el hisbah
Journal of Islamic Economic Law
https://e-journal.uingusdur.ac.id/el_hisbah

Vol. 4 No. 1 (2023)
ISSN : 2797-5819
E-ISSN : 2828-2981

Submitted: Mar 11, 2024 Revised: Apr 15, 2024 Published: May 30, 2024

Perlindungan terhadap Nasabah Akibat Serangan Ciber: Studi di Bank Syariah Indonesia KC Pekalongan Pemuda

Ghifari Wulandari Utami
Universitas Negeri Islam KH. Abdurrahman Wahid
Saifudin
Universitas Islam Negeri Walisongo Semarang
Akhmad Nurasikin
Universitas Wahid Hasyim

ghifariwulandariutami01@gmail.com

Abstract

Cyber attacks have a significant impact on the banking sector. One of the cyber attack incidents occurred at Bank Syariah Indonesia (BSI), including at the BSI Pekalongan Pemuda Branch Office (KC). The attack was marked by disruption of digital services, such as BSI Mobile, ATM machines, and teller services that could not be accessed by customers. This incident reflects the potential for bank negligence in carrying out its obligations to protect customer systems and data. This study aims to analyze the implementation of legal protection for customers due to cyber attacks, as well as to examine the legal consequences arising from the negligence of BSI KC Pekalongan Pemuda in anticipating cyber threats. This study is a juridical-empirical study with a qualitative approach. Data were collected through field studies, including interviews with related parties at BSI KC Pekalongan Pemuda, as well as literature studies covering legal literature, laws and regulations, and legal doctrines. The conceptual and legislative approaches were used to analyze the legal basis for customer protection and the bank's legal responsibility for cyber attacks. The results of the study show that customers are given the right to file a complaint with the Financial Services Authority (OJK) if they experience losses due to cyber attacks. The cyber attack that occurred at BSI KC Pekalongan Pemuda resulted in various legal and non-legal consequences, namely violations of the Personal Data Protection Act, violations of contractual obligations between the bank and customers, potential sanctions from authorities, the possibility of claims for compensation from customers, and losses to the bank's reputation.

Keywords: *Compensation, Customer protection, Cyber attacks*

Abstrak

Serangan siber memberikan dampak yang signifikan terhadap sektor perbankan. Salah satu insiden serangan siber terjadi pada Bank Syariah Indonesia (BSI), termasuk di Kantor Cabang (KC) BSI Pekalongan Pemuda. Serangan tersebut ditandai dengan gangguan layanan digital, seperti BSI Mobile, mesin ATM, dan layanan teller yang tidak dapat diakses oleh nasabah.

Kejadian ini mencerminkan adanya potensi kelalaian bank dalam melaksanakan kewajiban perlindungan terhadap sistem dan data nasabah. Penelitian ini bertujuan untuk menganalisis implementasi perlindungan hukum bagi nasabah akibat serangan siber, serta mengkaji akibat hukum yang timbul dari kelalaian BSI KC Pekalongan Pemuda dalam mengantisipasi ancaman siber. Penelitian ini merupakan penelitian yuridis-empiris dengan pendekatan kualitatif. Data dikumpulkan melalui studi lapangan, termasuk wawancara dengan pihak-pihak terkait di BSI KC Pekalongan Pemuda, serta studi kepustakaan yang mencakup literatur hukum, peraturan perundang-undangan, dan doktrin hukum. Pendekatan konseptual dan perundang-undangan digunakan untuk menganalisis dasar hukum perlindungan nasabah serta tanggung jawab hukum bank terhadap serangan siber. Hasil penelitian menunjukkan bahwa nasabah diberikan hak untuk mengajukan pengaduan kepada Otoritas Jasa Keuangan (OJK) apabila mengalami kerugian akibat serangan siber. Serangan siber yang terjadi di BSI KC Pekalongan Pemuda menimbulkan berbagai akibat hukum dan non-hukum, yaitu pelanggaran terhadap Undang-Undang Perlindungan Data Pribadi, pelanggaran kewajiban kontraktual antara bank dan nasabah, potensi sanksi dari otoritas, kemungkinan timbulnya tuntutan ganti rugi dari pihak nasabah, serta kerugian reputasi bank.

Kata Kunci: Ganti rugi, Perlindungan nasabah, Serangan siber

Pendahuluan

Perkembangan teknologi informasi telah membawa dampak yang signifikan terhadap berbagai aspek kehidupan, termasuk dalam sektor keuangan (Hutomo, 2019; Rahman & Astria, 2023). Seiring dengan kemajuan tersebut, serangan siber menjadi ancaman yang semakin serius bagi lembaga keuangan, khususnya perbankan (Pakina & Solekhan, 2024; Restika & Sonita, 2023). Serangan yang dilakukan melalui jaringan internet berpotensi menimbulkan dampak besar terhadap pertumbuhan kejahatan digital (Ariyaningsih et al., 2023; Hapsari & Pambayun, 2023). Dalam konteks layanan *internet banking* pada Bank Syariah Indonesia (BSI), kelemahan dalam sistem keamanan berpotensi dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan tindakan kriminal yang merugikan nasabah (Azizah et al., 2024).

Serangan siber dapat berdampak langsung pada pencurian data, penipuan keuangan, gangguan layanan, serta kerugian finansial bagi nasabah sebagai konsumen layanan perbankan (Putri et al., 2023). Sebagai ilustrasi, salah satu kasus serangan siber terjadi pada Bank Syariah Indonesia, termasuk di Kantor Cabang (KC) Pekalongan Pemuda. Insiden ini bermula dari gangguan pada layanan digital seperti BSI Mobile, mesin Anjungan Tunai Mandiri (ATM), dan layanan teller di kantor cabang yang menyebabkan nasabah tidak dapat mengakses layanan perbankan secara normal.

Kejadian tersebut mengancam keamanan dan privasi data nasabah, yang jumlahnya mencapai sekitar 14 juta secara nasional, di antaranya nasabah BSI KC Pekalongan Pemuda yang jumlahnya 48.200 di tahun 2022 (Mochamad Yusuf, 2023). Akibat dari serangan siber ini, sejumlah nasabah mengalami hambatan dalam bertransaksi, bahkan sebagian kehilangan dana. Kondisi ini berdampak pada munculnya kekecewaan dan menurunnya tingkat kepercayaan nasabah terhadap institusi perbankan tersebut.

Serangan siber yang menimpa lembaga keuangan seperti BSI merupakan indikasi kelalaian institusi dalam memenuhi kewajiban hukum sebagaimana diatur dalam peraturan perundang-undangan yang berlaku. Dalam hal ini, BSI KC Pekalongan Pemuda diduga telah melanggar ketentuan Pasal 4 Ayat (1) Undang-Undang Nomor 8 Tahun 1999 tentang

Perlindungan Konsumen, yang menyatakan bahwa konsumen berhak atas kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang dan/atau jasa (Ritonga, 2020; Suhadi & Fadilah, 2021).

Lebih lanjut, pelanggaran juga dapat ditinjau dari ketentuan Pasal 21 Ayat (1) dan (2) Peraturan Otoritas Jasa Keuangan (POJK) Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum (Fitriani et al., 2023). Regulasi tersebut mewajibkan bank untuk menjaga ketahanan siber melalui proses identifikasi aset, ancaman, dan kerentanan; perlindungan aset; deteksi insiden siber; serta penanggulangan dan pemulihan insiden siber (Andi & Anis, 2024).

Pasal 25 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan juga menegaskan bahwa pelaku usaha jasa keuangan wajib menjaga keamanan simpanan, dana, atau aset konsumen yang berada dalam tanggung jawabnya (Ahmad & Mujib, 2023; Wibowo, 2019). Demikian pula, Pasal 11 Ayat (5) POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan mengharuskan penggunaan teknologi informasi yang andal serta kewajiban pengecekan keamanan secara berkala terhadap data pribadi konsumen (Anisa & Syahrin, 2023).

Dalam konteks ini, perlindungan terhadap nasabah sebagai konsumen menjadi aspek yang sangat krusial. Nasabah merupakan aset strategis yang wajib dilindungi oleh pihak bank dari berbagai risiko, termasuk ancaman serangan siber. Hal ini sejalan dengan Pasal 4 Ayat (8) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang memberikan hak kepada konsumen untuk memperoleh kompensasi, ganti rugi, dan/atau penggantian apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian.

Selain itu, Pasal 19 Ayat (1) undang-undang yang sama menyatakan bahwa pelaku usaha bertanggung jawab memberikan ganti rugi atas kerusakan, pencemaran, dan/atau kerugian yang dialami konsumen sebagai akibat penggunaan barang dan/atau jasa. Dalam konteks pelindungan data pribadi, Pasal 12 Ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menyebutkan bahwa subjek data pribadi berhak menggugat dan memperoleh ganti rugi atas pelanggaran terhadap data pribadinya. Akhirnya, Pasal 29 Ayat (1) POJK Nomor 1/POJK.07/2023 menegaskan tanggung jawab pelaku usaha jasa keuangan atas kerugian konsumen yang disebabkan oleh kesalahan atau kelalaian pengurus, pegawai, atau pihak ketiga yang bekerja untuk kepentingan lembaga tersebut (Suryanto & Riyanto, 2024).

Beberapa studi sebelumnya telah membahas permasalahan ini dalam berbagai konteks. Misalnya, Nugraha dan Njatrijani (2016) meneliti perlindungan hukum terhadap nasabah yang mengalami pembobolan akun melalui metode malware dalam layanan *internet banking*, dan menyimpulkan bahwa tanggung jawab bank menjadi aspek penting dalam menjamin keamanan data nasabah. Penelitian oleh Chairunnisa, Murwadji, dan Harrieti (2023) menyoroti kejahatan *phishing* dan *hacking* serta pentingnya pertanggungjawaban bank digital berdasarkan hukum positif Indonesia. Afifah (2023) secara khusus menganalisis serangan ransomware yang menimpa Bank Syariah Indonesia (BSI), dan menemukan bahwa lemahnya sistem mitigasi risiko digital dapat berdampak langsung pada kerugian nasabah serta menurunkan kepercayaan publik terhadap institusi perbankan. Sementara itu, Putri, Andriani, dan Nabbila (2023) memaparkan bahwa insiden kebocoran data pada sistem digital banking BSI menuntut adanya regulasi yang lebih kuat dan sistem keamanan yang lebih andal untuk melindungi konsumen.

Namun demikian, masih minim kajian yang mengangkat kasus serangan siber dari sudut pandang lokasi cabang secara spesifik, serta mengkaji keterkaitan antara kelalaian institusi perbankan dan pelanggaran hak-hak hukum konsumen berdasarkan regulasi perundang-undangan yang berlaku. Oleh karena itu, penelitian ini memiliki kebaruan dalam mengkaji kasus serangan siber pada BSI Kantor Cabang Pekalongan Pemuda, serta menganalisis tanggung jawab hukum lembaga keuangan terhadap nasabah yang dirugikan. Penelitian ini bertujuan untuk menganalisis implementasi perlindungan hukum terhadap nasabah akibat dari serangan siber, serta mengkaji implikasi yuridis yang timbul akibat kelalaian Bank Syariah Indonesia Kantor Cabang Pekalongan Pemuda dalam mengantisipasi dan menanggulangi potensi ancaman siber.

Metode Penelitian

Jenis penelitian yuridis-empiris untuk menjembatani antara teori hukum dan kenyataan sosial yang terjadi akibat serangan siber pada sektor perbankan (Bachtiar, 2019). Pendekatan penelitian yang digunakan adalah pendekatan kualitatif, dengan memadukan pendekatan konseptual dan pendekatan perundang-undangan (Muhaimin, 2020). Data penelitian terdiri dari data primer dan data sekunder. Data primer diperoleh langsung dari lapangan melalui wawancara dengan pihak internal BSI KC Pekalongan Pemuda dan nasabah yang terdampak, sedangkan data sekunder diperoleh dari dokumen hukum seperti peraturan perundang-undangan, literatur ilmiah, jurnal hukum, dan putusan pengadilan yang relevan. Teknik pengumpulan data dilakukan melalui wawancara mendalam (in-depth interviews) dan studi kepustakaan (library research). Teknik analisis data yang digunakan adalah analisis deskriptif-kualitatif, yaitu dengan menggambarkan, menafsirkan, dan mengkaji data yang diperoleh secara sistematis berdasarkan kaidah hukum. Analisis dilakukan dengan mengaitkan data empiris dengan teori hukum dan ketentuan peraturan perundang-undangan, sehingga dapat diperoleh kesimpulan hukum yang komprehensif (Fajar & Achmad, 2010).

Hasil dan Pembahasan

Implementasi Perlindungan Hukum Terhadap Nasabah Akibat Serangan Siber di BSI KC Pekalongan Pemuda

Subjek hukum dalam perlindungan konsumen harus memenuhi kriteria yang ditetapkan dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Undang-undang ini secara eksplisit menjelaskan bahwa perlindungan diberikan kepada konsumen akhir, bukan kepada konsumen antara (Negara & Satria, 2021; Siswanto et al., 2022). Dalam hal ini, nasabah Bank Syariah Indonesia, termasuk yang berada di Kantor Cabang Pekalongan Pemuda, memenuhi kualifikasi sebagai konsumen akhir sebagaimana diatur dalam Pasal 1 Ayat (2) UU Perlindungan Konsumen, yang menyatakan bahwa: “Konsumen adalah setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri sendiri, keluarga, orang lain, maupun makhluk hidup lain dan tidak untuk diperdagangkan (Fista et al., 2023).”

Berdasarkan definisi tersebut, hubungan antara nasabah dan Bank Syariah Indonesia KC Pekalongan Pemuda merupakan hubungan hukum antara konsumen dan pelaku usaha. Perlindungan hukum terhadap konsumen mencakup penggunaan barang dan/atau jasa, sebagaimana diatur dalam Pasal 1 Ayat (4) dan (5) Undang-Undang yang sama, yang menyatakan bahwa: “Barang adalah setiap benda baik berwujud maupun tidak berwujud,

baik bergerak maupun tidak bergerak, dapat dihabiskan maupun tidak dapat dihabiskan, yang dapat untuk diperdagangkan, dipakai, dipergunakan, atau dimanfaatkan oleh konsumen." Sedangkan

"jasa adalah setiap layanan yang berbentuk pekerjaan atau prestasi yang disediakan bagi masyarakat untuk dimanfaatkan oleh konsumen."

Dengan demikian, telah jelas bahwa nasabah BSI KC Pekalongan Pemuda yang memanfaatkan layanan perbankan berhak mendapatkan perlindungan sebagai konsumen akhir. Hak-hak nasabah untuk memperoleh perlindungan atas kenyamanan, keamanan, dan keselamatan dalam menggunakan layanan perbankan dijamin oleh ketentuan Pasal 4 Ayat (1) Undang-Undang Perlindungan Konsumen menjelaskan bahwa: "Hak atas kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang dan/atau jasa." Oleh sebab itu, ketika terjadi serangan siber yang berdampak pada terganggunya layanan perbankan, termasuk ketidakmampuan nasabah dalam mengakses dananya atau menggunakan fasilitas perbankan secara normal, maka nasabah berhak menuntut pertanggungjawaban dari pihak bank selaku pelaku usaha. Implementasi perlindungan hukum ini tidak hanya mencerminkan tanggung jawab hukum institusi keuangan, tetapi juga menjadi indikator komitmen terhadap prinsip perlindungan konsumen dalam sistem hukum nasional.

Hak-hak yang seharusnya diterima oleh nasabah Bank Syariah Indonesia, termasuk yang berada di Kantor Cabang Pekalongan Pemuda, telah dilanggar akibat adanya serangan siber yang mengancam keamanan data pribadi mereka. Padahal, sudah menjadi kewajiban bank untuk menjamin keamanan dan kerahasiaan data nasabah sebagai bentuk tanggung jawab hukum dan etis dalam menjalankan layanan keuangan. Serangan siber tersebut menunjukkan adanya kelalaian pihak bank dalam mengimplementasikan sistem perlindungan data yang memadai, sehingga menimbulkan risiko hukum dan kehilangan kepercayaan publik.

Perlindungan terhadap konsumen dalam layanan perbankan, khususnya berkaitan dengan kepastian hukum dan keterbukaan informasi pada layanan internet banking, sangat penting untuk diwujudkan melalui regulasi yang tegas dan implementatif. Nasabah sebagai pengguna jasa perbankan memiliki hak untuk mendapatkan jaminan keamanan serta akses terhadap informasi yang transparan guna menghindari kerugian akibat kejahatan teknologi. Oleh karena itu, lembaga perbankan dituntut untuk memiliki dasar hukum dan sistem operasional yang mampu mengimbangi dinamika perkembangan teknologi informasi dan komunikasi, agar dapat menjalankan fungsi perbankan secara efisien, sehat, dan wajar (Kehakiman, 2019).

Dalam hal ini, Marulak Pardede (2020) menyebutkan bahwa sistem perlindungan terhadap nasabah penyimpan dana di Indonesia dapat dibedakan menjadi dua bentuk, yaitu perlindungan secara implisit dan eksplisit. Perlindungan implisit diperoleh melalui pengawasan dan pembinaan bank yang efektif untuk mencegah kebangkrutan, yang meliputi pengaturan dalam peraturan perundang-undangan, pengawasan oleh Bank Indonesia, pemeliharaan kesehatan bank, penerapan prinsip kehati-hatian, serta penyediaan informasi risiko yang transparan kepada nasabah. Sementara itu, perlindungan eksplisit dilakukan melalui pembentukan lembaga penjamin simpanan yang bertugas mengganti dana masyarakat jika terjadi kegagalan bank, sebagaimana diatur dalam Keputusan Presiden RI Nomor 26 Tahun 1998 dan Undang-Undang Nomor 24 Tahun 2004 tentang Lembaga Penjamin Simpanan (LPS).

Sejalan dengan pandangan tersebut, Hermansyah membagi perlindungan hukum terhadap nasabah ke dalam dua kategori, yaitu perlindungan tidak langsung (indirect

protection) dan perlindungan langsung (direct protection). Perlindungan tidak langsung dilakukan oleh pihak bank melalui penerapan prinsip kehati-hatian dalam operasional perbankan untuk menghindari risiko kerugian nasabah. Adapun perlindungan langsung diberikan dalam bentuk penetapan hak istimewa bagi nasabah penyimpan dana dan keberadaan lembaga asuransi deposito sebagai bentuk kompensasi atas risiko kehilangan dana. Dengan demikian, apabila terjadi gangguan layanan akibat serangan siber, seperti yang terjadi di BSI Kantor Cabang Pekalongan Pemuda, maka nasabah memiliki dasar hukum untuk menuntut pemulihan atas kerugian yang dialami. Hal ini sejalan dengan ketentuan Pasal 4 ayat (8) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang menyatakan bahwa konsumen berhak untuk mendapatkan kompensasi, ganti rugi, dan/atau penggantian apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya.

Apabila dikaitkan dengan peristiwa serangan siber yang mengancam data pribadi nasabah dan harta kekayaan mereka, Bank Syariah Indonesia (BSI), termasuk BSI Kantor Cabang (KC) Pekalongan Pemuda, sebagai badan hukum, seharusnya memiliki standar operasional yang memadai dalam hal layanan dan keamanan untuk kepentingan nasabah. Dalam hal ini, bank bertanggung jawab untuk menjaga keamanan data nasabah sebagai bagian dari kewajiban perlindungan hak-hak konsumen. Oleh karena itu, jika serangan siber terjadi dan data nasabah terancam, bank dapat dianggap telah melanggar kewajibannya dalam menjaga keamanan data dan informasi pribadi nasabah. Kewajiban pelaku usaha, dalam hal ini Bank Syariah Indonesia yang memiliki cabang di berbagai daerah, termasuk di Kantor Cabang Pekalongan Pemuda, diatur dalam Pasal 7 ayat 4 dan 7 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Pasal-pasal tersebut mengatur bahwa pelaku usaha wajib menjamin mutu barang dan/atau jasa yang diproduksi dan/atau diperdagangkan sesuai dengan standar mutu yang berlaku, serta memberikan kompensasi, ganti rugi, dan/atau penggantian apabila barang dan/atau jasa yang diterima atau dimanfaatkan oleh konsumen tidak sesuai dengan perjanjian.

Sebagaimana diatur dalam undang-undang tersebut, bank diwajibkan untuk menjamin mutu layanan yang sesuai dengan standar yang berlaku dan memberikan ganti rugi jika nasabah mengalami kerugian akibat layanan yang tidak sesuai. Untuk itu, Bank Syariah Indonesia Kantor Cabang Pekalongan Pemuda mengupayakan perlindungan kepada nasabahnya melalui beberapa langkah mitigasi risiko akibat serangan siber. Karyawan BSI KC Pekalongan Pemuda menjelaskan bahwa jika nasabah mengalami gangguan, mereka dapat mengajukan pengaduan dengan menghubungi call center BSI 14040 atau datang langsung ke cabang terdekat. Customer Service (CS) akan membantu nasabah dalam membuat tiket pengaduan dan meminta nomor telepon yang aktif, yang nantinya digunakan untuk menginformasikan perkembangan penyelesaian pengaduan (Inisial EE, 2023). Nasabah juga dapat langsung datang ke cabang BSI terdekat untuk membuat tiket pengaduan. Namun, jika terjadi keterlambatan dalam penyelesaian akibat gangguan pada sistem atau ketidaksesuaian dengan Service Level Agreement (SLA), pengaduan biasanya dapat diselesaikan dalam waktu maksimal 14 hari kerja, meskipun terkadang proses penyelesaian memerlukan waktu yang lebih lama (Inisial FF, 2023). Selain itu, Bank Syariah Indonesia menekankan pentingnya bagi nasabah untuk tidak memberikan informasi sensitif seperti PIN, OTP, atau password kepada siapapun, termasuk pegawai BSI, guna menghindari potensi penipuan. Nasabah juga diingatkan untuk selalu memverifikasi informasi yang beredar dan melakukan pengecekan ulang apabila diperlukan (Inisial GG, 2023).

Dalam konteks perlindungan hak konsumen, nasabah sebagai konsumen berhak untuk mendapatkan perlindungan hukum penuh, terutama dalam menghadapi ancaman serangan siber ini. Oleh karena itu, langkah-langkah yang diambil oleh Bank Syariah Indonesia, termasuk BSI KC Pekalongan Pemuda, bertujuan untuk menjaga keamanan data dan dana nasabah. Sebagai upaya perlindungan, BSI menyatakan bahwa mereka memastikan data dan dana nasabah aman, serta memastikan keamanan dalam bertransaksi. Selain itu, BSI juga berkomitmen untuk bekerja sama dengan otoritas terkait dalam mengatasi isu kebocoran data (Indonesia C., 2024). Mengenai isu serangan siber, BSI berharap masyarakat tidak mudah mempercayai informasi yang berkembang dan selalu melakukan pengecekan ulang atas informasi yang beredar, sambil memastikan bahwa data dan dana nasabah tetap aman (Indonesia C., 2024). Selain itu, BSI memiliki Standar Operasional Prosedur (SOP) keamanan siber yang telah disusun berdasarkan POJK 11/03/2022, di mana bank berkewajiban untuk meningkatkan prosedur operasional terkait pengelolaan keamanan siber (Indonesia C., 2024). Sebagai pelaku bisnis di era teknologi informasi yang semakin berkembang, BSI juga mengingatkan pentingnya kewaspadaan dan kolaborasi antara pelaku bisnis, pemerintah, regulator, serta masyarakat untuk mencegah berkembangnya kejahatan siber (Binekasri, 2024).

Upaya perlindungan konsumen yang diberikan oleh pemerintah dalam hal penyelesaian sengketa antara nasabah dan Bank Syariah Indonesia (BSI), termasuk BSI Kantor Cabang Pekalongan Pemuda, mengacu pada Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK). Dalam konteks ini, sengketa perbankan dapat diajukan melalui pengaduan atau keluhan kepada Otoritas Jasa Keuangan (OJK) sebagai lembaga yang bertugas melindungi kepentingan konsumen dan masyarakat. Berdasarkan fungsinya, OJK memiliki peran penting dalam pengawasan industri jasa keuangan untuk menjaga kepentingan konsumen dan stabilitas sistem keuangan.

Berdasarkan keterangan yang diberikan oleh karyawan BSI Kantor Cabang Pekalongan Pemuda, upaya yang dilakukan untuk menyelesaikan permasalahan akibat serangan siber adalah sebagai berikut: “Kami mengikuti arahan dari pusat, sesuai dengan yang disampaikan oleh Direktur Utama BSI, dan terus melakukan proses normalisasi dengan fokus utama menjaga dana dan data nasabah tetap aman.” “BSI memiliki Tim Petugas Keamanan Informasi atau Group Chief Information Security Officer (CISO) yang bertugas dan bertanggung jawab dalam menjaga keamanan data dan privasi nasabah.” “BSI menerapkan Business Continuity Plan (BCP), yang terdiri dari serangkaian tindakan yang dilakukan perusahaan apabila terjadi hal-hal yang tidak terduga. Dengan diterapkannya BCP, transaksi masih dapat dilakukan melalui teller, meskipun ada pembatasan dalam melakukan transaksi selama gangguan sistem tersebut. Ketika uang masuk dari nasabah, dana tersebut akan masuk ke rekening BSI di Bank Indonesia (BI), dan BSI akan menyusun daftar transaksi yang akan diposting secara internal ke masing-masing akun nasabah.” (Inisial EE, 2023) “Menurut saya, penguatan layanan IT melalui pembaruan perangkat lunak dan perangkat keras, termasuk penggantian komputer baru di BSI KC Pekalongan Pemuda, sangat diperlukan.” (Inisial FF, 2023) “Nasabah BSI diharapkan segera mengganti semua kredensial m-banking, internet banking, dan PIN ATM nasabah.” (Inisial GG, 2023)

Terkait dengan standar keamanan, produk yang berkaitan dengan Kesehatan, Keselamatan, Keamanan, dan Lingkungan (K3L) memiliki sifat yang wajib, termasuk dalam sektor perbankan yang sangat menekankan prinsip keamanan. Namun, dalam prakteknya, standardisasi keamanan yang diterapkan oleh Bank Syariah Indonesia, termasuk BSI KC

Pekalongan Pemuda, belum dilaksanakan dengan optimal. Hal ini terbukti dari kejadian serangan siber yang melibatkan kelompok hacker, LockBit, yang berhasil meretas sistem keamanan data BSI.

Untuk mencegah kejadian serupa di masa depan, pihak yang mengatur regulasi fintech perlu memperkuat sistem keamanan data. Menurut Ardi Sutedja, Kepala Indonesia Cyber Security Forum, penguatan infrastruktur dan regulasi saja tidak cukup. Keterbukaan informasi terkait serangan siber harus dijalankan sebagai bagian dari budaya yang melibatkan masyarakat untuk berpartisipasi dalam melindungi keamanan data dan sistem digital. Ia menegaskan: "Jika keterbukaan ini dijalankan sebagai budaya, masyarakat juga akan ikut berpartisipasi dalam mencari solusi dan berperan aktif dalam melindungi data dan sistem digital. Tanggung jawab keamanan siber merupakan tanggung jawab kolektif, tidak hanya terbatas pada pemilik jaringan atau infrastruktur." (Hidayat, 2024)

Namun, selama pemerintah tidak transparan dalam menangani kasus kebocoran data dan tidak memiliki aturan sanksi yang tegas, peristiwa serupa akan terus mengancam di masa mendatang, terutama dengan meningkatnya ekosistem digital. Akibatnya, masyarakat yang mempercayakan datanya kepada lembaga perbankan akan menjadi korban.

Kebocoran data ini jelas melanggar prinsip data security, data privacy, dan etika. Tindakan pencurian data menyebabkan hilangnya kerahasiaan, privasi, ketersediaan, dan integritas informasi nasabah Bank Syariah Indonesia. Kejadian ini mengakibatkan kerugian baik materiil maupun non-materiil bagi nasabah dan merusak kredibilitas bank di mata masyarakat. Meskipun demikian, BSI telah berupaya mengimplementasikan berbagai protokol keamanan untuk melindungi nasabahnya. Dalam menangani serangan ransomware, perusahaan yang menjadi korban harus segera menghubungi pihak penegak hukum, lembaga penanganan darurat serangan siber, atau perusahaan keamanan siber.

Perkembangan digitalisasi di sektor perbankan memang meningkatkan risiko serangan siber. Serangan siber yang semakin marak ini mendorong kebutuhan untuk meningkatkan ketahanan siber (cyber resilience) melalui penguatan keamanan siber (cyber security). Penguatan ini menjadi inisiatif penting di berbagai sektor industri, termasuk sektor perbankan, untuk mengatasi risiko siber. (OJK, 2024)

Sektor keuangan, terutama perbankan, merupakan salah satu target utama serangan siber, baik di tingkat global maupun di Indonesia. Berdasarkan catatan Bank for International Settlements (BIS), banyak regulator perbankan di negara-negara lain yang telah menerapkan kebijakan khusus terkait dengan keamanan siber. Beberapa best practices yang diadopsi oleh berbagai negara untuk meningkatkan keamanan siber antara lain meliputi kebijakan pengelolaan keamanan siber, kewajiban penilaian risiko siber, pengujian kerentanan teknologi informasi bank, penilaian tingkat maturitas siber, dan pelaksanaan pengujian keamanan siber bank. Menurut Dr. Pratama Persadha, Kepala Lembaga Riset Keamanan Siber CISSReC, sistem pertahanan siber di bank-bank Indonesia masih dinilai kurang memadai, yang menjadi masalah lebih luas setelah serangan siber yang menimpa Bank Indonesia pada awal 2022. (Ayu, 2024)

Ke depan, penting bagi Bank Syariah Indonesia dan bank-bank lain di Indonesia untuk memperkuat sistem pertahanan digital mereka. Sektor keuangan, khususnya perbankan, harus lebih siap menghadapi ancaman siber yang semakin meningkat. Sebagai langkah untuk membangun kembali kepercayaan nasabah di BSI KC Pekalongan Pemuda, upaya yang dapat dilakukan antara lain dengan menyampaikan informasi terkait pemulihan layanan melalui WA Blast kepada nasabah, serta mengadakan kunjungan atau silaturahmi dengan nasabah yang

memiliki dana lebih untuk menggunakan kembali layanan BSI dengan keyakinan bahwa dana dan data mereka aman. (Inisial EE, 2024)

Penerapan kebijakan terkait pengelolaan keamanan siber, penilaian risiko siber, pengujian kerentanan teknologi, dan pelaksanaan pengujian keamanan siber yang sesuai dengan best practices internasional harus dipertimbangkan untuk mengatasi potensi ancaman dan kerentanannya. Meskipun penguatan jaringan dan sistem melalui firewall, enkripsi data, dan pemantauan aktif dapat mengurangi risiko serangan, tidak ada jaminan bahwa sistem akan sepenuhnya aman. Oleh karena itu, mitigasi yang tepat dan persiapan yang matang sangat diperlukan untuk menghadapi potensi serangan ransomware. Selain itu, dalam konteks pertanggungjawaban hukum, Bank Syariah Indonesia harus mempertanggungjawabkan kesalahan yang terjadi, sesuai dengan prinsip pertanggungjawaban mutlak dalam Undang-Undang Perlindungan Konsumen. (Pasal 1365 KUHPerdata)

Berdasarkan hasil pembahasan di atas, implementasi perlindungan hukum terhadap nasabah Bank Syariah Indonesia (BSI) KC Pekalongan Pemuda akibat serangan siber telah memiliki dasar yuridis yang kuat, baik dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen maupun dalam regulasi sektoral seperti Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan dan Undang-Undang Nomor 24 Tahun 2004 tentang Lembaga Penjamin Simpanan. Dalam konteks ini, nasabah diposisikan sebagai konsumen akhir yang berhak mendapatkan perlindungan atas kenyamanan, keamanan, dan keselamatan dalam menggunakan layanan jasa keuangan, termasuk perlindungan atas data pribadi dan akses terhadap dana mereka.

Namun demikian, insiden serangan siber yang menimpa BSI KC Pekalongan Pemuda menunjukkan adanya celah dalam sistem keamanan informasi yang seharusnya menjadi prioritas utama lembaga keuangan. Serangan ini menandakan belum optimalnya implementasi standar perlindungan siber, meskipun bank telah memiliki SOP dan Business Continuity Plan (BCP). Ketidaksesuaian antara implementasi perlindungan hukum dengan ekspektasi perlindungan konsumen tersebut mengindikasikan kelemahan dalam pengawasan, kesiapan teknologi, dan transparansi informasi. Dalam perspektif perlindungan konsumen, kelalaian bank dalam menjaga keamanan data dan akses layanan nasabah dapat digolongkan sebagai bentuk pelanggaran terhadap hak konsumen dan kewajiban pelaku usaha sebagaimana diatur dalam Pasal 4 dan Pasal 7 Undang-Undang Perlindungan Konsumen.

Upaya penyelesaian oleh pihak BSI seperti pembentukan tim keamanan informasi (CISO), penerapan BCP, dan imbauan untuk tidak membagikan informasi sensitif kepada pihak ketiga memang telah dilakukan, namun dinilai belum cukup kuat untuk mengembalikan kepercayaan nasabah. Fakta bahwa sistem dapat diretas oleh kelompok kriminal siber internasional menunjukkan bahwa keamanan data belum menjadi prioritas utama dalam kebijakan strategis bank. Oleh karena itu, penguatan sistem keamanan digital yang sejalan dengan *best practices* internasional, peningkatan keterbukaan informasi kepada publik, dan penguatan peran pengawasan oleh OJK menjadi keharusan yang tidak dapat ditunda. Dalam konteks pertanggungjawaban hukum, bank sebagai pelaku usaha harus bertanggung jawab atas kerugian yang diderita nasabah berdasarkan prinsip pertanggungjawaban mutlak (strict liability) sebagaimana termuat dalam doktrin hukum perdata dan prinsip perlindungan konsumen.

Implikasi Yuridis Akibat Kelalaian dalam Mengantisipasi dan Menanggulangi Potensi Ancaman Siber

Serangan siber yang dialami oleh Bank Syariah Indonesia (BSI), termasuk Kantor Cabang Pekalongan Pemuda, membawa dampak hukum yang kompleks, terutama apabila pihak bank tidak menjalankan kewajiban perlindungan data sesuai regulasi yang berlaku. Salah satu implikasi yuridis yang paling menonjol adalah potensi pelanggaran terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 12 ayat (1) undang-undang tersebut menyatakan bahwa subjek data pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran dalam pemrosesan data. Dalam konteks ini, bank berperan sebagai pengendali data pribadi, yang bertanggung jawab dalam menentukan tujuan serta cara pemrosesan data nasabah. Kewajiban ini dipertegas dalam Pasal 47 yang menegaskan bahwa pengendali data wajib menunjukkan akuntabilitas dalam melaksanakan prinsip perlindungan data pribadi. Apabila terjadi kebocoran data, maka bank harus menanggung tanggung jawab penuh baik secara administratif maupun perdata atas kerugian yang dialami oleh nasabah.

Selain itu, kelalaian bank dalam mengantisipasi serangan siber juga dapat dikualifikasikan sebagai pelanggaran kewajiban kontraktual. Hal ini relevan dengan Pasal 4 ayat (1) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen yang menjamin hak konsumen atas rasa aman dan nyaman dalam mengakses layanan. Apabila layanan perbankan terganggu dan menyebabkan kerugian finansial bagi nasabah, maka hal ini dapat dianggap sebagai wanprestasi. Peraturan Otoritas Jasa Keuangan (POJK) juga menegaskan tanggung jawab bank dalam melindungi kepentingan konsumen. POJK Nomor 6 Tahun 2022 mewajibkan pelaku usaha jasa keuangan untuk bertanggung jawab atas kerugian konsumen akibat kesalahan atau kelalaian, termasuk yang dilakukan oleh pihak ketiga. Dalam kaitannya dengan keamanan teknologi informasi, POJK Nomor 11/POJK.03/2022 mewajibkan bank untuk menjaga ketahanan siber melalui proses identifikasi ancaman, perlindungan aset, deteksi, serta pemulihan insiden siber. Bank juga diwajibkan menjaga keamanan aset nasabah sebagaimana diatur dalam Pasal 25 POJK Nomor 1/POJK.07/2013, serta menjamin keamanan data melalui teknologi informasi yang andal sesuai Pasal 11 ayat (5) POJK Nomor 6 Tahun 2022 . Serangan siber yang melanggar prinsip keamanan dan etika digital mengindikasikan kegagalan bank dalam memenuhi kewajiban tersebut, yang membuka ruang gugatan oleh nasabah.

Kegagalan bank dalam menerapkan sistem keamanan yang memadai juga dapat menimbulkan sanksi administratif dari regulator. Berdasarkan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK), OJK memiliki kewenangan untuk mengawasi dan memberikan sanksi terhadap pelanggaran yang terjadi di sektor jasa keuangan, termasuk dalam hal ketidakpatuhan terhadap standar keamanan siber. OJK bersama Badan Siber dan Sandi Negara (BSSN) memiliki kewenangan untuk menjatuhkan sanksi apabila ditemukan bahwa bank tidak melaporkan insiden dengan benar atau tidak memiliki sistem mitigasi risiko yang memadai.

Dampak non-yuridis namun tetap signifikan adalah kerusakan reputasi institusi perbankan akibat serangan siber. Reputasi yang menurun berdampak pada kepercayaan nasabah, investor, dan masyarakat luas, yang pada akhirnya dapat memengaruhi stabilitas finansial dan keberlangsungan usaha bank. Kehilangan kepercayaan publik merupakan kerugian strategis yang sering kali memerlukan waktu dan sumber daya besar untuk dipulihkan.

Lebih lanjut, implikasi hukum lainnya adalah potensi tuntutan ganti rugi dari nasabah yang mengalami kerugian akibat kelalaian pihak bank dalam mencegah dan menangani insiden siber. Kerugian tersebut dapat berupa kehilangan dana, pencurian identitas, ataupun gangguan terhadap aktivitas finansial. Berdasarkan Pasal 4 ayat (8) dan Pasal 19 ayat (1) Undang-Undang Nomor 8 Tahun 1999, pelaku usaha bertanggung jawab memberikan ganti rugi apabila barang atau jasa yang diberikan tidak sesuai dengan perjanjian. Hal ini juga ditegaskan dalam Pasal 29 ayat (1) POJK Nomor 1/POJK.07/2023 yang mewajibkan tanggung jawab pelaku usaha atas kerugian yang timbul dari kelalaian pihak internal maupun pihak ketiga. Dalam konteks hukum perdata, dasar gugatan tersebut dapat merujuk pada ketentuan Pasal 1365 KUH Perdata mengenai perbuatan melawan hukum (PMH). Oleh karena itu, nasabah yang mengalami kerugian secara individu maupun kolektif memiliki dasar hukum untuk mengajukan gugatan terhadap bank, dan bank berkewajiban memberikan kompensasi yang sepadan dengan tingkat kerugian yang dialami.

Simpulan

Perlindungan hukum terhadap nasabah dalam konteks keuangan digital tidak hanya menuntut pemenuhan kewajiban secara yuridis, tetapi juga menuntut penguatan standar teknis keamanan siber, pembaruan perangkat kebijakan internal bank, serta peningkatan peran regulator dalam membentuk sistem pengawasan yang lebih tanggap dan transparan. Kolaborasi antara lembaga perbankan, pemerintah, regulator, serta masyarakat menjadi syarat penting dalam mewujudkan ekosistem digital yang aman, adil, dan berkelanjutan bagi seluruh pihak yang terlibat dalam transaksi keuangan. Implikasi yuridis atas serangan siber menunjukkan bahwa aspek keamanan digital tidak dapat dipisahkan dari tata kelola hukum dalam industri jasa keuangan. Kelalaian tidak lagi sekadar persoalan teknis, melainkan juga dapat dikonstruksikan sebagai perbuatan melawan hukum yang menimbulkan tanggung jawab ganti rugi. Dengan demikian, penting bagi institusi perbankan untuk tidak hanya mematuhi regulasi secara formal, tetapi juga menerapkan pendekatan strategis yang integratif dalam membangun sistem ketahanan siber yang adaptif, akuntabel, dan berorientasi pada perlindungan konsumen. Penelitian selanjutnya disarankan untuk mengkaji efektivitas mekanisme pengawasan dan penegakan hukum oleh Otoritas Jasa Keuangan (OJK) dan Badan Siber dan Sandi Negara (BSSN) dalam mendorong kepatuhan perbankan terhadap standar keamanan siber. Fokus penelitian dapat diarahkan pada evaluasi kelembagaan, instrumen kebijakan, serta koordinasi antarinstansi dalam merespons insiden siber di sektor keuangan digital.

Daftar Pustaka

Ahmad, S. S., & Mujib, A. (2023). Analisis Pojk No. 1/Pojk. 07/2013 Terkait Perlindungan Konsumen Dalam Aspek Jasa Keuangan Terhadap Telemarketing Asuransi Di Bni Life Syariah. Mu'amalat: Jurnal Kajian Hukum Ekonomi Syariah, 15(2), 159–172. https://doi.org/doi.org/10.20414/mu.v15i2.7377

Andi, A. N. H., & Anis, I. (2024). The impact of IT governance practices on profitability: Mediating role of financial technology adoption. Jurnal Akuntansi Trisakti, 11(1), 111–128. https://doi.org/10.25105/jat.v11i1.19418

Anisa, Y., & Syahrin, M. A. (2023). Pelaksanaan Peraturan Ojk Ri No. 6/Pojk. 07/2022 Tentang Perlindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan Online Di Kota

Pekanbaru. Journal of Sharia and Law, 2(1), 312–334. https://doi.org/10.1234001/jsl.v2i1

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. Justisia: Jurnal Ilmu Hukum, 1(1), 1–11. https://doi.org/10.56457/jjih.v1i1.38

Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile: Studi literatur mengenai cybercrime dan mitigasinya. Akuntansi Dan Teknologi Informasi, 17(2), 221–237. https://doi.org/10.24123/jati.v17i2.6409

Bachtiar. (2019). Metode Penelitian Hukum. Unpam Press.

Fajar, M., & Achmad, Y. (2010). Dualisme Penelitian Hukum Normatif dan Empiris. Pustaka Pelajar.

Fista, Y. L., Machmud, A., & Suartini, S. (2023). Perlindungan Hukum Konsumen Dalam Transaksi E-commerce Ditinjau dari Perspektif Undang-Undang Perlindungan Konsumen. Binamulia Hukum, 12(1), 177–189. https://doi.org/10.37893/jbh.v12i1.599

Fitriani, R., Subagiyo, R., & Asiyah, B. N. (2023). Mitigating IT Risk of Bank Syariah Indonesia: A Study of Cyber Attack on May 8, 2023. Al-Amwal: Jurnal Ekonomi Dan Perbankan Syari'ah, 15(1), 86–100. https://doi.org/10.24235/amwal.v15i1.14124.g5337

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. Jurnal Konstituen, 5(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Hutomo, C. I. (2019). Layanan urun dana melalui penawaran saham berbasis teknologi informasi (Equity crowdfunding). Perspektif: Kajian Masalah Hukum Dan Pembangunan, 24(2), 65–74. https://doi.org/10.30742/perspektif.v24i2.703

Muhaimin. (2020). Metode Penelitian Hukum. Mataram University Press.

Negara, A. A. G. P., & Satria, I. N. K. P. (2021). Upaya perlindungan konsumen terhadap maraknya penjualan pakaian merek tiruan. Ganesha Civic Education Journal, 3(2), 46–53. https://doi.org/10.23887/gancej.v3i2

Pakina, R., & Solekhan, M. (2024). Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan Di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia. Journal of Scientech Research and Development, 6(1), 273–286. https://doi.org/10.56670/jsrd.v6i1

Putri, D. F., Sari, W. R., & Nabbila, F. L. (2023). Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. Jurnal Ilmiah Ekonomi Dan Manajemen, 1(4), 173–181. https://doi.org/10.61722/jiem.v1i4.331

Rahman, M. A., & Astria, K. (2023). Dampak fintech terhadap perkembangan perbankan. Ekonomi Bisnis, 29(1), 12–19. https://doi.org/10.33592/jeb.v29i1.3493

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan Di Era Digital. Krigan: Journal of Management and Sharia Business, 1(2), 25–36. https://doi.org/10.30983/krigan.v1i2.7929

Ritonga, R. D. M. (2020). Itikad Baik Pelaku Usaha Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. Jurnal Gagasan Hukum, 2(01), 71–88. https://doi.org/10.31849/jgh.v2i01.8236

Siswanto, C. A., Indradewi, A. A., Pallo, K. X. E., & Purba, A. Z. (2022). Perlindungan konsumen terhadap pembelian obat mengandung psikotropika pada online marketplace. Jurnal USM Law Review, 5(2), 553–568.

Suhadi, E., & Fadilah, A. A. (2021). Penyelesaian Ganti Rugi Akibat Wanprestasi Perjanjian Jual Beli Online Dikaitkan Dengan Pasal 19 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. Jurnal Inovasi Penelitian, 2(7), 1967–1978. https://doi.org/10.47492/jip.v2i7.1078

Suryanto, D., & Riyanto, S. (2024). 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. https://doi.org/10.34005/veritas.v10i1.3711

Wibowo, D. E. (2019). Penerapan konsep utilitarianisme untuk mewujudkan perlindungan konsumen yang berkeadilan kajian peraturan otoritas jasa keuangan nomor: 1/POJK. 07/2013 tentang perlindungan konsumen sektor jasa keuangan. Syariah: Jurnal Hukum Dan Pemikiran, 19(1), 15–31. https://doi.org/10.18592/sy.v19i1.2296

Afifah, D. (2023). Perlindungan konsumen di sektor jasa keuangan pada kasus serangan siber ransomware yang menimpa perbankan. Jurnal Ilmiah Ilmu Pendidikan, 6(5), 3385–3394. https://doi.org/10.54371/jiip.v6i5.3176

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan hukum terhadap nasabah atas kejahatan phishing dan hacking pada layanan bank digital. Hakim: Jurnal Ilmu Hukum dan Sosial, 2(1), 289–301. https://journal.stekom.ac.id/index.php/Hakim/article/view/1535

Nugraha, F. S., & Njatrijani, R. (2016). Perlindungan hukum terhadap nasabah bank dalam pembobolan internet banking melalui metode malware. Diponegoro Law Journal, 5(3), 1–13. https://ejournal3.undip.ac.id/index.php/dlr/article/view/12348

Putri, D. F., Andriani, W. R. S., & Nabbila, F. L. (2023). Analisis perlindungan nasabah BSI terhadap kebocoran data dalam menggunakan digital banking. Jurnal Ilmiah Ekonomi dan Manajemen, 2(3), 110–119. https://ejurnal.kampusakademik.co.id/index.php/jiem/article/view/331