Jurnal Hukum dan HAM Wara Sains
Vol. 04, No. 02, Juni 2025, pp. 297-313

Kajian Eksistensi Pertanggungjawaban Lembaga Perbankan Terhadap Pembocoran Data Pribadi Nasabah Dalam Penggunaan M-Banking

Brenda Putri Tanoto[1], Jessica Daniella[2], Khairiyah Hanan Rafidah[3], Nadya Christallita Kurniawan[4], Valerine Anastasya[5]

[1] Universitas Pelita Harapan dan 01051220058@student.uph.edu
[2] Universitas Pelita Harapan dan 01051220083@student.uph.edu
[3] Universitas Pelita Harapan dan 01051220068@student.uph.edu
[4] Universitas Pelita Harapan dan 01051220043@student.uph.edu
[5] Universitas Pelita Harapan dan 01051220067@student.uph.edu

Article Info

Article history:

Received Apr, 2025
Revised Apr, 2025
Accepted Apr, 2025

Kata Kunci:

M-Banking, Kebocoran Data Pribadi, Tanggung Jawab Perbankan, Perlindungan Hukum, Kejahatan Siber

Keywords:

Mobile Banking, Personal Data Breach, Banking Responsibility, Legal Protection, Cybercrime

ABSTRAK

Perkembangan teknologi digital, khususnya layanan mobile banking (M-Banking), telah memudahkan transaksi perbankan bagi nasabah. Namun, kemudahan ini juga meningkatkan risiko kebocoran data pribadi akibat kelemahan sistem keamanan dan serangan siber. Penelitian ini bertujuan untuk menganalisis tanggung jawab hukum lembaga perbankan terhadap kebocoran data nasabah dalam penggunaan M-Banking serta mengevaluasi efektivitas perlindungan hukum yang berlaku di Indonesia. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Data dikumpulkan melalui studi literatur terhadap regulasi yang berlaku, prinsip hukum perbankan, serta studi kasus kebocoran data yang terjadi di sektor perbankan. Hasil penelitian menunjukkan bahwa meskipun terdapat regulasi yang mengatur perlindungan data pribadi, implementasinya masih menghadapi berbagai kendala, seperti kurangnya kepatuhan bank terhadap standar keamanan dan rendahnya kesadaran nasabah mengenai ancaman siber. Tanggung jawab bank dalam kasus kebocoran data dapat dikategorikan ke dalam tindakan preventif dan represif, di mana bank memiliki kewajiban menjaga keamanan sistem, memberikan edukasi kepada nasabah, serta bertanggung jawab atas kerugian akibat kelalaian sistem. Kebaruan penelitian ini terletak pada analisis mendalam terhadap celah regulasi dan tantangan dalam implementasi perlindungan data perbankan di era digital. Implikasi dari penelitian ini adalah perlunya penguatan kebijakan perlindungan data pribadi, peningkatan teknologi keamanan perbankan, serta edukasi berkelanjutan bagi nasabah guna meminimalisir resiko kebocoran data.

ABSTRACT

The development of digital technology, particularly mobile banking (M-Banking) services, has made banking transactions more convenient for customers. However, this convenience also increases the risk of personal data breaches due to security system vulnerabilities and cyberattacks. This study aims to analyze the legal responsibility of banking institutions regarding customer data breaches in M-Banking and to evaluate the effectiveness of legal protections in Indonesia. This research employs a normative legal method with a statutory,

conceptual, and case-based approach. Data is collected through a literature review of applicable regulations, banking legal principles, and case studies of data breaches in the banking sector. The findings indicate that despite existing regulations on personal data protection, implementation faces various challenges, such as banks' lack of compliance with security standards and customers' low awareness of cyber threats. The bank's responsibility in cases of data breaches can be categorized into preventive and repressive measures, where banks are obliged to maintain system security, educate customers, and be accountable for losses resulting from system negligence. The novelty of this study lies in its in-depth analysis of regulatory gaps and challenges in implementing banking data protection in the digital era. The implications of this research highlight the need to strengthen personal data protection policies, enhance banking security technology, and provide continuous education for customers to minimize the risk of data breaches.

Corresponding Author:

Name: Alexandrea Prabarini
Institution: Universitas Pelita Harapan
Email: 01051220001@student.uph.edu

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi sudah membawa transformasi besar dalam berbagai sektor, termasuk industri perbankan. Kemajuan teknologi tentunya telah mendorong perbankan untuk menghadirkan layanan digital guna meningkatkan efisiensi dan kemudahan bagi nasabah. Inovasi yang paling banyak digunakan saat ini adalah layanan *mobile banking* atau yang lebih sering disebut dengan M-Banking. Para bank berlomba-lomba untuk memperbarui aplikasi M-Banking untuk mendapatkan lebih banyak nasabah seperti BCA yang membuat aplikasi BCA Mobile dan myBCA yang bertujuan untuk memberikan solusi komprehensif layanan perbankan bagi para nasabah.[1]

M-Banking adalah sistem layanan yang mempermudahkan nasabah bank dalam menjalani transaksi perbankan dengan hanya menggunakan smartphone. Dalam aplikasi M-Banking yang diunduh oleh nasabah, terdapat menu untuk mengakses sistem layanan mobile banking. Aplikasi tersebut lebih mudah dan nyaman untuk digunakan jika dibandingkan dengan SMS banking, dikarenakan para nasabah tidak harus mengingat format dan nomor tujuan SMS banking. M-Banking terdapat fitur layanan yang berisi layanan informasi yang berisi lokasi cabang/ATM terdekat, saldo, suku bunga, perubahan rekening, layanan transaksi seperti transfer, pembayaran maupun tagihan.

Dengan kehadiran M-Banking, maka sangat mempermudah nasabah dalam melakukan kegiatan keuangan dengan cara lebih cepat, mudah, dan aman. Apabila nasabah ingin memakai

[1] Dionisio, D. *Kenali Perbedaan antara BCA Mobile dan myBCA*. https://finansial.bisnis.com/read/20220316/90/1511330/kenali-perbedaan-antara-bca-mobile-dan-mybca. Akses pada 2 Februari 2025 pukul 12.30 WIB.

layanan perbankan, tentunya pihak bank memerlukan data-data pribadi seseorang tersebut yang berguna untuk menunjukkan kepemilikan, langkah keamanan dan mengakses layanan perbankan. Namun, seiring dengan kemudahan dan perlindungan yang ditawarkan, terdapat berbagai kelemahan seperti M-Banking hanya dapat digunakan apabila smartphone terhubung dengan internet, juga dengan adanya M-Banking muncul pihak yang tidak bertanggung jawab yang berusaha meretas akun dan mencuri data pribadi nasabah sehingga terjadinya kebocoran data pribadi nasabah karena kemudahan yang diberikan oleh sistem layanan M-Banking.

Kebocoran data nasabah dalam layanan m-banking adalah isu yang sangat serius dan dapat mengakibatkan dampak besar, baik bagi nasabah maupun institusi keuangan. Penyebab utama dari masalah ini adalah adanya celah keamanan yang belum teridentifikasi atau tidak segera diperbaiki, yang memungkinkan aktor ancaman seperti peretas mengeksploitasi sistem. Selain itu, faktor lain seperti kelalaian manusia, kurangnya pengawasan terhadap pihak ketiga, dan serangan berbasis sosial seperti *phishing* turut berkontribusi pada terjadinya insiden kebocoran data.[2] Kebocoran data ini tidak hanya menimbulkan kerugian materi, tetapi juga mengancam hilangnya kepercayaan publik terhadap sistem perbankan digital. Di era digital yang semakin kompleks ini, perlindungan hukum yang kuat sangat diperlukan untuk memastikan keamanan data nasabah serta untuk menegakkan keadilan apabila terjadi pelanggaran, demi menjaga integritas dan kepercayaan terhadap sektor perbankan. Menurut data yang diambil oleh Otoritas Jasa Keuangan **("OJK")**, dalam periode 2020 hingga 2023 telah dilaporkan lebih dari 20 kasus kebocoran data nasabah di berbagai bank, yang menyebabkan kerugian finansial bagi nasabah maupun lembaga perbankan dengan estimasi total mencapai triliunan rupiah.[3] Evaluasi terhadap regulasi yang berlaku mengungkapkan adanya kesenjangan dalam implementasi perlindungan data nasabah. Meskipun terdapat ketentuan yang mengharuskan bank menjaga data nasabah sesuai dengan standar keamanan tertentu, penerapannya di lapangan masih menghadapi berbagai hambatan, baik dari segi teknis maupun operasional. Kendala tersebut meliputi keterbatasan sumber daya, infrastruktur teknologi yang belum sepenuhnya optimal, serta rendahnya kesadaran akan pentingnya keamanan data di tingkat operasional. Selain itu, ancaman siber yang terus berkembang, seperti *phishing*, *malware*, dan serangan peretasan, semakin menambah kompleksitas dalam menjaga keamanan data nasabah. Berdasarkan artikel-artikel sebelumnya, para penulis akan membahas terkait dengan pertanggungjawaban lembaga perbankan terhadap pembocoran data pribadi nasabah dalam penggunaan M-Banking bermaksud untuk meneliti secara mendalam tanggung jawab hukum yang harus dilakukan oleh bank dalam menghadapi kasus kebocoran data nasabah. Selain itu, penelitian ini berusaha merumuskan rekomendasi untuk memperkuat sistem perlindungan data di sektor perbankan Indonesia dengan memperhitungkan aspek regulasi, teknologi, serta praktik operasional terbaik. Diharapkan, temuan dalam penelitian ini dapat berkontribusi dalam meningkatkan keamanan data nasabah serta mendukung terciptanya ekosistem perbankan yang lebih aman dan terpercaya di era saat ini.

[2] Khansa, I. S., Maria, C. A., Ambar, K. P., & Ahida, L. (2024). Perlindungan Hukum Nasabah Terhadap Bocornya Rahasia Data M-Banking Di Era Digital. Jurnal Multidisiplin Ilmu Akademik, 1(6), 335-347. DOI: https://doi.org/10.61722/jmia.v1i6.3039, Hal. 340

[3] Syafa, W. A., Hanintya, P. G. H. S., & Meira, A. A. (2024). Tanggung Jawab Hukum Bank dalam Kasus Kebocoran Data Nasabah. Jurnal Multidisiplin Ilmu Akademik, 1(6), 129-135. DOI: https://doi.org/10.61722/jmia.v1i6.2885, Hal. 129.

2. TINJAUAN PUSTAKA

2.1 Perlindungan Data Pribadi dalam Perbankan Digital

Data pribadi yang tersimpan dalam sistem elektronik membentuk jejak digital yang sulit dihapus, sehingga penting untuk memberikan perlindungan guna mencegah kebocoran dan penyalahgunaan data tersebut. Meskipun demikian, dalam praktiknya sering kali terjadi kesalahan yang tidak disengaja akibat sistem keamanan yang kurang memadai, sehingga membuka celah bagi pihak yang tidak bertanggung jawab untuk mencuri, memperjualbelikan, atau memanfaatkan data pribadi untuk tujuan yang tidak sah. (Alfitri et al., 2024).

Kerahasiaan data konsumen merupakan aspek privasi yang wajib dijaga secara kehati-hatian. Demi mencegah peretasan, pencurian, serta penyalahgunaan data diperlukan perlindungan data konsumen. Hal tersebut diperlukan agar kepercayaan nasabah terhadap transaksi elektronik tetap terjaga, industri perbankan diwajibkan untuk menyediakan fitur keamanan (*security features*). Terdapat juga hak-hak nasabah sebagai konsumen yang harus dilindungi oleh perlindungan hukum. (Rahmahdhani et al,, 2023).

2.2 Tanggung Jawab Perbankan terhadap Kebocoran Data Nasabah

Dalam menjalankan perannya, tanggung jawab yang besar dipegang oleh bank untuk menjaga kerahasiaan data nasabah. Adanya hubungan kontraktual antara nasabah dan bank dibangun berdasarkan prinsip kerahasiaan (confidential principle) dan prinsip kerahasiaan (confidential principle). Oleh Sebab itu bank harus dapat memberikan suatu jaminan keamanan yang maksimal terhadap data nasabahnya untuk melindungi privasi nasabahnya. Bank memiliki kewajiban untuk memperhatikan kepentingan nasabahnya dan menjaga kerahasiaan data nasabahnya. (Usman., 2001).

Tanggung jawab yang dimiliki dunia perbankan yaitu melindungi data nasabah, undang-undang tentang perlindungan data pribadi telah menegaskan mengenai hal tersebut. Langkah-langkah yang harus dilakukan bank yaitu melatih karyawan secara efektif, menerapkan langkah-langkah perlindungan data yang ketat, dan memastikan semua taat terhadap standar peraturan yang ada. (Rivaldo et al., 2024).

2.3 Regulasi Perlindungan Data Pribadi di Indonesia

Pemerintah telah mengeluarkan regulasi mengenai pelaksanaan bank digital, namun hal tersebut belum mampu mencukupi semua kebutuhan nasabah dalam aktivitas perbankan digital. Kebocoran data nasabah yang kerap terjadi sangat bertentangan dengan prinsip dunia perbankan, yakni prinsip kerahasiaan (*secrecy principle*) dan prinsip kehati-hatian (*prudential principle*). (Hendarto., 2024).

Selain mengatur UU ITE, OJK pun mengurus perlindungan data pribadi nasabah yang terdapat dalam layanan perbankan elektronik. Hal tersebut diatur dalam Peraturan OJK No.12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum yang memberikan panduan bagi bank dalam menjalankan layanan perbankan digital dengan memperhatikan aspek perlindungan data pribadi nasabah. Peraturan tersebut memotivasi bank-bank agar mengambil metode keamanan yang aman untuk menjalankan data pribadi nasabah. Diwajibkan kepada Bank agar

menerapkan kebijakan keamanan yang tepat, termasuk penggunaan alat otentikasi ganda untuk melindungi data pribadi nasabah. (Maisah et al., 2023).

3. METODE PENELITIAN

Metode penelitian hukum dengan tiga pendekatan utama digunakan dalam penelitian ini. Pertama, pendekatan perundang-undangan (*statute approach*) digunakan untuk mengkaji regulasi yang mengatur perlindungan data nasabah, termasuk Undang-Undang Perbankan, Undang-Undang Perlindungan Data Pribadi, serta peraturan yang dikeluarkan oleh OJK. Kedua, pendekatan konseptual (*conceptual approach*) dimanfaatkan untuk memahami prinsip-prinsip hukum yang berkaitan dengan pertanggungjawaban bank atas keamanan data nasabah. Ketiga, pendekatan kasus (*case approach*) diterapkan dengan menelaah berbagai kasus kebocoran data yang pernah terjadi di sektor perbankan guna memperoleh gambaran mengenai penerapan regulasi serta tantangan dalam praktiknya.

4. HASIL DAN PEMBAHASAN

4.1 Mekanisme kerja M-Banking (brenda) dan Risiko Kebocoran Data Pribadi

Menurut lembaga Otoritas Jasa Keuangan (OJK) di Indonesia, m-Banking merupakan platform yang melayani pelaksanaan kegiatan transaksi perbankan oleh nasabah bank melalui perangkat elektronik seperti telepon seluler. Dalam penggunaannya, m-banking beroperasi dengan menggunakan data-data yang disalurkan ataupun disediakan oleh USSD, SIM Card, ataupun melalui aplikasi tertentu oleh nasabah bank.[4] Layanan m-banking pada umumnya memiliki 2 jenis layanan yakni:

1. layanan non-finansial seperti penyediaan informasi mutasi dan/atau e-statement, informasi tunggakan, maupun pelayanan informatif seperti informasi terkait lokasi kantor cabang dan lain-lain; dan
2. layanan finansial seperti transfer dana, pembayaran tunggakan, pembelian, dan lain-lain.

Berdasarkan data dari Asosiasi Fintech Pendanaan Indonesia, Penggunaan m-banking mulai bertumbuh pesat pada tahun 1988, dengan Bank Internasional Indonesia sebagai pelopor pengguna m-banking pertama.[5] Namun, dalam perkembangannya, BCA menjadi salah satu lembaga perbankan yang berani mengoperasikan m-banking secara masif di Indonesia pada tahun 2001.[6] Masing-masing lembaga perbankan di Indonesia memiliki nama dan sistem m-banking tersendiri. Teruntuk BCA, m-banking BCA dikenal dengan istilah m-BCA.[7] Transaksi yang dapat dilakukan dengan m-BCA antara lain adalah m-Info, m-Transfer, m-Payment, m-Commerce, dan m-Admin.

[4] Otoritas Jasa Keuangan. (2015). Bijak Ber-eBanking. Retrieved Februari 11, 2025, from https://www.ojk.go.id /Files/box/buku%20bijak%20ber-ebanking.pdf

[5] Asosiasi Fintech Pendanaan Bersama Indonesia. (n.d). Sejarah Perkembangan Fintech di Indonesia.. Retrieved Februari 11, 2025, from https://afpi.or.id/articles/detail/sejarah-perkembangan-fintech-di-indonesia

[6] *Ibid.*

[7] Indrati, A. & Saputra, B. (2023). Analisis Usability Layanan BCA Mobile Banking Berdasarkan Persepsi Pengguna Menggunakan Heuristic Evaluation. Jurnal Ilmiah Teknik, 2(1), 35-42. https://doi.org/10.56127/juit.v2i1.469

Dalam menjalankan kegiatan perbankan, lembaga bank wajib mematuhi asas-asas perbankan yakni asas demokrasi ekonomi, asas kepercayaan, asas kerahasiaan, asas kehati-hatian, asas prinsip mengenal nasabah.[8] Sebagai upaya untuk mewujudkan asas-asas berikut, BCA mengembangkan sistem m-banking guna meningkatkan efisiensi pelayanan perbankan darinya kepada nasabahnya. [9]

a. Asas demokrasi ekonomi

Asas tersebut menekankan pentingnya pemerataan kesempatan dan akses terhadap berbagai layanan ekonomi, termasuk layanan perbankan. Melalui pengembangan m-BCA, masyarakat luas dapat menikmati layanan perbankan tanpa harus terbatas oleh jarak atau waktu. Nasabah juga akan merasakan keuntungan efisiensi pelayanan seperti *one-stop service* melalui penggunaan m-Banking tidak perlu lagi datang langsung ke kantor cabang untuk bertransaksi. Layanan ini dapat diakses secara fleksibel memungkinkan nasabah dari berbagai lapisan masyarakat untuk mengakses layanan perbankan dengan mudah dan praktis, sehingga menciptakan pemerataan layanan yang lebih inklusif.

b. Asas kepercayaan

Asas tersebut adalah asas fundamental dalam hubungan berkelanjutan antara bank dan nasabah yang mewujudkan integritas bank sebagai bank terpercaya. Berhubungan dengan asas tersebut maka BCA telah mengimplementasikan berbagai langkah keamanan dalam sistem m-BCA. Langkah keamanan yang dimaksud meliputi antara lain autentikasi dua faktor, enkripsi SSL/TLS, dan pengawasan transaksi secara real-time.[10] Dengan fitur-fitur keamanan tersebut, nasabah diberi keyakinan dan kepastian terhadap perlindungan data pribadi dan informasi transaksi yang sifatnya rahasia.

c. Asas kerahasiaan

Asas kerahasiaan adalah salah satu prinsip penting dalam layanan perbankan sebab hal-hal yang berkaitan dengan transaksi keuangan adalah hal yang perlu dirahasiakan. Dalam hal ini, m-BCA dirancang dengan menggunakan protokol enkripsi yang kuat untuk memastikan bahwa keamanan penyimpanan dan penggunaan data-data nasabah, seperti informasi rekening dan/atau transaksi melalui transmisi antara perangkat pengguna dan server BCA. Fitur ini menjamin bahwa hanya nasabah yang berhak yang dapat mengakses informasi sensitif tersebut. Dengan demikian, BCA berusaha untuk memenuhi asas kerahasiaan melalui penerapan teknologi enkripsi dan kebijakan perlindungan data yang ketat.

d. Asas kehati-kehatian

Asas kehati-hatian adalah kunci dari keberlangsungan bank. Asas tersebut menuntut bank untuk selalu melakukan tindakan pencegahan guna menghindari risiko yang dapat merugikan nasabah. Dalam pengembangan m-BCA, BCA wajib memastikan bahwa sistem perbankan digital

[8] SIP Law Firm. (2023). Asas dan Prinsip Hukum Perbankan. Retrieved Februari 11, 2025, from https://siplawfirm.id/asas-dan-prinsip-hukum-perbankan/?lang=id

[9] Alfarizi, R., Satrio, A.J., Prasetyo, Y.O., Syahputra, M.F. (2024). Analisis Perkembangan Teknologi m-BCA dan Keamanan Siber di Bank Central Asia. Kampus Akademik Publishing: Jurnal Akademik Ekonomi dan Manajemen, 1(4), 43-53. https://doi.org/10.61722/jaem.v1i4.3204

[10] BCA. (n.d). Kebijakan. Retrieved Februari 11, 2025, from https://www.bca.co.id/id/informasi/Kebijakan

yang mereka tawarkan bebas dari kejahatan-kejahatan siber oleh para pihak yang tidak bertanggung jawab yang mengancam aspek keamanan bagi nasabah yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Proses verifikasi transaksi yang ketat, penggunaan PIN, serta pengiriman One-Time Password (OTP) ke perangkat nasabah merupakan contoh penerapan kehati-hatian dalam M-BCA. Selain itu, sistem BCA juga dilengkapi dengan pemantauan dan deteksi penipuan secara otomatis yang akan memperingatkan nasabah jika ada transaksi yang mencurigakan. Dengan demikian, BCA menjaga agar setiap transaksi dilakukan dengan hati-hati dan meminimalisir potensi risiko penipuan.

e. Asas prinsip mengenal nasabah

Nasabah memainkan peran penting dalam menjaga keberlangsungan perbankan. Dengan itu, maka lembaga perbankan wajib menerapkan prinsip Know Your Customer (KYC). Dalam implementasi m-BCA, BCA mengadopsi kebijakan KYC dengan tujuan untuk mengenali nasabah secara lebih mendalam, baik pada saat pendaftaran akun maupun dalam setiap transaksi yang dilakukan. Proses KYC ini melibatkan verifikasi data pribadi nasabah, seperti nama, alamat, serta informasi identitas lainnya. Selain itu, BCA juga menerapkan langkah-langkah verifikasi berlapis untuk memastikan bahwa nasabah yang mengakses layanan M-BCA adalah benar-benar pihak yang terdaftar. Penerapan prinsip KYC ini penting dalam mencegah penyalahgunaan layanan perbankan untuk kegiatan ilegal, seperti pencucian uang atau pendanaan terorisme.

Meskipun BCA telah menerapkan sistem perlindungan berlapis, mengingat bahwa m-Banking berbasis *online* atau dalam jaringan, maka penggunaan m-BCA tidak lekas dari kemungkinan adanya pembocoran data pribadi. Pembocoran data pribadi adalah salah satu bentuk kejahatan dunia maya (*cybercrime*) yang dapat diakibatkan oleh faktor-faktor eksternal ataupun internal. Faktor eksternal yang dimaksud adalah seperti *phising*, *virus, spyware, bot* dimana para pelaku kejahatan (*hacker)* menggunakan metode penanaman objek asing untuk meretas sistem keamanan yang telah diimplementasikan oleh BCA dan menarik data-data pribadi nasabah BCA yang berguna untuk keperluan transaksional.[11] Adapun faktor internal yang dimaksud adalah peretasan data pribadi nasabah oleh penjaga data BCA yang tidak bertanggung jawab.

4.2 Jenis-Jenis Kejahatan Dunia Maya yang Mengancam Keamanan Data Pribadi Nasabah dalam Penggunaan M-Banking.

Kejahatan dunia maya (*cybercrime*) dalam perbankan digital mencakup berbagai jenis kejahatan yang memanfaatkan teknologi informasi dan internet untuk menargetkan individu, lembaga perbankan, serta pengguna layanan perbankan digital. Seiring pesatnya perkembangan teknologi informasi, hampir semua aktivitas perbankan kini dilakukan secara elektronik, termasuk dalam sistem pembayaran yang mengarah pada transaksi tanpa kertas (*paperless*). Layanan transaksi elektronik seperti ATM, *phone banking*, dan *internet banking* telah mengubah cara penyediaan layanan perbankan, beralih dari metode tradisional menjadi berbasis teknologi. Perubahan ini mendorong pelaku usaha untuk mengintegrasikan teknologi dalam inovasi produk dan layanan mereka.[12]

Kemajuan teknologi ini juga membawa tantangan baru, terutama dalam bentuk ancaman kejahatan dunia maya yang dapat merugikan berbagai pihak yang terlibat dalam sistem perbankan.

[11] *Ibid*.

[12] CYBERCRIME *dan CYBERSECURITY pada Sektor Keuangan*. (n.d.). Retrieved February 22, 2025, from https:/maksi.binus.ac.id/2023/05/16/cybercrime-dan-cybersecurity-pada-sektor-keuangan/

Kejahatan dunia maya di bidang perbankan digital tidak hanya mencakup kejahatan baru yang melibatkan perangkat komputer dan jaringan, tetapi juga kejahatan tradisional yang kini difasilitasi oleh teknologi. Dalam konteks ini, *cybercrime* dapat dipahami sebagai kejahatan yang memanfaatkan internet untuk menargetkan korban seperti bank, *merchant*, toko *online*, maupun nasabah. Pelaku sering kali mengeksploitasi kelalaian dari pihak bank, *merchant*, atau nasabah yang rentan terhadap serangan.

Serangan siber terhadap bank tidak hanya berdampak pada kerugian finansial, tetapi juga dapat merusak reputasi lembaga keuangan tersebut. Ketika data nasabah diretas atau sistem bank mengalami gangguan akibat serangan siber, kepercayaan pelanggan bisa terguncang. Nasabah yang kehilangan kepercayaan terhadap keamanan bank cenderung mencari alternatif lain, yang pada akhirnya dapat mengurangi jumlah pengguna layanan bank tersebut. Selain itu, serangan siber juga berpotensi mengganggu operasional bank, menyebabkan layanan perbankan tidak dapat diakses dalam waktu yang tidak menentu. Dalam beberapa kasus, peretasan juga dapat digunakan untuk kegiatan kriminal yang lebih luas, seperti pencucian uang atau pendanaan ilegal.

Salah satu ancaman siber paling berbahaya yang sering menargetkan sektor perbankan adalah ***ransomware***. *Ransomware* merupakan jenis perangkat lunak berbahaya (*malware*) yang mengenkripsi data korban dan menuntut pembayaran tebusan agar akses dapat dikembalikan. Penyerang sering kali mengancam untuk menghapus atau mempublikasikan data jika tuntutan mereka tidak dipenuhi. Ancaman siber lain yang semakin meningkat adalah **serangan berbasis *cloud***. Dengan semakin banyaknya bank yang mengadopsi teknologi *cloud* untuk menyimpan dan mengelola data mereka, risiko keamanan terhadap infrastruktur *cloud* juga semakin besar. Kerentanan dalam sistem cloud dapat dimanfaatkan oleh peretas untuk mengakses data sensitif atau mengganggu layanan perbankan. Kesalahan konfigurasi dalam pengaturan keamanan *cloud*, penggunaan kata sandi yang lemah, serta kelalaian dalam pembaruan sistem merupakan beberapa faktor utama yang sering dimanfaatkan oleh pelaku kejahatan siber. Jika bank tidak secara rutin memperbarui sistem keamanannya dan memastikan konfigurasi yang benar, maka mereka berisiko menjadi korban peretasan yang dapat mengakibatkan kebocoran data dan gangguan operasional.[13]

Ancaman siber lainnya yang juga patut diwaspadai adalah s**erangan rantai pasokan (*supply chain attacks*)**. Dalam serangan ini, penjahat siber menargetkan vendor atau pemasok yang memiliki akses ke sistem bank. Dengan menyusup ke sistem pemasok, peretas dapat menggunakan akses tersebut untuk menyerang bank secara tidak langsung. Salah satu metode umum yang digunakan dalam serangan rantai pasokan adalah memasukkan *malware* atau kode berbahaya ke dalam pembaruan perangkat lunak yang diberikan pemasok kepada bank. Karena pembaruan ini berasal dari vendor yang dipercaya, bank sering kali tidak menyadari bahwa sistem mereka telah disusupi. Begitu *malware* tersebut berhasil diinstal, penjahat siber bisa mendapatkan akses ke data sensitif atau jaringan internal bank. Serangan seperti ini sangat berbahaya karena dapat menyebar dengan cepat dan sulit untuk dideteksi, terutama jika bank tidak memiliki sistem keamanan yang mampu memantau aktivitas mencurigakan dalam jaringan mereka.[14]

[13] Cloud Managed Services. (2024, September 24). *5 Ancaman Siber yang Sering Dihadapi Bank*. Elitery. https://elitery.com/articles/5-ancaman-siber-yang-sering-dihadapi-bank/

[14] Sukmana, Y. (2021, November 10). Kenali Jenis-jenis Kejahatan Siber di Sektor Perbankan. *Kompas.Com*. https://money.kompas.com/read/2021/11/10/071027026/kenali-jenis-jenis-kejahatan-siber-di-sektor-perbankan#google_vignette

Selain serangan berbasis teknologi, **metode rekayasa sosial (*social engineering*)** juga menjadi ancaman serius bagi perbankan. Dalam metode ini, penjahat siber menggunakan manipulasi psikologis untuk menipu korban agar secara tidak sadar memberikan informasi sensitif seperti kata sandi atau data keuangan. Salah satu teknik rekayasa sosial yang paling umum adalah ***phishing***, di mana pelaku memanfaatkan kelengahan dan kepercayaan korban untuk memperoleh informasi sensitif. Dalam serangan phishing, penjahat siber menyamar sebagai entitas yang sah dan terpercaya, seperti bank atau lembaga resmi lainnya, untuk menipu korban agar mengungkapkan informasi pribadi mereka. Biasanya, penjahat siber akan mengirimkan email atau pesan yang tampaknya berasal dari sumber yang terpercaya, seperti bank atau penyedia layanan online. Pesan tersebut seringkali mengandung tautan atau lampiran yang berisi *malware* atau formulir palsu yang meminta korban untuk memasukkan data pribadi, seperti nama pengguna, kata sandi, nomor kartu kredit, atau data keuangan lainnya.[15]

Metode *phishing* ini memanfaatkan kecenderungan manusia untuk mempercayai komunikasi yang tampaknya sah. Karena itu, serangan ini sering kali sangat sulit dideteksi oleh korban yang tidak waspada. Salah satu bentuk *phishing* yang umum adalah ***email phishing***, di mana penjahat siber mengirim *email* palsu dengan tujuan untuk menipu korban agar mengklik tautan yang mengarahkan mereka ke situs web palsu atau mengunduh lampiran yang mengandung *malware*.[16] Selain itu, ada juga ***spear phishing***, yang lebih terfokus pada individu atau kelompok tertentu dengan mempersonalisasi pesan untuk membuatnya lebih meyakinkan. Dalam spear phishing, penjahat siber sering kali mengumpulkan informasi pribadi tentang korban sebelum melakukan serangan, sehingga pesan yang dikirim terasa lebih relevan dan dapat dipercaya.[17] Terakhir, ***whaling*** adalah varian dari *spear phishing* yang ditujukan pada eksekutif atau orang-orang penting dalam organisasi, seperti CEO atau direktur, yang memiliki akses ke informasi yang sangat berharga.[18]

Kasus *phising* yang menarik perhatian publik dan menunjukkan dampak besar dari jenis serangan ini terjadi pada tahun 2022 lalu, yang melibatkan Bank Central Asia (BCA). Dalam kasus ini, seorang pelaku bernama Mohammad Thoha berhasil membobol rekening milik nasabah BCA, Muin Zachry, yang memiliki saldo sebesar Rp 345 juta. Namun, modus yang digunakan oleh Thoha jauh lebih cerdik dari serangan phishing biasa. Thoha menyewa kamar kos di rumah Muin Zachry untuk dapat memanipulasi korban dan mencuri data pribadi yang sangat penting. Selama tinggal di rumah Muin, Thoha mengamati dan memanfaatkan informasi yang dimiliki korban, termasuk data pribadi yang ada di kamar kos tersebut. Setelah memperoleh data tersebut, Thoha melanjutkan aksinya dengan mengirimkan invoice palsu kepada staf BCA dengan menggunakan identitas Muin Zachry. Invoice tersebut disetujui oleh pihak bank tanpa kecurigaan, yang membuka celah bagi Thoha untuk melanjutkan aksinya. Tak hanya itu, Thoha juga berhasil mengakses buku tabungan, KTP, dan kartu ATM milik Muin Zachry yang ditemukan di kamar kos yang tidak terkunci. Informasi tersebut digunakan untuk memalsukan dokumen-dokumen yang diperlukan dalam

[15] Shaid, N. J. (2022, November 25). Apa Itu Phising: Definisi, Cara Kerja, Ciri-ciri, dan Cara Mencegahnya. Kompas.Com. https://money.kompas.com/read/2022/06/16/183024326/apa-itu-phising-definisi-cara-kerja-ciri-ciri-dan-cara-mencegahnya

[16] Hanif, L. (2024, November 1). Email Phishing: Jenis, Contoh, dan Cara Menghindarinya. *Rumahweb Journal*. https://www.rumahweb.com/journal/email-phishing-adalah/

[17] IBM. (n.d.). Spear phishing. IBM. Retrieved February 22, 2025, from https://www.ibm.com/id-id/topics/spear-phishing

[18] IBM. (n.d.-b). Whale phishing. *IBM*. Retrieved February 22, 2025, from https://www.ibm.com/id-id/topics/whale-phishing

proses penarikan dana. Dengan informasi yang telah diperolehnya, Thoha kemudian menghubungi Setu, seorang tukang becak yang ia ajak untuk membantu melaksanakan aksi tersebut. Thoha memberi Setu instruksi lengkap mengenai cara menarik uang dari rekening Muin, termasuk memberikan nomor PIN, slip penarikan yang telah dipalsukan, serta tanda tangan palsu dari Muin. Pada tanggal 5 Agustus 2022, Setu berhasil melakukan penarikan uang sebesar Rp 320 juta di salah satu cabang Bank BCA di Surabaya. Setelah berhasil mengambil uang tersebut, Setu menyerahkannya kepada Thoha, yang kemudian memberikan imbalan sebesar Rp 5 juta kepada Setu.[19]

Kasus ini menjadi perhatian publik karena melibatkan teknik manipulasi yang sangat terperinci dan menyeluruh. BCA pun segera mengimbau nasabah untuk lebih berhati-hati dan tidak membagikan informasi sensitif seperti KTP, kartu ATM, buku tabungan, atau data pribadi lainnya kepada pihak yang tidak dikenal. Bank juga menekankan pentingnya kesadaran akan keamanan digital, mengingat risiko tinggi yang ditimbulkan oleh serangan phishing yang bisa mengarah pada pembobolan rekening dan penyalahgunaan data pribadi. Kejadian ini juga mengingatkan kita bahwa selain serangan phishing yang dilakukan melalui email atau pesan digital, serangan siber bisa saja terjadi melalui manipulasi langsung terhadap orang yang memiliki akses ke informasi sensitif, sehingga kewaspadaan di tingkat individu sangat penting untuk mencegah terjadinya kasus serupa.[20]

Maka dapat disimpulkan bahwa, kejahatan dunia maya dalam sektor perbankan digital merupakan ancaman serius terhadap keamanan data pribadi nasabah. Seiring dengan pesatnya perkembangan teknologi, baik dalam transaksi maupun penyimpanan data, risiko serangan siber juga semakin meningkat. Oleh karena itu, penting bagi semua pihak, termasuk bank, nasabah, dan pemangku kepentingan lainnya, untuk meningkatkan kewaspadaan dan kesadaran terhadap potensi ancaman yang ada. Langkah-langkah keamanan yang lebih ketat serta edukasi mengenai perlindungan data pribadi sangat diperlukan untuk mengurangi risiko *cybercrime*. Kolaborasi antara lembaga perbankan, pemerintah, dan masyarakat juga menjadi kunci dalam menciptakan ekosistem digital yang aman dan terpercaya, demi menjaga kepercayaan nasabah terhadap sistem perbankan digital.

4.3 Perlindungan Hukum Bagi Nasabah atas Terjadinya Kebocoran Data

Dari sudut pandang hukum, hubungan antara nasabah dan bank terbagi menjadi dua kategori, yaitu hubungan non-kontraktual dan kontraktual. Hubungan non-kontraktual tidak didasarkan pada perjanjian tertulis, melainkan berlandaskan prinsip kepercayaan, kehati-hatian,

[19] Yanwardhana, E. (2023, January 21). Kronologi & Nasib Uang Nasabah BCA yang Dibobol Tukang Becak. *Cnbcindonesia.Com*. https://www.cnbcindonesia.com/market/20230121172736-17-407343/kronologi-nasib-uang-nasabah-bca-yang-dibobol-tukang-becak

[20] Ulum, M. (2023, Januari 25). Kronologi Lengkap Kasus Pembobolan Rekening Nasabah BCA di Surabaya. Bisnis.com.https://surabaya.bisnis.com/read/20230125/531/1621396/kronologi-lengkap-kasus-pembobolan-rekening-nasabah-bca-di-surabaya

kerahasiaan serta mengenal nasabah.[21] Sementara itu, hubungan kontraktual merujuk pada perjanjian tertulis yang mengatur hak dan kewajiban kedua belah pihak.[22]

Salah satu hubungan kontraktual antara bank dengan nasabah adalah kewajiban bank untuk menjaga rahasia bank. Pada Pasal 14 angka 1 Undang-Undang Nomor 2 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan **("UU P2SK")** yang merubah Pasal 1 angka 28 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan **("UU Perbankan")**, rahasia bank mencakup segala informasi yang berkaitan dengan penyimpanan serta simpanan milik nasabah.[23] Kewajiban ini berlaku bagi pihak terafiliasi dengan bank, termasuk pejabat serta karyawan bank.[24] Namun, terdapat 12 (dua belas) kondisi di mana bank diperbolehkan mengungkapkan informasi tersebut, seperti pertukaran informasi antar-bank, dan kepentingan lembaga negara dalam penyelenggaraan pemerintahan serta kepentingan umum sesuai kewenangan yang diatur dalam undang-undang.[25]

Lebih lanjut, OJK juga memiliki otoritas untuk memberikan persetujuan mengungkap rahasia bank dalam hal keperluan peradilan pada perkara pidana serta memenuhi bantuan timbal balik dalam masalah pidana.[26] Tidak hanya itu, rahasia bank juga dapat diungkapkan berdasarkan permintaan, persetujuan, ataupun kuasa tertulis dari nasabah penyimpan. Sehingga, nantinya bank wajib memberikan informasi tersebut kepada pihak yang telah ditunjuk oleh nasabah.[27]

Selain pada UU P2SK, pelindungan terhadap nasabah diatur pula dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi **("UU PDP")**. Data nasabah sendiri termasuk sebagai data personal yang bersifat spesifik dalam bentuk informasi finansial.[28] Dalam undang-undang tersebut, bank dikategorikan sebagai pengontrol data personal.[29] Dengan demikian, apabila terjadi kebocoran data nasabah, bank dapat dianggap gagal dalam melindungi data pribadi.

Kegagalan dalam pelindungan informasi personal dijelaskan pada Penjelasan Pasal 46 ayat (1) UU PDP, yang merujuk pada kegagalan dalam menjaga kerahasiaan, integritas, serta ketersediaan data pribadi, baik yang terjadi secara sengaja maupun tidak. Oleh karena itu, atas kegagalan tersebut, bank diwajibkan memberikan pemberitahuan tertulis kepada nasabah dan lembaga terkait dalam waktu paling lama 3x24 jam.[30] Jika tidak, bank dapat dikenakan sanksi administratif, seperti teguran tertulis, penghentian sementara pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda administratif.[31]

Lebih lanjut, dengan merujuk pada UU PDP dan UU P2SK sebagai dasar hukum, nasabah memiliki hak untuk melaporkan kasus pembocoran rahasia bank kepada kepolisian. Selain melapor,

---

[21] Sukarini, E. (2021, Oktober 26). Penerapan Prinsip Kehati-hatian Bank dalam Pencairan Dana Nasabah Dihubungkan dengan Undang-Undang tentang Perbankan. Jurnal Yustitia. 7(1). 106-107. https://yustitia.unwir.ac.id/index.php/yustitia/article/view/136

[22] Yudistira, I. (2024). Tanggung Jawab Hukum Bank Terhadap Kebocoran Data Nasabah Akibat Tindakan Peretasan dalam Perspektif Hukum Positif di Indonesia. Jurnal Ilmiah. 8. https://ifrelresearch.org/index.php/Doktrin-widyakarya/article/view/3202

[23] Pasal 14 angka 1 UU yang mengubah Pasal 1 angka 28 UU Perbankan

[24] Pasal 14 angka 27 UU P2SK yang mengubah Pasal 40 ayat (1) UU Perbankan

[25] Pasal 14 angka 38 UU P2SK yang memuat baru Pasal 40A ayat (1) UU Perbankan

[26] Pasal 14 angka 38 UU P2SK yang memuat baru Pasal 40B UU Perbankan

[27] Pasal 14 angka 46 UU P2SK yang membuat baru Pasal 44A ayat (1) UU Perbankan

[28] Pasal 4 ayat (2) huruf f UU PDP

[29] Pasal 1 angka 4 UU PDP

[30] Pasal 46 ayat (1) UU PDP

[31] Pasal 57 ayat (1) UU PDP

nasabah juga dapat mengajukan gugatan perdata terhadap bank. Di mana subjek data pribadi (dalam hal ini nasabah) dapat melayangkan gugatan dan menuntut kompensasi akibat kesalahan dalam pemrosesan informasi pribadinya sesuai dengan peraturan yang berlaku.[32]

Tidak hanya itu, nasabah juga dapat melaporkan pelanggaran bank dalam menjaga kerahasiaan informasi ke OJK maupun Bank Indonesia. Terakhir, penyelesaian sengketa melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan **("LAPS SJK")**. Penyelesaian melalui LAPS SJK sendiri dapat dilakukan baik secara mediasi maupun arbitrase.

4.4 Beban Tanggung Jawab Perbankan Terhadap Nasabah dalam Hal Terjadinya Kejahatan Mobile Banking

Mobile banking telah mengalami perkembangan pesat seiring dengan perkembangan teknologi digital dan kebutuhan masyarakat akan pelayanan keuangan yang lebih efisien. Layanan m-banking memungkinkan nasabah untuk melakukan transaksi perbankan melalui perangkat seluler seperti smartphone dan tablet, tanpa harus mengunjungi kantor cabang fisik. Fitur utama yang tersedia dalam mobile banking meliputi transfer dana, pembayaran tagihan, pembelian pulsa, cek saldo, hingga investasi dan pinjaman online. Dengan fleksibilitas dan kenyamanan yang ditawarkan, mobile banking telah menjadi salah satu pilar utama dalam industri perbankan modern.

Namun di balik semua kemudahan yang telah disediakan dengan layanan mobile banking, terdapat banyak resiko yang dapat terjadi. Perkembangan teknologi sendiri dapat digambarkan sebagai pisau bermata dua dimana melalui perkembangan ini memberikan banyak kemudahan dan solusi bagi sektor perbankan agar masyarakat dapat melakukan transaksi lebih mudah, namun di sisi lain perkembangan ini menimbulkan celah bagi individu yang tidak bertanggung jawab dalam melakukan cybercrime dan mobile banking juga memiliki risiko yang cukup besar, terutama terkait dengan keamanan data dan kejahatan siber. Dimana diantaranya kejahatan digital seperti phishing, malware, dan hacking menjadi ancaman utama yang dapat merugikan nasabah. Salah satunya diantaranya, phishing merupakan metode penipuan di mana pelaku mengirimkan tautan atau email palsu yang menyerupai bank untuk mencuri informasi login nasabah. Menurut laporan Kaspersky pada tahun 2024, terdapat lebih dari 97.226 kasus ransomware, 16,4 juta insiden serangan lokal, 11,7 juta serangan Remote Desktop Protocol (RDP), dan hampir 100.000 serangan phishing finansial di Indonesia. Angka ini mencerminkan bahwa ancaman kejahatan digital terus meningkat seiring dengan meningkatnya penggunaan layanan perbankan digital.

Menarik jangka rentang waktu dari Januari 2017 hingga awal Desember 2020, portal Patroli Siber menerima sebanyak 12.538 laporan terkait kejahatan siber. Dari jumlah tersebut, hanya 6.694 kasus yang berhasil diselesaikan, dengan total kerugian mencapai Rp 1,17 triliun. Jenis kejahatan yang dilaporkan mencakup 5.477 kasus penipuan online, 802 kasus akses ilegal, 317 kasus pencurian data, 244 kasus peretasan sistem elektronik, serta 331 kasus manipulasi data, selain beberapa insiden lain di berbagai sektor.[33]

Menghadapi maraknya kejahatan siber yang dapat dilakukan, bank sebagai penyedia layanan keuangan memiliki tanggung jawab dalam memastikan keamanan sistem perbankannya serta melindungi nasabah dari berbagai risiko kejahatan siber. Dimana perlindungan ini sudah sejalan dengan hak privasi yang diakui sebagai hak konstitusional. Hal ini sejatinya telah termaktub dalam Bab XA Pasal 28 A sampai J. Perlindungan data pribadi diatur pada Pasal 28G ayat (1) UUD

[32] Pasal 12 UU PDP

[33] Faridi, Muhammad Khairul, *Loc. Cit.*

NRI 1945 yang berbunyi: *"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."*[34] .Dalam mengamalkan hal tersebut bank memiliki beban tanggung jawab terhadap nasabah dalam menghadapi kasus kejahatan mobile banking dapat dikategorikan ke dalam dua aspek utama, yaitu tindakan preventif dan tindakan represif.

a. Tindakan Preventif: Upaya Pencegahan Kejahatan Mobile Banking

Sebagai upaya pencegahan, bank memiliki kewajiban untuk menerapkan sistem keamanan yang kuat guna melindungi data dan transaksi nasabah. Hal ini sejalan dengan ketentuan dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan yang mengatur bahwa bank harus menyediakan sistem yang aman bagi penggunanya. Selain itu, Pasal 40 Undang-Undang Perbankan juga mewajibkan bank untuk menjaga kerahasiaan informasi nasabah, termasuk dalam layanan mobile banking. [35]

Salah satu langkah yang dapat dilakukan bank adalah dengan menerapkan sistem autentikasi berlapis seperti OTP (One Time Password), enkripsi data, serta sistem deteksi anomali transaksi yang dapat mengidentifikasi aktivitas mencurigakan. Selain itu, bank juga harus terus mengedukasi nasabah mengenai cara mengenali modus penipuan dan langkah-langkah untuk melindungi diri dari phishing serta serangan siber lainnya. Otoritas Jasa Keuangan (OJK) melalui Peraturan OJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen di Sektor Jasa Keuangan juga mewajibkan bank untuk memberikan informasi yang jelas kepada nasabah mengenai risiko kejahatan digital serta cara menghindarinya.

Selain edukasi, bank juga harus secara rutin melakukan pembaruan sistem keamanan dan meningkatkan teknologi perlindungan siber. Contohnya, beberapa bank telah menerapkan teknologi AI (Artificial Intelligence) untuk mendeteksi transaksi mencurigakan secara otomatis dan mengurangi risiko fraud. Dengan menerapkan sistem keamanan yang ketat, bank dapat mengurangi kemungkinan nasabah menjadi korban kejahatan digital. [36]

b. Tindakan Represif: Pertanggungjawaban Bank terhadap Kerugian Nasabah

Jika seorang nasabah mengalami kerugian akibat kejahatan mobile banking, maka tanggung jawab bank bergantung pada penyebab utama insiden tersebut. Jika terbukti bahwa kerugian terjadi akibat kelalaian atau kegagalan sistem keamanan bank, maka bank wajib mengganti rugi dana nasabah yang hilang. Hal ini sesuai dengan ketentuan dalam Peraturan Bank Indonesia (PBI) Nomor 16/1/2014 tentang Perlindungan Konsumen, yang menyatakan bahwa bank harus bertanggung jawab atas dana nasabah yang hilang akibat kegagalan sistem.

Namun, jika kerugian terjadi akibat kelalaian nasabah sendiri, seperti memberikan informasi login atau OTP kepada pihak yang tidak bertanggung jawab, maka bank tidak berkewajiban untuk mengganti rugi. Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) menyatakan bahwa perlindungan terhadap data

[34] Pasal 28G ayat (1) Undang Undang Dasar 1945

[35] Wiguna, K. D., & Dananjaya, N. S. (2021). PERTANGGUNGJAWABAN BANK ATAS KERUGIAN NASABAH YANG MENGGUNAKAN ELECTRONIC BANKING. In *Jurnal Kertha Desa* (Vols. 9–9, Issue 12, pp. 23–35) [Journal-article].

[36]Mutia, N. C., & Firdaus, N. R. (2024). Analisis penipuan digital teknik phishing terhadap layanan mobile banking. Jurnal Transformasi Bisnis Digital, 1(4), 05–10. https://doi.org/10.61132/jutrabidi.v1i4.191

pribadi adalah tanggung jawab individu yang bersangkutan. Oleh karena itu, jika nasabah secara tidak sadar memberikan informasi penting mereka kepada pelaku kejahatan siber, maka tanggung jawab berada pada nasabah itu sendiri.

Lain hal dalam banyak kasus, batasan tanggung jawab ini sering kali menjadi area abu-abu, terutama ketika nasabah mengklaim bahwa mereka telah menjadi korban modus penipuan yang sangat canggih. Untuk mengatasi hal ini, OJK memberikan hak kepada nasabah untuk mengajukan pengaduan melalui mekanisme penyelesaian sengketa baik di dalam maupun di luar pengadilan. Bank diwajibkan untuk menyediakan layanan pengaduan yang responsif dan memastikan bahwa keluhan nasabah ditangani secara transparan serta profesional. Jika nasabah tidak puas dengan penanganan yang diberikan oleh bank, mereka dapat melapor ke OJK untuk mendapatkan mediasi dan penyelesaian lebih lanjut.

5. KESIMPULAN

Perkembangan teknologi digital dalam sektor perbankan telah membawa kemudahan bagi nasabah melalui layanan mobile banking (M-Banking). Namun, dibalik manfaat tersebut, risiko kebocoran data pribadi semakin meningkat akibat celah keamanan sistem, serangan siber, serta kelalaian pihak bank dan nasabah. Kejahatan dunia maya seperti *phishing, malware, hacking,* dan *social engineering* menjadi ancaman serius yang dapat menyebabkan pencurian data dan kerugian finansial bagi nasabah. Dari segi hukum, perlindungan data pribadi di sektor perbankan telah diatur dalam berbagai regulasi, seperti Undang-Undang Perbankan, UU PDP, dan regulasi OJK. Bank memiliki tanggung jawab besar dalam menjaga kerahasiaan data nasabah, yang didasarkan pada asas kepercayaan dan prinsip kehati-hatian. Namun, dalam prakteknya, masih terdapat kesenjangan dalam implementasi kebijakan perlindungan data, baik dari aspek regulasi maupun teknis.

Tanggung jawab perbankan dalam menghadapi kebocoran data dapat dikategorikan ke dalam dua aspek utama: preventif dan represif. Dari sisi preventif, bank wajib menerapkan sistem keamanan yang kuat, seperti enkripsi, autentikasi berlapis, serta pemantauan transaksi yang mencurigakan. Selain itu, edukasi bagi nasabah mengenai keamanan digital juga menjadi langkah penting untuk mencegah terjadinya kejahatan siber. Dari sisi represif, jika terjadi kebocoran data akibat kelalaian sistem bank, maka bank wajib memberikan ganti rugi kepada nasabah. Sebaliknya, jika kebocoran terjadi akibat kelalaian nasabah, seperti memberikan informasi login kepada pihak tidak bertanggung jawab, maka tanggung jawab beralih ke nasabah itu sendiri. Kasus-kasus kebocoran data yang terjadi dalam beberapa tahun terakhir menunjukkan bahwa masih terdapat tantangan besar dalam perlindungan data perbankan. Oleh karena itu, diperlukan penguatan kebijakan perlindungan data, peningkatan teknologi keamanan, serta pengawasan ketat terhadap implementasi regulasi oleh lembaga keuangan. Selain itu, kolaborasi antara bank, pemerintah, dan masyarakat sangat diperlukan untuk menciptakan ekosistem perbankan digital yang lebih aman dan terpercaya.

Dengan demikian, penelitian ini menegaskan bahwa meskipun regulasi terkait perlindungan data sudah ada, tantangan dalam implementasi masih menjadi kendala utama. Bank harus lebih proaktif dalam meningkatkan sistem keamanan, sementara nasabah juga harus lebih waspada dalam menjaga data pribadinya. Keberlanjutan industri perbankan digital sangat bergantung pada sejauh mana semua pihak dapat memastikan keamanan data nasabah di era digital yang semakin kompleks ini.

DAFTAR PUSTAKA

Alfitri, N. A., Rahmawati, R., & Firmansyah, F. (2024). *Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022.* Pustaka Digital Indonesia: Journal Social Society, 4(2). https://doi.org/10.54065/jss.4.2.2024.511

Alfarizi, R., Satrio, A.J., Prasetyo, Y.O., Syahputra, M.F. (2024). Analisis Perkembangan Teknologi m-BCA dan Keamanan Siber di Bank Central Asia. Kampus Akademik Publishing: Jurnal Akademik Ekonomi dan Manajemen, 1(4), 43-53. https://doi.org/10.61722/jaem.v1i4.3204

Asosiasi Fintech Pendanaan Bersama Indonesia. (n.d). Sejarah Perkembangan Fintech di Indonesia. Retrieved Februari 11, 2025, from https://afpi.or.id/articles/detail/sejarah-perkembangan-fintech-di-indonesia BCA. (n.d). Kebijakan. Retrieved Februari 11, 2025, from https://www.bca.co.id/id/informasi/Kebijakan

Cloud Managed Services. (2024, September 24). *5 Ancaman Siber yang Sering Dihadapi Bank*. Elitery. https://elitery.com/articles/5-ancaman-siber-yang-sering-dihadapi-bank/

CYBERCRIME dan CYBERSECURITY pada Sektor Keuangan. (n.d.). Retrieved February 22, 2025, from https://maksi.binus.ac.id/2023/05/16/cybercrime-dan-cybersecurity-pada-sektor-keuangan/

Damara, D. (2022, Maret 16). *Kenali Perbedaan antara BCA Mobile dan myBCA*. Bisnis.com. https://finansial.bisnis.com/read/20220316/90/1511330/kenali-perbedaan-antara-bca-mobile-dan-mybca.

Hanif, L. (2024, November 1). Email Phishing: Jenis, Contoh, dan Cara Menghindarinya. *Rumahweb Journal*. https://www.rumahweb.com/journal/email-phishing-adalah/

IBM. (n.d.-a). Spear phishing. *IBM*. Retrieved February 22, 2025, from https://www.ibm.com/id-id/topics/spear-phishing

IBM. (n.d.-b). Whale phishing. *IBM*. Retrieved February 22, 2025, from https://www.ibm.com/id-id/topics/whale-phishing

Indrati, A. & Saputra, B. (2023). Analisis Usability Layanan BCA Mobile Banking Berdasarkan Persepsi Pengguna Menggunakan Heuristic Evaluation. Jurnal Ilmiah Teknik, 2(1), 35-42. https://doi.org/10.56127/juit.v2i1.469

Khansa, I. S., Maria, C. A., Ambar, K. P., & Ahida, L. (2024). Perlindungan Hukum Nasabah Terhadap Bocornya
Rahasia Data M-Banking Di Era Digital. Jurnal Multidisiplin Ilmu Akademik, 1(6), 335-347. https://doi.org/10.61722/jmia.v1i6.3039

Maisah, M., Sari, S. P., Sudiarni, S., & Ompusunggu, H. P. (2023). Analisis hukum terhadap perlindungan data pribadi nasabah dalam layanan perbankan digital di Indonesia. *Aufklarung: Jurnal Pendidikan, Sosial dan Humaniora*, *3*(3). https://pijarpemikiran.com/index.php/Aufklarung/article/view/574

Otoritas Jasa Keuangan. (2015). Bijak Ber-eBanking. Retrieved Februari 11, 2025, from https://www.ojk.go.id/Files/box/buku%20bijak%20ber-ebanking.pdf

Rahmahdhani, D. N., Nasution, M. I. P., & Sundari, S. S. A. (2023). *Perlindungan data privasi yang dilakukan perbankan terhadap penggunaan layanan mobile banking.* Jurnal Ekonomi dan Bisnis, 2(2). https://doi.org/10.57218/jueb.v2i2.693

Rivaldo, A., & Syailendra, M. R. (2024). *Tanggung jawab penyedia layanan perbankan terhadap penyalahgunaan data nasabah berdasarkan Pasal 46 Ayat 1 UU PDP (Kasus Putusan 615/Pdt.G/2023/PN Surabaya).* UNES Law Review, 6(4). https://doi.org/10.31933/unesrev.v6i4

SIP Law Firm. (2023). Asas dan Prinsip Hukum Perbankan. Retrieved Februari 11, 2025, from https://siplawfirm.id/asas-dan-prinsip-hukum-perbankan/?lang=id

Shaid, N. J. (2022, November 25). Apa Itu Phising: Definisi, Cara Kerja, Ciri-ciri, dan Cara Mencegahnya. *Kompas.Com*. https://money.kompas.com/read/2022/06/16/183024326/apa-itu-phising-definisi-cara-kerja-ciri-ciri-dan-cara-mencegahnya

Sholikhah, I. H. (2024). Implikasi pengaruh minimnya pengaturan perlindungan privasi data pribadi nasabah pada perbankan digital. *Journal Justiciabelen (JJ)*, *4*(2), 129-140. https://jurnal.unsur.ac.id/JJ/article/view/4440/pdf

Sukarini, E. (2021, Oktober 26). Penerapan Prinsip Kehati-hatian Bank dalam Pencairan Dana Nasabah Dihubungkan dengan Undang-Undang tentang Perbankan. Jurnal Yustitia. 7(1). 106-107. https://yustitia.unwir.ac.id/index.php/yustitia/article/view/136

Sukmana, Y. (2021, November 10). Kenali Jenis-jenis Kejahatan Siber di Sektor Perbankan. *Kompas.Com*. https://money.kompas.com/read/2021/11/10/071027026/kenali-jenis-jenis-kejahatan-siber-di-sektor-perbankan#google_vignette

Syafa, W. A., Hanintya, P. G. H. S., & Meira, A. A. (2024). Tanggung Jawab Hukum Bank dalam Kasus Kebocoran

Data Nasabah. Jurnal Multidisiplin Ilmu Akademik, 1(6), 129-135. https://doi.org/10.61722/jmia.v1i6.2885

Ulum, M. (2023, Januari 25). Kronologi Lengkap Kasus Pembobolan Rekening Nasabah BCA di Surabaya. Bisnis.com. https://surabaya.bisnis.com/read/20230125/531/1621396/kronologi-lengkap-kasus-pembobolan-rekening-nasabah-bca-di-surabaya

Usman, R. (2001). *Aspek-aspek hukum perbankan di Indonesia.* PT Gramedia Pustaka Utama.

Undang-Undang Nomor 2 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan

Yanwardhana, E. (2023, January 21). Kronologi & Nasib Uang Nasabah BCA yang Dibobol Tukang Becak. *Cnbcindonesia.Com*. https://www.cnbcindonesia.com/market/20230121172736-17-407343/kronologi-nasib-uang-nasabah-bca-yang-dibobol-tukang-becak

Yetno, A. (2024). *Tanggung jawab bank dalam menjaga keamanan dan kerahasiaan data nasabah perbankan di Indonesia.* Morality: Jurnal Ilmu Hukum, 10(1), 67–76. http://dx.doi.org/10.52947/morality.v10i1.424

Yudistira, I. (2024). Tanggung Jawab Hukum Bank Terhadap Kebocoran Data Nasabah Akibat Tindakan Peretasan dalam Perspektif Hukum Positif di Indonesia. Jurnal Ilmiah. 8. https://ifrelresearch.org/index.php/Doktrin-widyakarya/article/view/3202