu terjadi. Setelah itu, risiko dievaluasi untuk menentukan prioritas penanganan, di mana risiko dengan dampak terbesar akan ditangani terlebih dahulu. Terakhir, pengendalian risiko melibatkan tindakan konkret untuk mengurangi, menghindari, atau mentransfer risiko tersebut. Untuk memberikan pembatasan pengertian tentang risiko maka Bank Indonesia memberikan definisi risiko adalah potensi kerugian akibat terjadinya suatu peristiwa *(events*) tertentu. Menurut pendapat penulis dengan hadirnya internet banking ini memungkinkan nasabah untuk melakukan berbagai transaksi perbankan dan menguntungkan karena memberikan akses mudah dan cepat untuk melakukan transaksi keuangan tanpa harus datang ke kantor cabang, seperti transfer dana, pembayaran tagihan, pembelian pulsa, cek saldo, dan lainnya secara online dalam waktu yang cukup cepat. Namun dibalik kemudahan yang di dapat dari nasabah pengguna internet banking, ada juga resiko yang di dapat dalam pengguna layanan ini, seperti masalah teknis yaitu gangguan jaringan sistem, pembaruan perangkat lunak atau kegagalan koneksi internet bisa menjadi hambatan dalam

[2] Antasari, Arga Satria. Pengaruh Penggunaan Internet Banking Terhadap Kepuasan Nasabah. *Universitas Brawijaya*, 2013.

[3] Pasal 36-38 Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 Tentang Penerapan Manajemen Resiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum .

mengakses atau menggunakan layanan internet banking, keamanan yaitu, resiko phishing, malware, ataupun serangan cyber lainnya yang dapat mengancam informasi pribadi keuangan pengguna, kesalahan pengguna, keterbatasan fitur, tidak semua fitur yang tersedia di kantor cabang dapat diakses melalui internet banking, sehingga dalam beberapa kasus nasabah mungkin perlu datang langsung ke bank untuk melakukan transaksi tertentu.

Bank Rakyat Indonesia (BRI) menyediakan layanan *e-banking*, termasuk Internet Banking, yang memungkinkan nasabah melakukan transaksi dengan mudah tanpa harus pergi ke bank. Namun, meskipun menawarkan kemudahan, layanan ini juga memiliki risiko seperti masalah teknis, gangguan jaringan, dan potensi risiko keamanan yang dapat mempengaruhi pengalaman nasabah. Salah satu contoh terjadi di Nusa Tenggara Timur, di mana BL, mengalami kehilangan Rp 35 juta setelah bertransaksi menggunakan aplikasi BRImo. Kejadian ini bermula pada 23 Desember 2022, ketika BL melakukan pembelian pulsa listrik sebesar Rp 100 ribu. Namun, pada hari yang sama, ia menerima notifikasi bahwa uang sebesar Rp 35 juta ditarik dari rekeningnya. Penelusuran menunjukkan bahwa dana tersebut ditransfer ke rekening BNI atas nama UAI. Karena merasa dirugikan, BL melapor ke Polda NTT pada 31 Desember 2022.[4] Terdapat peraturan yang dirancang untuk melindungi pelanggan dan Bank BRI sebagai entitas bisnis. Menurut Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK), Pasal 4 mengatur tentang hak konsumen, termasuk hak untuk memperoleh informasi yang jelas mengenai produk atau layanan yang mereka gunakan. Sementara itu, Pasal 7 menjelaskan tanggung jawab pelaku usaha, yang diwajibkan memberikan informasi yang benar, jelas, dan jujur kepada konsumen. Ini berarti Bank BRI bertanggung jawab untuk memberikan informasi yang lengkap mengenai produk dan layanan yang mereka tawarkan, termasuk Internet Banking, guna melindungi hak-hak konsumen. Hal yang seharusnya dijalankan, belum sepenuhnya dilakukan Bank BRI. Berdasarkan informasi di atas, Pihak Perbankan harus bisa menyiapkan fitur keamanan sehingga mampu menjaga kepercayaan masyarakat bahwa transaksi eletronik itu aman, hak-hak pengguna Internet Banking sebagai nasabah perbankan harus dilindungi dari potensi kerugian, baik melalui regulasi maupun dampak dari penggunaan produk perbankan. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menjamin hak nasabah untuk mendapatkan informasi yang jelas, serta perlindungan terhadap kerugian yang mungkin timbul akibat layanan perbankan digital. Bank bertanggung jawab memastikan keamanan, transparansi, dan keandalan layanan, sehingga nasabah terlindungi dari risiko seperti penipuan, gangguan teknis, atau penyalahgunaan data pribadi. Fitur keamanan yang paling umum dan penting dalam transaksi digital yang disiapkan oleh Pihak Perbankan sehingga mampu menjaga kepercayaan masyarakat bahwa transaksi eletronik itu aman adalah *Multi-Factor Authentication (MFA)* atau Autentikasi Multi-Faktor. MFA memastikan bahwa proses login atau transaksi tidak hanya bergantung pada satu proses verifikasi seperti kata sandi saja. Verifikasi berlapis ini bisa berupa sesuatu yang pengguna ketahui *(password)*, sesuatu yang pengguna miliki *(smartphone, token)*, atau sesuatu yang melekat pada pengguna (sidik jari, pengenalan wajah).

[4] https://www.victorynews.id/kupang/pr-3317006924/uang-rp35-juta-milik-m antan-wakil gubernur-ntt-hilang-via-bri-mobidiakses tanggal 07 Maret 2024.

2. Metode

Penelitian yuridis normatif adalah jenis penelitian ilmiah yang menemukan kebenaran berdasarkan logika keilmuan hukum dari sisi normatifnya. Penelitian ini dilakukan dengan melihat bahan kepustakaan atau bahan hukum, yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.[5]

3. Perlindungan Hukum Terhadap Nasabah Pengguna Internet Banking Pada Bank BRI

Untuk memberikan layanan kepada pelanggan, operasi perbankan dapat dilakukan secara langsung maupun tidak langsung. Salah satu contoh operasi perbankan yang dilakukan secara tidak langsung adalah melalui penggunaan layanan perbankan online, di mana nasabah dapat melakukan berbagai transaksi perbankan tanpa perlu datang langsung ke kantor cabang, melainkan melalui platform digital seperti internet banking atau mobile banking. Masalah utama dalam pelaksanaan perlindungan hukum pengguna internet banking adalah bagaimana regulasi internet banking di indonesia dan bagaimana pihak bank bisa bertanggungjawab atas keamanan data dan informasi nasabah selama menggunakan internet banking. Menurut Peraturan Otoritas Jasa Keuangan No. 12/POJK.03/2018, Bank Rakyat Indonesia (BRI) menawarkan sejumlah layanan elektronik banking yang memudahkan nasabah dalam melakukan transaksi keuangan. Layanan tersebut meliputi:

a) ATM BRI
b) SMS Banking BRI
c) BRIMO
d) Internet Banking BRI
e) Agen BRILINK
f) BRIZZI

Layanan-layanan ini bertujuan untuk memberikan kemudahan dan fleksibilitas bagi nasabah BRI dalam melakukan transaksi keuangan secara elektronik. Menurut Peraturan Otoritas Jasa Keuangan No. 12/POJK.03/2018, bank diharuskan untuk terus meningkatkan kapabilitas dalam menyediakan layanan yang berkelanjutan dan andal bagi pelanggan. Selain itu, peraturan ini juga menekankan pentingnya memberikan kemudahan akses ke layanan perbankan berbasis teknologi informasi (TI) yang dapat diakses tanpa batasan tempat dan waktu. Tujuannya adalah untuk mendorong pengelolaan keuangan yang lebih baik di masyarakat, dengan menyediakan solusi perbankan yang fleksibel dan dapat diakses kapan saja, di mana saja. Hal ini diharapkan dapat meningkatkan literasi dan inklusi keuangan, serta memperkuat hubungan antara bank dan nasabah melalui layanan perbankan yang lebih mudah dijangkau.

Beberapa undang-undang, seperti Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, dirancang untuk menghadapi pertumbuhan perekonomian nasional yang cepat, kompetitif, dan kompleks. Undang-undang ini bertujuan untuk menyesuaikan kebijakan ekonomi dan perbankan dengan perkembangan global dan sistem keuangan

[5]Soerjono Soekanto dan Sri Mamudji. Penelitian Hukum Normatif Suatu Tinjauan Singkat, Jakarta: CV.Rajawali, 1985.

yang maju. Selain itu, undang-undang ini juga melindungi nasabah internet banking dengan menyediakan regulasi yang memastikan keamanan dan kepastian hukum dalam transaksi perbankan online. Melalui peraturan ini, diharapkan perlindungan hukum bagi nasabah dapat terjamin, serta perbankan dapat beroperasi dengan lebih aman dan efisien di era digital. Menurut Peraturan OJK No. 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum, "layanan perbankan digital adalah layanan perbankan elektronik yang dikembangkan dengan mengoptimalkan pemanfaatan data nasabah untuk memberikan pelayanan yang lebih cepat, mudah, dan sesuai dengan kebutuhan nasabah (pengalaman pelanggan). Layanan ini memungkinkan nasabah untuk melakukan transaksi secara mandiri, dengan memperhatikan aspek pengamanan." Peraturan ini memberikan landasan bagi pengembangan layanan perbankan digital, memastikan bahwa pelayanan dapat dilakukan secara efisien dan aman sesuai dengan kebutuhan nasabah.

Dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Pasal 40 menyatakan bahwa bank harus merahasiakan informasi terkait dengan uang yang disimpan oleh nasabahnya. Kewajiban kerahasiaan ini berlaku kecuali dalam hal-hal yang diatur dalam Pasal 41, Pasal 41, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44A, di mana bank diperbolehkan untuk mengungkapkan informasi tersebut sesuai dengan ketentuan yang berlaku. Dalam Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, data nasabah internet banking dilindungi secara hukum. Peraturan ini menegaskan bahwa pengembangan Teknologi Informasi (TI) dapat meningkatkan efisiensi operasional dan layanan bank. Namun, TI juga dapat menambah risiko yang dihadapi bank, sehingga diperlukan manajemen risiko yang efektif. Fakta ini menunjukkan bahwa TI merupakan aset berharga bagi bank dan pengelolaannya yang tepat sangat penting untuk memanfaatkan potensi TI tanpa mengabaikan aspek keamanan.[6] Sedangkan menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen di dalam Pasal 3 pada huruf a,b,d,f Perlindungan Konsumen bertujuan:

a. Meningkatkan kesadaran, kemampuan dan kemandirian konsumen untuk melindungi diri;
b. Mengangkat harkat dan martabat konsumen dengan cara menghindarkannya dari ekses negative pemakaian barang dan/atau jasa;
c. Menciptakan sistem perlindungan konsumen yang mengandung unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi;
d. Meningkatkan kualitas barang dan/atau jasa yang menjamin kelangsungan usaha produksi barang dan/atau jasa, kesehatan, kenyamanan, keamanan, dan keselamatan konsumen.[7]

Dalam Pasal 4 huruf a Hak konsumen adalah: “Hak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa”. Dalam peraturan perlindungan konsumen, konsumen dilindungi melalui kepastian hukum dan keterbukaan informasi. Hal ini penting karena internet banking memerlukan aturan yang jelas untuk melindungi data nasabah dan informasi yang diberikan, serta untuk mencegah kejahatan teknologi. Pasal 4 menyebutkan bahwa konsumen memiliki hak

[6] Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko.
[7] Pasal 3 huruf a, b, d, f Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

atas keamanan dalam menggunakan barang dan jasa, termasuk layanan perbankan digital. Peraturan ini memastikan bahwa nasabah internet banking dapat merasa aman dan terlindungi dari potensi risiko dan penyalahgunaan data.[8] Sementara itu hasil analisa Pada Undang-Undang OJK terdapat pada Pasal 7 huruf c. pengaturan dan pengawasan mengenai aspek kehati-hatian bank, meliputi:

a. Manajemen risiko;
b. Tata kelola bank;
c. Prinsip mengenal nasabah dan anti pencucian uang; dan
d. Pencegahan pembiayaan terorisme dan kejahatan perbankan.[9]

Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Teknologi Elektronik pada Pasal 16 huruf b dan d: (1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

a. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
b. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau symbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut.

Hasil analisa dalam Pasal ini dalam Manajemen risiko dengan prinsip kehati-hatian bisa dikatakan bahwa disini OJK telah mengikuti peraturan yang sudah ada yang diatur sebelumnya pada Undang-Undang Perbankan, manajemen resiko terkait dalam Undang-Undang Perlindungan Konsumen yang mana dapat menjamin keamanan suatu produk yaitu internet banking, serta berkaitan dengan Undang-Undang ITE yang dapat melindungi kerahasian informasi data nasabah.

Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Tentang penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum dirumuskan dalam Pasal 10 dan 14 dapat diuraikan sebagai berikut :

Pasal 10

1) “Bank wajib melakukan proses manajemen risiko yang mencakup identifikasi, pengukuran, pemantauan dan pengendalian atas risiko terkait penggunaan Teknologi Informasi.
2) Proses manajemen risiko dilakukan terhadap aspek-aspek terkait Teknologi Informasi yang paling kurang mencakup pengembangan dan pengadaan Teknologi Informasi, operasional Teknologi Informasi, jaringan komunikasi, pengamanan informasi, Business Continuity Plan, end user computing, Electronic Banking, dan penggunaan pihak penyedia jasa Teknologi Informasi.
3) Dalam hal Bank menggunakan jasa pihak lain untuk menyelenggarakan Teknologi Informasi, Bank wajib memastikan bahwa pihak penyedia jasa Teknologi Informasi menerapkan juga manajemen risiko yang paling kurang sesuai dengan ketentuan dalam Peraturan Bank Indonesia ini”.

[8] Pasal 4 huruf a Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.
[9] Pasal 7 huruf c Undang-Undang Otoritas Jasa Keuangan.

Pasal 14

a. “pengamanan informasi ditujukan agar informasi yang dikelola terjaga kerahasiaan (confidentiality), integritas (integrity) dan ketersediaannya (availability) secara efektif dan efisien dengan memperhatikan kepatuhan terhadap ketentuan yang berlaku;
b. pengamanan informasi dilakukan terhadap aspek teknologi, sumber daya manusia dan proses dalam penggunaan Teknologi Informasi;
c. pengamanan informasi mencakup pengelolaan aset bank yang terkait dengan informasi, kebijakan sumber daya manusia, pengamanan fisik,pengamanan akses, pengamanan operasional, dan aspek penggunaan Teknologi Informasi lainnya”.

Kedua pasal ini berfokus pada keamanan dan manajemen risiko TI dalam perbankan, dengan tujuan menjaga keandalan operasional dan melindungi data yang dikelola oleh bank, baik dari segi teknologi maupun sumber daya manusia. Selanjutnya dalam Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.03/2015 yang selanjutnya disebut POJK No.13/POJK.03/2015 Tentang Penerapan Manajemen Risiko bagi BPR. Risiko[10] adalah potensi kerugian akibat suatu peristiwa tertentu. Berdasarkan definisi ini, maka dapat disimpulkan bahwa risiko adalah suatu keadaan yang tidak diperkirakan akan terjadi, dalam hal ini suatu kegagalan membayar pemerintah dalam kontrak pengadaan barang dan jasa. Seperti halnya perbankan, menurut penulis, pemerintah juga memerlukan manajemen risiko pengaturan dalam kontrak pengadaan barang dan jasa dalam rangka mengurangi atau bahkan menghilangkan perlunya kompensasi dari penyedia barang dan jasa karena hal tersebut mengganggu kemampuan pemerintah dalam melaksanakan tugas pemerintahan dan pembangunan. Mempertaruhkan Manajemen merupakan suatu bidang ilmu yang membahas tentang cara kerja suatu organisasi. POJK menetapkan bahwa manajemen risiko merupakan serangkaian metodologi dan prosedur yang akan digunakan untuk mengidentifikasi, mengukur, memantau, dan mengendalikan risiko yang timbul dari seluruh aktivitas BPR. Sehubungan dengan pasal ini, dapat dikatakan bahwa menurut pendapat penulis, pemerintah memerlukan manajemen.Prinsip Kehatian-hatian yang diberikan oleh pihak perbankan dan OJK harus mampu untuk memantau dan mengendalikan resiko yang timbul dari adanya penggunaan internet banking oleh masyarakat agar prinsip kehati2an dan prinsip kepercayaan kepada pihak perbankan tetap ada, adalah:

a) Bank dilarang melakukan tindakan baik secara langsung maupun tidak langsung yang mengakibatkan nasabah menganggap produk keuangan LN adalah produk bank;
b) Bank wajib menerapkan prinsip mengenal nasabah (KYC) sesuai ketentuan yang berlaku;dan
c) Bank Indonesia dapat sewaktu-waktu menghentikan aktivitas keagenan produk keuangan LN tertentu apabila kegiatan tersebut tidak sesuai dengan peraturan yang berlaku dan/atau memiliki potensi risiko yang dapat membahayakan bank. Risiko dalam kontrak pengadaan barang atau jasa dari suatu barang perspektif iman, dimana dengan adanya itikad baik para pihak untuk melaksanakan kewajibannya dalam kontrak, pihak lain dapat menikmati hak-hak yang harus diperoleh dari kegiatan tersebut kontrak. Manajemen risiko mencakup pengawasan, kebijakan,

[10] Nubatonis, Orpa Juliana. “Good Faith Governance: Risk Management in Government Procurement Contracts.” vol. 7 (December 18, 2023): 10–20. https://doi.org/10.30996/jhbbc.v7i1.9474.

prosedur manajemen risiko, menentukan batasan risiko, proses, dan sistem. Dari penjelasan ini jelas bahwa pihak perbankan dan OJK harus mampu untuk memantau dan mengendalikan resiko yang timbul dari adanya penggunaan internet banking oleh masyarakat agar prinsip kehati-hatian dan prinsip kepercayaan kepada pihak perbankan tetap ada.

Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia, yang terakhir diubah dengan Undang-Undang Nomor 7 Tahun 2009, Bank Indonesia memiliki wewenang untuk mengatur, mengkoordinir, mengawasi, dan melakukan tindakan terkait perbankan. Peraturan ini memberikan Bank Indonesia kewenangan dan tanggung jawab untuk mengawasi bank, termasuk menetapkan peraturan perbankan yang berlandaskan prinsip kehati-hatian, mengenakan sanksi kepada bank, serta memberikan dan mencabut izin untuk kelembagaan dan kegiatan usaha tertentu. Dengan demikian, Bank Indonesia berperan penting dalam menjaga stabilitas dan integritas sektor perbankan di Indonesia.

Dalam Pasal 15 ayat 1 dan 2 Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi yang berbunyi: (1) Atas kesalahan dan atau kelalaian penyelenggara telekomunikasi yang menimbulkan kerugian, maka pihak-pihak yang dirugikan berhak mengajukan tuntutan ganti rugi kepada penyelenggara telekomunikasi. (2) Penyelenggara telekomunikasi wajib memberikan ganti rugi sebagaimana dimaksud pada ayat (1), kecuali penyelenggara telekomunikasi dapat membuktikan bahwa kerugian tersebut bukan diakibatkan oleh kesalahan dan atau kelalaiannya. mengatur bahwa atas kesalahan dan kelalaian penyelenggara telekomunikasi yang menimbulkan kerugian, maka pihak-pihak yang dirugikan berhak untuk mengajukan tuntutan ganti rugi kepada penyelenggara telekomunikasi. Ganti rugi yang dimaksud adalah ganti rugi yang diberikan penyelenggara telekomunikasi kepada pengguna atau masyarakat luas yang dirugikan karena kelalaian atau kesalahannya. Ganti rugi wajib diberikan, kecuali penyelenggara tersebut dapat membuktikan bahwa kerugian tersebut bukan diakibatkan oleh kesalahan dan kelalaiannya.[11]

Dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana, terdapat beberapa aturan perlindungan bagi pelanggan. Aturan tersebut mencakup:

a) Tanggung jawab atas keterlambatan: Jika penyelenggara transfer dana terlambat dalam melaksanakan perintah transfer, mereka wajib membayar jasa, bunga, atau kompensasi kepada penerima atas keterlambatan tersebut.
b) Perbaikan kesalahan: Apabila penyelenggara pengirim melakukan kesalahan dalam proses transfer dana, mereka harus segera memperbaiki kesalahan tersebut dengan mengirimkan surat resmi kepada penerima.

Peraturan ini bertujuan untuk melindungi hak-hak pelanggan dan memastikan transparansi serta akuntabilitas dalam layanan transfer dana.

Menurut Peraturan Bank Indonesia Nomor 7/6/PBI/2005tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah, bank diharuskan untuk:

a) Menunjukkan transparansi informasi: Bank harus memberikan informasi yang jelas dan cukup kepada klien dan calon klien tentang produk yang ditawarkan, termasuk fitur, manfaat, risiko, dan biaya terkait.

[11] Pasal 15 ayat 1 dan 2 Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.

b) Penggunaan data pribadi: Bank wajib menjelaskan bagaimana data pribadi nasabah digunakan, termasuk bagaimana data tersebut dikumpulkan, disimpan, dan diproses, serta hak-hak nasabah terkait data pribadi mereka.

Peraturan ini bertujuan untuk melindungi hak-hak nasabah dan memastikan bahwa mereka membuat keputusan yang terinformasi tentang produk dan layanan perbankan.[12]

Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 mengatur perlindungan konsumen dalam sektor jasa keuangan dengan prinsip-prinsip berikut:

a) Transparansi : Pelaku usaha jasa keuangan harus memberikan informasi yang jelas dan jujur tentang produk atau layanan mereka.
b) Perlakuan Adil: Konsumen harus diperlakukan secara adil dalam semua transaksi dan interaksi.
c) Keandalan : Produk dan layanan harus dapat diandalkan sesuai dengan informasi yang diberikan.
d) Kerahasiaan dan Keamanan: Data dan informasi konsumen harus dijaga kerahasiaannya dan diamankan dengan baik.

Dalam Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, Pasal 27 menetapkan bahwa bank yang menyelenggarakan kegiatan e-banking harus memenuhi ketentuan yangditetapkan oleh Otoritas Jasa Keuangan (OJK) dan/atau otoritas terkait lainnya. Peraturan ini juga mengharuskan bank untuk memberikan edukasi kepada nasabah mengenai produk e-banking dan memastikan keamanan penggunaan layanan tersebut.[13]. Dalam Pasal juga 28 diatur tentang perizinan produk electronic banking.

Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.07/2018 mengenai Layanan Pengaduan Konsumen di Sektor Jasa Keuangan menetapkan bahwa bank harus mengikuti mekanisme penyelesaian pengaduan nasabah yang telah ditetapkan untuk mengurangi publikasi negatif dan menjamin penanganan yang cepat. Bank diwajibkan untuk menangani setiap pengaduan dengan menetapkan kebijakan dan prosedur tertulis yang jelas untuk menerima, menangani, dan menyelesaikan pengaduan dari pelanggan atau perwakilan mereka. Menurut Hadjon, perlindungan hukum bagi rakyat meliputi dua hal,yakni :

a) Perlindungan Hukum Preventif, yakni bentuk perlindungan hukum dimana kepada rakyat diberi kesempatan untuk mengajukan keberatan atau pendapatnya sebelum suatu keputusan pemerintah mendapat bentuk yang definitive.[14]Pemerintah mengeluarkan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen untuk melindungi pengguna mobile banking. Selain itu, bank diwajibkan untuk memberi tahu pelanggan mengenai privasi dan keamanan dalam bertransaksi melalui mobile banking, memastikan bahwa nasabah mendapatkan informasi yang jelas dan memadai untuk melindungi data dan transaksi mereka.

---

[12] Rosadi, Sinta Dewi. "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya." *Sosiohumaniora* 19.3 (2017): 206-212.

[13] Pasal 27 Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum.

[14] Philipus M. Hadjon. Perlindungan Bagi Rakyat Indonesia. Surabaya: PT.Bina Ilmu, 1987, 4-5.

b) Perlindungan Hukum Represif, yakni bentuk perlindungan hukum dimana lebih ditujukan dalam penyelesaian sengketa[15].Dalam upaya perlindungan hukum represif, terdapat berbagai macam cara untuk dilaksanakan, setidaknya ada tiga (3) cara, yaitu:
   1) Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.07/2018 tentang Layanan Pengaduan Konsumen di Sektor Jasa Keuangan mewajibkan pelaku usaha jasa keuangan untuk menangani pengaduan dari nasabah. Ini merupakan bagian dari perlindungan hukum represif. Proses ini mencakup penerimaan, pengendalian, dan penyelesaian pengaduan, yang bertujuan untuk melindungi hak konsumen dan memastikan bahwa masalah mereka ditangani dengan baik.
   2) Penyelesaian melalui Lembaga Alternatif Penyelesaian Sengketa Perbankan Indonesia (LAPSPI) Dalam eksistensinya, Lembaga Alternatif Penyelesaian Sengketa Perbankan Indonesia (LAPSPI) menyediakan layanan berupa:
      a. Mediasi: Metode penyelesaian sengketa di luar pengadilan yang melibatkan perundingan dengan bantuan mediator untuk mencapai kesepakatan damai antara pihak-pihak yang bersengketa.
      b. Adjudikasi: adalah metode penyelesaian sengketa di luar arbitrase dan pengadilan umum yang melibatkan seorang adjudikator untuk memutuskan sengketa tersebut. Proses ini bertujuan menghasilkan suatu keputusan yang disepakati oleh pihak-pihak yang bersengketa dan bersifat mengikat bagi kedua belah pihak. Adjudikasi sering digunakan dalam konteks perjanjian bisnis atau kontrak, di mana adjudikator akan memberikan putusan yang harus dipatuhi oleh semua pihak yang terlibat.
      c. Arbitrase: Proses penyelesaian sengketa perdata di bidang perbankan yang dilakukan di luar peradilan umum. Arbitrase dilakukan oleh adjudikator yang menghasilkan putusan yang mengikat para pihak, berdasarkan perjanjian arbitrase yang dibuat secara tertulis.
   3) Penyelesaian melalui pengadilan Penyelesaian melalui pengadilan dapat diselesaikan melalui, antara lain : Penyelesaian sengketa melalui pengadilan dapat dilakukan dengan beberapa cara,termasuk:
      a. Mediasi: Proses di mana pihak ketiga yang netral membantu pihak-pihak yang bersengketa untuk bernegosiasi dan mencapai kesepakatan yang memuaskan kedua belah pihak.
      b. Gugatan Perdata: Jika nasabah bank mengalami kerugian seperti kehilangan simpanan, mereka dapat mengajukan gugatan perdata ke pengadilan negeri. Gugatan ini dapat mencakup pelanggaran atau wanprestasi, memberikan perlindungan hukum kepada nasabah untuk mendapatkan kompensasi atas kerugian yang dialaminya.

Bank BRI memberikan perlindungan preventif dilakukan untuk mencegah terjadinya kerugian nasabah mobile banking.

Perlindungan represif dan preventif memiliki fokus yang berbeda dalam melindungi nasabah pengguna internet banking:

1) Perlindungan Represif: Fokus pada penyelesaian sengketa setelah kerugian terjadi. Ini melibatkan mekanisme penyelesaian sengketa, kemungkinan membawa kasus ke

[15] ibid

pengadilan, dan pemberian ganti rugi jika kerugian disebabkan oleh kelalaian pihak bank.

2) Perlindungan Preventif: Ditujukan untuk mencegah kerugian sejak awal. Ini termasuk:
   a) Undang-Undang dan Peraturan: Menyediakan kerangka hukum untuk perlindungan konsumen, seperti yang diatur oleh Bank Indonesia dan OJK.
   b) Pelatihan dan Edukasi: Memberikan pelatihan kepada nasabah mengenai cara menggunakan internet banking dengan aman.
   c) Pengawasan: Implementasi teknologi seperti Secure Socket Layer (SSL) untuk melindungi data dan transaksi.

4. Hambatan Perlindungan Hukum Terhadap Nasabah Pengguna Internet Banking Pada Bank BRI

Perlindungan hukum terhadap nasabah pengguna internet banking di Bank BRI (Bank Rakyat Indonesia) memiliki beberapa kendala dan tantangan yang sering dihadapi.

4.1 Regulasi dan Penegakan Hukum

a. Kompleksitas Hukum Siber

   Hukum siber, khususnya dalam konteks perlindungan nasabah bank yang menggunakan layanan internet banking, memiliki kompleksitas tersendiri yang muncul dari interaksi antara perkembangan teknologi, ancaman siber, dan dinamika regulasi. Meskipun Indonesia telah memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan terkait lainnya, proses penerapan hukum terhadap pelaku kejahatan siber sering kali terkendala oleh kurangnya pemahaman teknis di kalangan aparat penegak hukum. Hal ini dikarenakan teknologi informasi dan komunikasi berkembang dengan cepat, dan hukum seringkali tertinggal dalam mengatur teknologi baru. Misalnya, penggunaan kecerdasan buatan (AI) dan teknologi blockchain dalam layanan perbankan menciptakan tantangan baru yang belum sepenuhnya diatur oleh hukum yang ada. Regulasi yang dibuat untuk mengatasi kejahatan siber bisa menjadi usang dalam waktu singkat, mengingat sifat dinamis dari ancaman teknologi tersebut.[16]

b. Jurisdiksi Lintas Negara

   Jurisdiksi lintas negara menjadi salah satu kendala terbesar dalam penanganan kejahatan siber, termasuk dalam upaya perlindungan nasabah bank yang menggunakan layanan internet banking. Dalam hukum internasional, konsep yurisdiksi mengacu pada wewenang suatu negara untuk memberlakukan hukum terhadap individu, objek, atau kegiatan tertentu. Namun, dalam dunia siber, batas-batas yurisdiksi tradisional sering kali menjadi kabur karena sifat global dan borderless dari internet. Kejahatan siber sering kali melibatkan pelaku yang berada di satu negara, dengan korban yang berada di negara lain, dan server yang digunakan untuk melakukan serangan berada di negara ketiga. Situasi ini menciptakan kerumitan dalam menentukan yurisdiksi mana yang berwenang untuk menangani kasus tersebut hal ini menciptakan tantangan dalam mengekstradisi atau membawa pelaku ke pengadilan di Indonesia. Meskipun hukum internasional

[16] Solum, Lawrence B. "The Impact of Technology on the Development of the Law." Journal of Law, Technology & Policy, 2015.

mengakui prinsip-prinsip yurisdiksi seperti yurisdiksi teritorial, nasional, dan universal, penegakan hukum lintas negara sering kali terbatas oleh kerangka hukum domestik masing-masing negara. Karena, tidak semua negara memiliki undang-undang yang secara spesifik mengatur kejahatan siber, atau prosedur ekstradisi yang memungkinkan penyerahan pelaku ke negara yang memiliki yurisdiksi. Akibatnya, pelaku kejahatan siber dapat memanfaatkan perbedaan hukum ini untuk menghindari penuntutan.[17]

c. Sumber Daya dan Kapasitas
   Kejahatan siber, terutama yang menyasar layanan internet banking, memerlukan penanganan yang teknis dan mendalam. Investigasi kejahatan siber melibatkan teknik forensik digital, analisis malware, dan pengawasan komunikasi elektronik yang memerlukan keahlian tinggi. Untuk melakukan investigasi yang efektif, diperlukan juga peralatan canggih dan infrastruktur teknologi yang memadai, seperti perangkat lunak analisis siber dan laboratorium forensik digital. Namun, tidak semua lembaga penegak hukum di Indonesia memiliki akses dan keterampilan di bidang ini, sehingga membatasi kemampuan mereka dalam menangani kasus kejahatan siber yang kompleks sehingga menyebabkan hambatan dalam mendeteksi, menginvestigasi, dan menindak kejahatan siber secara efektif.[18]
d. Tantangan Bagi BSSN (Badan Siber dan Sandi Negara)
   Upaya BSSN untuk mewujudkan keamanan siber Indonesia dalam periode 2020–2024 terdapat beberapa tantangan sebagai berikut:
   1) Revolusi Industri 4.0 yang sedang berlangsung mendorong lahirnya teknologi baru dan peningkatan pengguna internet di Indonesia. Namun, tanpa diimbangi dengan peningkatan kesadaran keamanan siber, ancaman keamanan siber yang semakin masif dapat menyasar infrastruktur penting dan mengancam kedaulatan negara. Keamanan siber yang kuat dan kesadaran yang tinggi menjadi krusial untuk melindungi data dan infrastruktur vital dari potensi serangan.
   2) Pengelolaan keamanan siber nasional mencakup pengelolaan sumber daya manusia dalam keamanan siber dan sandi, penyusunan kebijakan dan regulasi keamanan siber serta strategi nasional. Ini juga melibatkan kolaborasi antara berbagai pihak dan pengembangan teknologi keamanan siber domestik untuk memastikan kedaulatan siber Indonesia. Tujuannya adalah untuk melindungi infrastruktur penting, data sensitif, dan menjaga kedaulatan siber negara.

Sebaliknya, ada beberapa tantangan yang masih perlu diatasi di dalam organisasi BSSN, seperti aspek kelembagaan yang perlu dievaluasi untuk mencapai sasaran strategis, tatalaksana pedoman dan standar operasional prosedur yang belum diterapkan secara menyeluruh, peningkatan kualitas sumber daya manusia, serta sistem informasi yang tidak memadai.[19] Kurangnya sosialisasi dan edukasi terkait keamanan siber di Indonesia menjadi salah satu faktor yang memperburuk situasi kejahatan siber. Masyarakat,

[17] Solum, Lawrence B. "Jurisdiction and the Internet: A New Paradigm for Cyberspace?" Journal of Internet Law, 2010.

[18] Lembaga Riset Siber Indonesia CISSReC. (2020). Analisis Ancaman Siber terhadap Infrastruktur Kritikal di Indonesia.Jakarta:CISSReC.https://www.cissrec.org/search?cx=011105698729379298933%3Asralza0n_eq&cof=FORID%3A11&q=Analisis+Ancaman+Siber+terhadap+Infrastruktur+Kritikal+di+Indonesia.

[19] Peraturan BSSN Nomor 5 Tahun 2020 Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024.

termasuk nasabah bank yang menggunakan layanan internet banking, sering kali tidak memiliki pemahaman yang memadai tentang ancaman siber dan cara melindungi diri dari risiko tersebut. Salah satu dampak dari minimnya sosialisasi dan edukasi adalah rendahnya kesadaran publik tentang ancaman siber. Menurut Arifin banyak individu yang tidak menyadari risiko yang terkait dengan aktivitas online, seperti phishing, malware, dan serangan man-in-the-middle. Ketidaktahuan ini membuat mereka rentan terhadap serangan siber, karena tidak mengambil langkah-langkah pencegahan yang diperlukan, seperti menggunakan kata sandi yang kuat atau menghindari mengklik tautan mencurigakan.[20] Bank sebagai penyedia layanan internet banking juga dinilai belum optimal dalam memberikan edukasi kepada nasabahnya. Sutanto menyatakan bahwa sebagian besar bank di Indonesia belum secara konsisten menyediakan pelatihan atau penyuluhan tentang keamanan siber kepada nasabah mereka. Akibatnya, nasabah sering kali tidak mengetahui cara mengidentifikasi tanda-tanda penipuan atau prosedur yang aman dalam bertransaksi secara online.[21]

4.2 Evolusi Ancaman Siber

Ancaman keamanan digital terus berkembang seiring dengan perkembangan teknologi dan meningkatnya penggunaan layanan internet banking di Indonesia, termasuk di Bank BRI.

1) Kecanggihan Teknik Serangan

   Serangan Phishing dan Spear Phishing: Phishing, yaitu upaya untuk mencuri informasi pribadi melalui penipuan, telah menjadi lebih canggih. Spear phishing, yang menargetkan individu tertentu dengan informasi yang telah dikumpulkan sebelumnya, semakin sulit dideteksi. Penyerang dapat menggunakan data pribadi yang dikumpulkan dari berbagai sumber untuk membuat pesan yang tampak sangat meyakinkan, sehingga korban lebih mungkin untuk terjebak.

   Malware dan Ransomware: Malware yang digunakan untuk menyerang sistem perbankan juga terus berevolusi. Varian baru malware yang lebih sulit dideteksi dan dihapus terus bermunculan. Ransomware, yang mengenkripsi data korban dan meminta tebusan, telah menjadi ancaman serius bagi keamanan siber. Dalam konteks perbankan, serangan semacam ini bisa melumpuhkan layanan dan menimbulkan kerugian besar.[22]

2) Kemampuan Penyerang untuk Menyusup ke Sistem yang Semakin Aman

   Eksploitasi Kerentanan Baru: Penyerang siber selalu mencari dan mengeksploitasi kerentanan baru dalam sistem keamanan. Setiap kali sistem keamanan diperbarui, ada kemungkinan kerentanan baru yang belum ditemukan, yang bisa dimanfaatkan oleh penyerang. Hal ini berarti bahwa ancaman siber tidak pernah sepenuhnya hilang, tetapi terus berubah bentuk.[23]

---

[20]https://www.kominfo.go.id/content/detail/9754/menkominfo-kesadaran-masyarakat-terhadap-cyber-security-masih-rendah/0/sorotan_media.

[21] Sutanto, B. Peran Bank dalam Edukasi Keamanan Siber bagi Nasabah. Bandung: Penerbit ITB, 2019.

[22] Safa, N. S., & Khedher, N. B. (2019). A Survey on Recent Trends and Techniques in Cyber Attacks. Journal of Cyber Security and Privacy, 1(2), 151-166. doi:10.3390/cybersec1010012.

[23] Yuliana, N., & Setiawan, D. (2019). Evolusi Ancaman Siber di Indonesia: Analisis dan Tindakan Penanggulangan. Jurnal Teknologi dan Keamanan Informasi, 11(2), 112-125.

3) Penggunaan Kecerdasan Buatan (AI) dalam Serangan Siber

AI untuk Otomatisasi Serangan: Penyerang mulai menggunakan kecerdasan buatan untuk mengotomatiskan serangan siber, membuat serangan lebih cepat, lebih efektif, dan lebih sulit dideteksi. AI dapat digunakan untuk mempelajari pola pertahanan siber dan menyesuaikan serangan sesuai dengan itu.

Deepfake dan Pemalsuan Digital: Teknologi deepfake, yang menggunakan AI untuk membuat video atau audio palsu yang sangat realistis, dapat digunakan untuk menipu individu atau organisasi. Misalnya, penyerang bisa membuat pesan suara palsu dari seorang eksekutif bank yang meminta transfer dana mendesak, yang bisa sangat meyakinkan dan sulit dikenali sebagai penipuan.[24]

5. Kesimpulan

Beberapa upaya dan cara industri perbankan memastikan keamanan data nasabah untuk masyarkat kecil dan menengah kebawah: (1) Menggunakan enkripsi untuk menjaga keamanan data nasabah saat dikirimkan atau disimpan; (2) Menggunakan sistem otentikasi multi-faktor untuk memastikan hanya orang yang berwenang yang dapat mengakses data nasabah; (3) Menjaga keamanan fisik data nasabah dengan menyimpan data tersebut di server yang terlindungi dengan baik dan menggunakan prosedur keamanan yang ketat di pusat penyimpanan data; (4) Melakukan audit keamanan secara berkala untuk memastikan sistem keamanan masih efektif dan menangani kelemahan keamanan yang mungkin terjadi; (5) Memberikan pelatihan keamanan data kepada karyawan perbankan agar mereka mengetahui pentingnya keamanan data nasabah dan bagaimana cara menjaga keamanan data tersebut; (6) Menandatangani perjanjian kerahasiaan dengan karyawan, vendor dan mitra untuk memastikan bahwa data nasabah tidak akan diungkapkan kepada pihak yang tidak berwenang; (7) Menyediakan mekanisme laporan kebocoran data bagi nasabah sehingga nasabah dapat segera melaporkan jika terjadi kebocoran data pribadinya. Perlindungan hukum terhadap nasabah pengguna internet banking di Bank BRI menghadapi berbagai kendala signifikan. Kompleksitas hukum siber, terutama terkait dengan regulasi yang belum sepenuhnya mengakomodasi perkembangan teknologi baru seperti AI dan blockchain, mempersulit penegakan hukum terhadap pelaku kejahatan siber. Jurisdiksi lintas negara juga menjadi kendala utama, karena kejahatan siber sering melibatkan pelaku dan korban dari berbagai negara, dengan masalah ekstradisi yang kompleks. Selain itu, keterbatasan sumber daya dan kapasitas lembaga penegak hukum, serta proses hukum yang lambat, menambah tantangan dalam penanganan kasus kejahatan siber. Kurangnya sosialisasi dan edukasi tentang keamanan siber di kalangan nasabah juga meningkatkan kerentanan terhadap serangan. Ancaman siber yang terus berkembang, dengan teknik serangan yang semakin canggih dan penggunaan AI dalam serangan, memperburuk situasi dan menjadikannya lebih sulit untuk diidentifikasi dan ditangani secara efektif.

[24] Rifai, M. N., & Kurnia, D. (2019). Ancaman Siber dan Teknik Serangan: Studi Kasus di Indonesia. Jurnal Keamanan Siber dan Privasi, 6(3), 80-95.

Referensi

Antasari, Arga S., et al. *"Pengaruh Penggunaan Internet Banking Terhadap Kepuasan Nasabah (Studi Pada PT. Bank Rakyat Indonesia (Persero) Tbk Cabang Bontang)." Jurnal Administrasi Bisnis S1 Universitas Brawijaya,* vol. 1, (2013).

B. Sutanto. Peran Bank dalam Edukasi Keamanan Siber bagi Nasabah. Bandung: ITB, 2019.

Lembaga Riset Siber Indonesia CISSReC. Analisis Ancaman Siber terhadap Infrastruktur Kritikal di Indonesia. Jakarta, 2020.

M. Hadjon,Philipus. Perlindungan Bagi Rakyat di Indonesia. Surabaya: Bina Ilmu, 1987.

Nubatonis, Orpa Juliana. "Good Faith Governance: Risk Management in Government Procurement Contracts." *vol.* 7 (December 18, 2023): 10–20.

Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

Peraturan BSSN Nomor 5 Tahun 2020 Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024.

Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 Tentang Penerapan Manajemen Resiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

Rifai, M. N., & Kurnia, D. "Ancaman Siber dan Teknik Serangan: Studi Kasus di Indonesia". Jurnal Keamanan Siber dan Privasi. 6(3) (2019): 80-95.

Rosadi, Sinta Dewi. "Prinsip-prinsip perlindungan data pribadi nasabah kartu kredit menurut ketentuan nasional dan implementasinya".Jurnal Sosiohumaniora. Vol.19 No.3 (2017) : 207.

Safa, N. S., & Khedher, N. B. A ."Survey on Recent Trends and Techniques in Cyber Attacks. Journal of Cyber Security and Privacy". 1(2) (2019): 151-166.

Soekanto, Soerjono dan Sri Mamudja. *Penelitian Hukum Normatif* (Suatu Tinjauan Singkat). Jakarta: Rajawali Pers, 2001.

Solum, Lawrence B. "Jurisdiction and the Internet: A New Paradigm for Cyberspace?" Journal of Internet Law (2010): 156.

----------. "The Impact of Technology on the Development of the Law." Journal of Law, Technology & Policy (2015): 53.

Sudarsono. *Kamus Hukum*.Jakarta: Rineka Cipta, 2007.

Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.

Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Yuliana, N., & Setiawan, D. "Evolusi Ancaman Siber di Indonesia: Analisis dan Tindakan Penanggulangan". Jurnal Teknologi dan Keamanan Informasi, 11(2) (2019): 112-125.