KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.1, No.6 Desember 2024
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 335-347
DOI: https://doi.org/10.61722/jmia.v1i6.3039

PERLINDUNGAN HUKUM NASABAH TERHADAP BOCORNYA RAHASIA DATA M-BANGKING DI ERA DIGITAL

Khansa Inggita Sari
Universitas Negeri Semarang
Maria Claudita Abigael
Universitas Negeri Semarang
Ambar Krisna Putri
Universitas Negeri Semarang
Ahida Lainatusyifa
Universitas Negeri Semarang
Alamat: Sekaran, Kec. Gn. Pati, Kota Semarang, Jawa Tengah 50229
Korespondensi penulis: khasainggita@student.unnes.ac.id

Abstrak. *The advancement of digital technology has brought about significant transformation in the banking sector, especially through mobile banking (m-banking) services that offer convenience and efficiency of financial transactions. However, these services also present the risk of customer data leakage that can threaten trust in the digital banking system. This study aims to examine legal protection for customers against data leakage in m-banking services in Indonesia, evaluate the responsibility of service providers, and provide effective legal solutions to address these challenges. Using normative legal methods and descriptive analysis, this study highlights the role of laws such as the Banking Law, the ITE Law, the PDP Law, and regulations from the OJK and Bank Indonesia. This study finds that despite the existence of an adequate legal framework, implementation in the field is still weak due to lack of supervision, low user awareness, and increasing threats of cybercrime. This study recommends strengthening regulations, customer education, and the implementation of layered security technology to ensure optimal customer data protection.*

Keywords: *digital era, legal protection, m-banking*

Abstrak. *Kemajuan teknologi digital telah membawa transformasi signifikan dalam sektor perbankan, terutama melalui layanan mobile banking (m-banking) yang menawarkan kemudahan dan efisiensi transaksi keuangan. Namun, layanan ini juga menghadirkan risiko kebocoran data nasabah yang dapat mengancam kepercayaan terhadap sistem perbankan digital. Penelitian ini bertujuan untuk mengkaji perlindungan hukum bagi nasabah terhadap kebocoran data dalam layanan m-banking di Indonesia, mengevaluasi tanggung jawab penyedia layanan, serta memberikan solusi hukum yang efektif untuk menghadapi tantangan ini. Dengan menggunakan metode yuridis normatif dan analisis deskriptif, penelitian ini menyoroti peran undang-undang seperti UU Perbankan, UU ITE, UU PDP, dan regulasi dari OJK dan Bank Indonesia. Studi ini menemukan bahwa meskipun terdapat kerangka hukum yang memadai, implementasi di lapangan masih lemah akibat kurangnya pengawasan, rendahnya kesadaran pengguna, serta meningkatnya ancaman kejahatan siber. Penelitian ini merekomendasikan penguatan regulasi, edukasi nasabah, dan penerapan teknologi keamanan berlapis untuk memastikan perlindungan data nasabah secara optimal.*
Kata Kunci: *era digital, perlindungan hukum, m-bangking*

PENDAHULUAN

Berdasarkan Pasal 1 Angka 1 Undang –Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (yang selanjutnya akan disebut sebagai UU Perbankan) menyebutkan bahwa “Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkan kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk

Received September 30, 2024; Revised Oktober 30, 2024;Desember 02, 2024
* Khansa Inggita Sari, khasainggita@student.unnes.ac.id

lainnya dalam rangka meningkatkan taraf hidup rakyat banyak." Perkembangan teknologi digital telah mengubah banyak aspek kehidupan manusia, termasuk industri perbankan. Layanan perbankan mobile, atau m-banking, memudahkan pelanggan untuk melakukan berbagai transaksi perbankan dengan cepat, efektif, dan praktis melalui perangkat seluler mereka. Ini merupakan salah satu inovasi yang paling menonjol. Di tengah kemajuan ini, muncul masalah baru terkait menjaga data pribadi nasabah, terutama kerahasiaan data, yang merupakan hak penting dalam bisnis perbankan. Data nasabah yang tersimpan dalam layanan m-banking memiliki potensi untuk menjadi sasaran pihak-pihak yang tidak bertanggung jawab, baik melalui serangan siber, penyalahgunaan teknologi, maupun kelalaian dari penyedia layanan. Kebocoran data ini tidak hanya berdampak pada kerugian material, tetapi juga mengancam kepercayaan publik terhadap sistem perbankan digital. Pada era digital yang semakin kompleks, perlindungan hukum menjadi sangat penting untuk menjamin keamanan data nasabah dan menjaga keadilan apabila terjadi pelanggaran.

Di Indonesia, meskipun belum ada peraturan khusus yang mengatur mengenai mobile banking, terdapat beberapa ketentuan yang dapat diinterpretasikan dan dijadikan dasar untuk menetapkan perlindungan hukum bagi nasabah pengguna mobile banking. Salah satunya adalah Pasal 29 Ayat (4) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang mengharuskan bank untuk memberikan informasi terkait potensi risiko kerugian yang dapat timbul akibat transaksi yang dilakukan nasabah. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji perlindungan hukum bagi nasabah dalam menghadapi ancaman kebocoran rahasia data m-banking, menganalisis tanggung jawab penyedia layanan, serta mengidentifikasi solusi hukum yang efektif dalam menjawab tantangan era digital. Sehingga dapat ditarik rumusan masalah Bagaimana pengaturan hukum terkait perlindungan data nasabah dalam layanan m-banking di Indonesia?, Faktor apa saja yang menjadi penyebab kebocoran rahasia data nasabah dalam layanan m-banking dan bagaimana upaya penanggulangannya?

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan perlindungan data yang lebih baik di Indonesia

KAJIAN TEORI

Bagian Perlindungan hukum bagi nasabah terhadap kebocoran data m-banking di era digital dapat dianalisis melalui beberapa pendekatan teori. Teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon menjelaskan bahwa perlindungan hukum

terbagi menjadi dua: preventif dan represif. Perlindungan preventif bertujuan mencegah terjadinya kebocoran data melalui regulasi yang ketat dan penerapan standar keamanan, sementara perlindungan represif memberikan solusi berupa sanksi hukum dan ganti rugi jika pelanggaran terjadi. Selanjutnya, teori kepercayaan (trust theory) menggarisbawahi pentingnya kepercayaan nasabah terhadap lembaga perbankan. Kepercayaan ini dibangun melalui transparansi, integritas, dan pengelolaan keamanan data, sebagaimana dinyatakan oleh Morgan dan Hunt (1994). Dalam konteks hak asasi manusia, perlindungan data pribadi nasabah juga merupakan bagian dari hak atas privasi yang dijamin oleh Deklarasi Universal Hak Asasi Manusia Pasal 12, di mana setiap individu memiliki hak atas keamanan informasi pribadi mereka.

Dalam perspektif teori sistem hukum Lawrence M. Friedman, perlindungan nasabah melibatkan tiga elemen utama: struktur hukum, substansi hukum, dan budaya hukum. Struktur hukum mencakup keberadaan lembaga pengawas perbankan dan otoritas perlindungan data, sedangkan substansi hukum merujuk pada undang-undang seperti Undang-Undang Perlindungan Data Pribadi di Indonesia yang menjadi dasar pengaturan perlindungan data. Budaya hukum, di sisi lain, menyoroti pentingnya kesadaran dan kepatuhan baik dari pihak lembaga perbankan maupun masyarakat terhadap tanggung jawab menjaga privasi data. Dengan kombinasi pendekatan ini, perlindungan hukum nasabah terhadap kebocoran data m-banking dapat lebih efektif diimplementasikan dalam menghadapi tantangan era digital.

METODE PENELITIAN

Metode penelitian yang digunakan dalam studi ini adalah metode yuridis normatif dengan spesifikasi deskriptif analitis. Pendekatan ini mengandalkan data sekunder yang dikumpulkan melalui studi kepustakaan atau library research. Penelitian ini menggunakan kedua jenis sumber data, yaitu primer dan sekunder. Sumber data primer diperoleh dari buku-buku dan jurnal penelitian yang relevan dengan topik yang dibahas, sedangkan sumber data sekunder berasal dari artikel-artikel daring yang membahas isu-isu terkait. Proses penelitian ini melibatkan pengumpulan data dari berbagai sumber yang relevan dengan topik, guna mendukung analisis dan pembahasan secara menyeluruh.

HASIL PENELITIAN DAN PEMBAHASAN

1. Perlindungan Hukum Terkait Perlindungan Data Nasabah dalam Layanan M-banking di Indonesia

Pengembangan pesat teknologi digital telah menyebabkan perubahan besar dalam layanan perbankan, termasuk munculnya layanan perbankan mobile, yang memungkinkan pelanggan melakukan transaksi melalui perangkat digital kapan saja dan di mana saja mereka mau. Namun, dengan kemajuan ini, muncul masalah baru untuk melindungi data pelanggan, terutama karena m-banking melibatkan penyimpanan, pemrosesan, dan pertukaran informasi pribadi. Berbagai undang-undang di Indonesia mengatur perlindungan data pelanggan dan sektor perbankan dan jasa keuangan. Berikut ini adalah penjelasan menyeluruh tentang pengaturan hukum tersebut.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen) membahas tentang Hak-hak konsumen, termasuk nasabah perbankan, dilindungi oleh undang-undang Perlindungan Konsumen. Menurut Pasal 4(c), konsumen berhak atas informasi yang akurat, lugas, dan jujur tentang barang atau jasa yang diberikan, termasuk layanan m-banking. Kebijakan privasi dan penggunaan data pribadi dijelaskan dengan jelas dalam artikel ini. Selain itu, Pasal 19 menetapkan bahwa pelaku usaha bertanggung jawab untuk memberikan ganti rugi kepada konsumen jika layanan yang tidak memenuhi standar menyebabkan kerugian.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), UU PDP merupakan tonggak penting dalam regulasi perlindungan data pribadi di Indonesia, termasuk untuk data nasabah perbankan. Pasal 3 menegaskan bahwa pengolahan data pribadi harus berlandaskan prinsip-prinsip dasar, seperti menghormati hak asasi manusia, menjaga keamanan, dan menjamin kerahasiaan. Dalam undang-undang ini juga diatur peran pengendali data (data controller) dan pemroses data (*data processor*), yang mencakup institusi perbankan sebagai pengelola utama data nasabah. Bank bertanggung jawab untuk memastikan keamanan data pribadi nasabah, baik yang dihimpun melalui layanan m-banking maupun dalam proses pengelolaannya, dengan menerapkan sistem perlindungan yang memadai. UU PDP juga memberikan sanksi tegas bagi pelanggaran terkait perlindungan data pribadi, baik dalam bentuk administratif maupun pidana. Contohnya, jika terjadi kebocoran data akibat kelalaian bank, pihak bank dapat dikenai denda dalam jumlah besar. Aturan ini diharapkan menjadi insentif bagi perbankan untuk meningkatkan standar keamanan data.

Peraturan Otoritas Jasa Keuangan (POJK) Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan POJK ini memberikan kewajiban kepada

penyedia jasa keuangan untuk melindungi hak konsumen, termasuk menjaga kerahasiaan data pribadi mereka. Dalam Pasal 29 dan 30 disebutkan bahwa pelaku usaha tidak boleh membocorkan data nasabah kepada pihak lain tanpa persetujuan nasabah yang bersangkutan. Peraturan ini juga menekankan pentingnya memberikan edukasi kepada nasabah terkait risiko keamanan, sehingga mereka dapat memahami dan mengelola risiko dalam menggunakan layanan m-banking.

Peraturan Bank Indonesia (PBI) Nomor 22/20/PBI/2020 tentang Sistem Pembayaran PBI ini menjadi panduan penting untuk pengelolaan data nasabah dalam transaksi pembayaran digital, termasuk m-banking. Bank Indonesia mewajibkan penyedia layanan pembayaran, termasuk perbankan, untuk mengadopsi teknologi keamanan yang memadai guna melindungi data nasabah dari ancaman serangan siber. Bank juga harus memastikan bahwa sistem autentikasi transaksi dijalankan dengan prosedur yang aman, seperti melalui penggunaan enkripsi data dan autentikasi multifaktor, untuk meminimalkan potensi penyalahgunaan.

Surat Edaran Otoritas Jasa Keuangan (SEOJK) Nomor 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data Konsumen SEOJK ini memberikan panduan teknis tambahan untuk menjaga keamanan data pribadi nasabah. Bank diwajibkan untuk menerapkan langkah-langkah teknis dan administratif guna melindungi data konsumen dari akses yang tidak sah. Selain itu, bank juga harus menyusun kebijakan internal yang memastikan bahwa seluruh karyawan memahami dan mematuhi prinsip kerahasiaan data nasabah. Hal ini bertujuan untuk mencegah terjadinya kebocoran data akibat kelalaian pihak internal.

Tantangan dan Implementasi Perlindungan Data

Meskipun kerangka hukum perlindungan data nasabah sudah cukup lengkap, implementasinya di lapangan masih menghadapi berbagai tantangan. Beberapa di antaranya adalah:

1. Kurangnya kesadaran nasabah Banyak nasabah yang kurang memahami pentingnya melindungi data pribadi mereka, sehingga secara tidak sadar membagikan informasi sensitif kepada pihak yang tidak bertanggung jawab.
2. Meningkatnya ancaman kejahatan siber. Serangan seperti phishing dan malware terus berkembang, menargetkan sistem m-banking yang belum memiliki perlindungan optimal.

3. Keterbatasan pengawasan. Layanan m-banking yang melibatkan infrastruktur teknologi pihak ketiga sering kali sulit diawasi sepenuhnya oleh regulator.

Untuk mengatasi tantangan ini, diperlukan upaya bersama dari pemerintah, otoritas keuangan, bank, dan nasabah itu sendiri. Pemerintah perlu memperkuat pengawasan terhadap pelaksanaan regulasi, sedangkan perbankan harus terus meningkatkan keamanan teknologi yang digunakan. Di sisi lain, edukasi kepada masyarakat juga menjadi kunci untuk meningkatkan kesadaran nasabah dalam menjaga kerahasiaan data pribadi mereka.

2. Faktor Penyebab Kebocoran Rahasia Data Nasabah Dalam Layanan M-banking dan Upaya Penanggulangannya

Kebocoran data nasabah dalam layanan m-banking adalah isu yang sangat serius dan dapat mengakibatkan dampak besar, baik bagi nasabah maupun institusi keuangan. Salah satu 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.Pada kasus seperti kebocoran data MyBCA, aktor ancaman tidak hanya memanfaatkan kerentanan teknis, tetapi juga melibatkan software jahat (*malware*) yang disisipkan secara tersembunyi, serta kemungkinan adanya akses dari pihak dalam (*insider threats*). Kombinasi ini menunjukkan bahwa ancaman terhadap keamanan data nasabah tidak hanya berasal dari luar, tetapi juga dari lingkungan internal bank itu sendiri. Untuk mengurangi risiko kebocoran data, institusi perbankan harus mengambil langkah-langkah preventif dan proaktif, termasuk:

1. Peningkatan Keamanan Teknologi

a. Menerapkan enkripsi tingkat tinggi untuk melindungi data sensitif selama pengiriman dan penyimpanan.

b. Melakukan pembaruan sistem secara berkala untuk menutup celah keamanan yang baru ditemukan.

c. Menggunakan teknologi pemantauan berbasis AI untuk mendeteksi dan merespons aktivitas mencurigakan secara real-time.

2. Penguatan Protokol Pengamanan

. Memastikan autentikasi multifaktor (MFA) diterapkan pada setiap akses akun m-banking.

a. Menyediakan sistem notifikasi keamanan instan bagi nasabah saat terjadi aktivitas mencurigakan di akun mereka.

3. Pengawasan terhadap Faktor Internal

. Melakukan audit keamanan berkala untuk memantau aktivitas karyawan dan mendeteksi potensi insider threats.

a. Memberikan pelatihan berkala kepada karyawan tentang pentingnya menjaga kerahasiaan informasi dan tanda-tanda aktivitas mencurigakan.

4. Edukasi Nasabah

. Memberikan edukasi kepada nasabah mengenai ancaman seperti phishing, serangan malware, dan praktik terbaik untuk menjaga keamanan akun.

a. Menyediakan pusat bantuan yang responsif untuk melaporkan dan menangani potensi pelanggaran keamanan.

5. Kolaborasi dengan Pihak Ketiga

. Bekerja sama dengan perusahaan cyber security untuk mengidentifikasi dan mencegah potensi ancaman.

a. Melakukan penilaian risiko secara berkala terhadap vendor atau mitra pihak ketiga yang memiliki akses ke data nasabah.

Kasus kebocoran data seperti ini juga menjadi pengingat akan pentingnya kepatuhan terhadap regulasi, seperti Undang-Undang Perlindungan Data Pribadi (PDP) di Indonesia. Bank dan penyedia layanan m-banking perlu memastikan bahwa sistem mereka mematuhi standar perlindungan data yang ketat untuk menjaga kepercayaan nasabah.

Selain celah keamanan teknis, regulasi yang lemah terkait perlindungan data pribadi di Indonesia menjadi faktor signifikan yang memperburuk risiko kebocoran data dalam layanan *m-banking*. Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) telah disahkan, implementasinya masih menghadapi berbagai tantangan, seperti kurangnya pengawasan yang ketat, sanksi yang tidak cukup berat untuk memberikan efek jera, serta rendahnya kesadaran perusahaan terhadap pentingnya keamanan data. Banyak perusahaan, termasuk bank, lebih mengutamakan efisiensi bisnis dan profitabilitas dibandingkan investasi dalam keamanan data. Hal ini terlihat dari kurangnya alokasi

anggaran untuk teknologi keamanan canggih, minimnya kebijakan keamanan internal yang ketat, dan kecenderungan untuk merahasiakan insiden kebocoran demi melindungi reputasi perusahaan. Kondisi ini semakin diperparah dengan tidak adanya tekanan yang signifikan dari regulasi untuk memastikan kepatuhan terhadap standar perlindungan data. Akibatnya, banyak perusahaan tidak merasa perlu menerapkan langkah-langkah keamanan yang memadai, sehingga data pribadi nasabah menjadi sangat rentan terhadap ancaman. Sanksi yang ringan juga membuat perusahaan lebih memilih menanggung risiko denda kecil daripada mengalokasikan anggaran besar untuk meningkatkan keamanan. Selain itu, minimnya transparansi mengenai insiden kebocoran data dapat menurunkan kepercayaan pengguna terhadap layanan digital seperti m-banking, yang pada akhirnya menghambat pertumbuhan ekonomi digital di Indonesia. Untuk mengatasi masalah ini, diperlukan penguatan implementasi UU PDP dengan memastikan adanya pengawasan yang efektif serta penegakan hukum yang tegas, termasuk pemberian sanksi berat seperti denda yang proporsional dan kemungkinan pencabutan izin operasi bagi perusahaan yang tidak patuh. Standar keamanan internasional, seperti ISO/IEC 27001, perlu diadopsi sebagai kewajiban hukum bagi perusahaan yang mengelola data pribadi, disertai kewajiban menerapkan enkripsi end-to-end, otentikasi multifaktor, dan audit keamanan secara berkala. Selain itu, masyarakat perlu diedukasi mengenai hak mereka atas data pribadi serta cara melaporkan insiden kebocoran data. Pemerintah, institusi perbankan, perusahaan teknologi, dan komunitas cyber security juga perlu bekerja sama untuk menciptakan ekosistem digital yang lebih aman. Simulasi serangan siber secara nasional dapat dilakukan secara berkala untuk menguji ketahanan sistem, sementara insentif seperti potongan pajak dapat diberikan kepada perusahaan yang mematuhi standar keamanan tinggi. Dengan langkah-langkah ini, Indonesia dapat memperkuat perlindungan data pribadi, mengurangi insiden kebocoran, dan meningkatkan kepercayaan masyarakat terhadap layanan m-banking sekaligus mendukung pertumbuhan ekonomi digital yang berkelanjutan.

Selain celah keamanan teknis dan regulasi yang lemah, perilaku pengguna juga menjadi salah satu faktor utama yang berkontribusi terhadap kebocoran data dalam layanan m-banking. Banyak nasabah masih kurang menyadari pentingnya menjaga kerahasiaan informasi pribadi mereka. Hal ini sering terlihat dari kebiasaan berbagi data sensitif seperti nomor rekening, PIN, atau kode OTP melalui media yang tidak aman,

seperti jaringan publik, pesan teks, atau panggilan telepon. Kesadaran yang rendah ini memberikan celah bagi pelaku kejahatan siber untuk melakukan berbagai serangan, termasuk phishing (penipuan melalui email atau situs web palsu), vishing (penipuan melalui telepon), dan skimming (pencurian data kartu menggunakan perangkat fisik). Risiko ini semakin meningkat seiring dengan tingginya adopsi layanan digital tanpa diimbangi edukasi yang memadai kepada pengguna.

Serangan-serangan ini sering kali dirancang untuk mengecoh pengguna agar secara tidak sadar memberikan akses ke data pribadi mereka. Sebagai contoh, dalam kasus phishing, pelaku menciptakan halaman login yang menyerupai situs m-banking asli untuk mencuri kredensial pengguna. Dalam vishing, pelaku memanfaatkan teknik manipulasi psikologis untuk membuat korban percaya bahwa mereka berbicara dengan pihak bank resmi. Sementara itu, skimming memanfaatkan perangkat keras untuk mencuri data kartu secara langsung dari mesin ATM atau perangkat pembayaran. Ancaman-ancaman ini tidak hanya membahayakan individu, tetapi juga menimbulkan kerugian besar bagi penyedia layanan keuangan. Untuk mengatasi masalah ini, penyedia layanan m-banking perlu mengadopsi sistem keamanan berlapis yang dirancang untuk melindungi aplikasi perbankan dan data nasabah dari berbagai jenis ancaman. Beberapa metode yang efektif meliputi:

1. Penggunaan Sertifikat Digital

   Sertifikat digital memastikan bahwa komunikasi antara aplikasi m-banking dan server bank terenkripsi dengan aman, sehingga mencegah intersepsi data oleh pihak tidak bertanggung jawab.
2. Autentikasi Multifaktor (MFA)

   Penerapan One-Time Password (OTP) atau sistem biometrik seperti sidik jari dan pengenalan wajah dapat digunakan sebagai lapisan autentikasi tambahan untuk memperkuat keamanan akses ke akun.
3. Proteksi Melalui Browser dan Aplikasi

   Fitur keamanan seperti browser yang dioptimalkan untuk m-banking atau aplikasi yang secara otomatis mendeteksi aktivitas mencurigakan, seperti login dari lokasi yang tidak biasa, dapat membantu melindungi data pengguna.
4. Keyboard Virtual

   Penggunaan keyboard virtual dalam aplikasi m-banking dapat mencegah

pencurian data melalui malware seperti keylogger, yang dirancang untuk merekam input dari keyboard fisik.

5. Peringatan Real-Time

   Nasabah harus diberi notifikasi instan untuk setiap transaksi atau upaya login yang mencurigakan, sehingga mereka dapat segera mengambil tindakan jika terjadi aktivitas yang tidak sah.

Selain solusi teknis, edukasi pengguna memainkan peran yang sangat penting. Bank perlu aktif mengedukasi nasabah tentang ancaman siber dan cara melindungi informasi pribadi mereka, seperti menghindari berbagi PIN atau OTP, menggunakan jaringan internet yang aman, dan memverifikasi keaslian situs web atau aplikasi sebelum memasukkan data sensitif. Kampanye kesadaran keamanan digital yang terarah dan berkelanjutan dapat membantu mengubah perilaku pengguna ke arah yang lebih aman.

Upaya penanggulangan kebocoran data dalam layanan m-banking tidak hanya bergantung pada teknologi dan regulasi, tetapi juga harus melibatkan edukasi intensif kepada nasabah. Hal ini penting karena perilaku dan kebiasaan pengguna sering kali menjadi titik lemah yang dimanfaatkan oleh pelaku kejahatan siber. Edukasi ini harus mencakup pemahaman tentang pentingnya menjaga kerahasiaan data pribadi serta panduan tentang cara-cara aman bertransaksi secara online. Nasabah disarankan untuk mengganti password secara berkala dan memastikan kombinasi password yang digunakan kuat, dengan menggabungkan huruf besar, huruf kecil, angka, dan simbol. Penggunaan password yang unik untuk setiap akun digital juga sangat dianjurkan untuk mencegah risiko jika salah satu akun diretas. Selain itu, nasabah harus hanya mengunduh aplikasi m-banking dari sumber resmi, seperti toko aplikasi terpercaya atau situs web resmi bank, untuk menghindari aplikasi palsu yang sering kali disusupi malware. Langkah lain yang perlu ditekankan adalah menghindari penggunaan jaringan wifi publik saat melakukan transaksi keuangan, karena jaringan ini sering kali tidak terenkripsi, sehingga memungkinkan peretas untuk mengakses data yang dikirimkan. Jika terpaksa menggunakan jaringan publik, nasabah dianjurkan untuk menggunakan *Virtual Private Network* (VPN) untuk mengenkripsi koneksi mereka. Bank juga harus mendorong pengguna untuk selalu memperbarui aplikasi m-banking mereka ke versi terbaru, karena pembaruan ini biasanya mencakup perbaikan keamanan untuk melindungi pengguna dari ancaman terbaru. Fitur-fitur seperti autentikasi biometrik, notifikasi real-time, dan

pemantauan aktivitas mencurigakan harus diaktifkan untuk memberikan lapisan perlindungan tambahan. Selain langkah-langkah teknis bank dapat mengadakan kampanye kesadaran keamanan digital melalui media sosial, email, atau bahkan melalui pesan dalam aplikasi m-banking itu sendiri. Kampanye ini harus mencakup informasi tentang ancaman siber terkini, seperti phishing dan skimming, serta tips untuk mengidentifikasi tanda-tanda penipuan. Bank juga dapat menyediakan tutorial interaktif atau seminar online untuk membantu nasabah memahami praktik keamanan yang baik.

KESIMPULAN

Perlindungan hukum dalam konteks perlindungan data nasabah beberapa regulasi di Indonesia telah mengatur keamanan data, seperti Undang-Undang Perlindungan Konsumen, UU ITE, UU PDP, dan berbagai peraturan Otoritas Jasa Keuangan. Meski kerangka hukumnya cukup lengkap, implementasinya masih menghadapi tantangan besar termasuk kurangnya pengawasan dan sanksi yang lemah. Faktor kebocoran data nasabah disebabkan oleh beberapa faktor utama seperti celah keamanan teknis, kelalaian manusia, kurangnya kesadaran nasabah, dan ancaman siber seperti phishing dan malware. Kasus kebocoran data seperti MyBCA menunjukkan bahwa ancaman ini bisa berasal dari luar maupun dalam organisasi. Tantangan implementasi perlindungan hukum meliputi kesadaran nasabah yang rendah, meningkatnya ancaman siber, serta keterbatasan pengawasan terhadap pihak ketiga yang terlibat dalam pengelolaan data. Langkah mitigasi melibatkan penerapan teknologi keamanan yang canggih seperti enkripsi data, autentikasi multifaktor, dan edukasi pengguna mengenai pentingnya menjaga kerahasiaan data pribadi. Sehingga penulis memberikan saran yaitu Penguatan regulasi pemerintah perlu memperkuat pengawasan implementasi regulasi perlindungan data serta memberlakukan sanksi yang lebih tegas untuk memberikan efek jera kepada pelaku pelanggaran.,Peningkatan keamanan teknologi bank harus terus memperbarui sistem keamanan mereka, mengadopsi teknologi seperti enkripsi end-to-end, otentikasi biometrik, dan deteksi ancaman berbasis AI untuk melindungi data nasabah.,Edukasi masyarakat bank dan regulator harus gencar melakukan kampanye edukasi tentang keamanan digital untuk meningkatkan kesadaran nasabah mengenai risiko siber dan cara melindungi informasi pribadi.,Kolaborasi multisektor kerjasama antara pemerintah, institusi perbankan, perusahaan teknologi, dan komunitas keamanan siber sangat penting untuk menciptakan ekosistem digital yang lebih aman dan dapat diandalkan. Simulasi dan

uji keamanan berkala bank perlu melakukan simulasi serangan siber secara berkala untuk menguji ketahanan sistem mereka dan memastikan kesiapan menghadapi ancaman terbaru.

DAFTAR PUSTAKA

Undang-Undang

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, beserta perubahannya melalui UU Nomor 19 Tahun 2016.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.

Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Sistem Pembayaran.

Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data Konsumen.

Jurnal

Alia, R., Firdausy, F. A., & Lutfiana, S. A. (2024). ANALISIS EFEKTIVITAS PERLINDUNGAN HUKUM TERHADAP NASABAH DALAM TRANSAKSI PERBANKAN DIGITAL. *Causa: Jurnal Hukum dan Kewarganegaraan*, *7*(3), 1-10.

Bhoki, A., Aloysius, S., & Bire, C. M. D. (2024). PERLINDUNGAN HUKUM TERHADAP KEBOCORAN DATA NASABAH DITINJAU DARI UNDANG-UNDANG NOMOR 10 TAHUN 1998 TENTANG PERBANKAN. *Petitum Law Journal*, *2*(1), 245-256.

Ferdiansyah, D. S., Ameeralia, N. V., Putri, A. A. K., & Fikrie, S. N. (2024). Peran OJK Dalam Perlindungan Konsumen Terhadap Kebocoran Data Pada Konsumen Jasa Keuangan Indonesia. *Media Hukum Indonesia (MHI)*, *2*(3).

Hayati, A. S., & Setiawan, D. A. (2023, January). Perlindungan Hukum Nasabah Bank Pengguna M-Banking sebagai Korban Tindak Pidana Penipuan Ditinjau dari Hukum Positif di Indonesia. In *Bandung Conference Series: Law Studies* (Vol. 3, No. 1, pp. 546-551).

Hendrik Khoirul Muhid.(2022). *Serba-serbi Transaksi Digital, Mengenal Apa Itu Keamanan Berlapis.* Tempo.

Indriani, N. A. (2024). Perlindungan Hukum Bagi Para Pihak Terhadap Terjadinya Sistem Error Pada Penyelenggaraan M-Banking. *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora*, *2*(3), 93-105.

Kadari, P. N., Saharuddin, S., & Syahril, M. A. F. (2023). Perlindungan Hukum Nasabah atas Penggunaan E-Banking. *Jurnal Litigasi Amsir*, *10*(2), 167-179.

Katiandagho, V., Putong, D. D., & Melo, I. J. (2023). Undang–Undang Perlindungan Data Pribadi Memperkuat Undang–Undang Perbankan Dalam Menjaga Rahasia

Data Nasabah Dan Untuk Melindungi Data Pribadi Masyarakat Indonesia. *Jurnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat*, *9*(1), 106-114.

Moh. Khory Alfarizi. (2023). *Data MyBCA Diduga Bocor, Simak Pendapat Ahli Siber soal Penyebab, Risiko, dan Solusinya.* Tempo. https://mufdana.muf.co.id/berita/2023/04/tips-aman-menggunakan-mobile-banking-anti-kebobolan/

Rahmahdhani, D. N., Nasution, M. I. P., & Sundari, S. S. A. (2023). Perlindungan Data Privasi yang dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking. *JUEB: Jurnal Ekonomi dan Bisnis*, *2*(2), 88-96.

ZAHRO, L. H., & Muharrami, R. S. (2023). *PENGARUH PENGGUNAAN MOBILE BANKING DAN PERLINDUNGAN NASABAH TERHADAP CYBERCRIME DI KOTA SURAKARTA* (Doctoral dissertation, UIN RADEN MAS SAID).

Berita

https://www.cnnindonesia.com/ekonomi/20230515141653-78-949738/data-perbankan-bocor-apa-yang-perlu-dilakukan-nasabah