JIGE 5 (4) (2024) 2876-2886
JURNAL ILMIAH GLOBAL EDUCATION
ejournal.nusantaraglobal.or.id/index.php/jige
DOI: https://doi.org/10.55681/jige.v5i4.3592

Analisis Hukum Tantangan Bank Digital Dihubungkan dengan Perlindungan Hukum Bagi Nasabah Berdasarkan Perundang-Undangan di Indonesia

Erika Yolanda[1], Pan Lindawaty Suherman Sewu[1], Christian Andersen[1]

[1] Fakultas Hukum dan Bisnis Digital, Universitas Kristen Maranatha, Bandung, Indonesia
Corresponding author email: erika.yolanda2019@gmail.com

Article Info

Article history:

Received November 22, 2024
Approved Desember 30, 2024

Keywords:

Digital Banking Services, Customer Data, Security, Regulation, Law.

ABSTRACT

Banks in Indonesia are a crucial component of the country's economy, acting as a bridge for the public to conduct transactions such as payments, saving money, and facilitating both business and economic activities. In addition to conventional banks, digital banks have now emerged, regulated under Financial Services Authority Regulation No. 21 of 2023 on the Provision of Digital Banking Services by Commercial Banks. Digital banking services offer quick and easy access; however, with the rise of digital banks, new challenges and risks have also emerged, particularly concerning issues of personal data protection, cybersecurity, and customer data breaches. The rapid development of fintech in Indonesia has shifted consumer behavior towards digital financial transactions, especially since the COVID-19 pandemic in 2020, which required the public to reduce physical transactions. This study employs a normative legal research method, focusing on examining existing norms, principles, and legal regulations. In normative legal research, legal sources such as laws, books, journals, news, and other legal literature serve as the primary objects of study. The research findings conclude that legal regulations related to data and privacy protection for digital bank customers in Indonesia need strengthening, as current regulations remain partial in nature. Legal regulations should be comprehensive and cover all aspects related to the collection, storage, use, and security of customers personal data. To improve these legal regulations, harmonization of related laws and regulations is necessary. Additionally, public awareness, education, and outreach to digital banks are needed to emphasize the importance of data and privacy protection.

ABSTRAK

Bank di Indonesia merupakan komponen penting dalam perekonomian di Indonesia karena berfungsi sebagai jembatan masyarakat untuk melakukan transaksi seperti pembayaran, menyimpan uang, dan kunci dalam melakukan bisnis maupun ekonomi. Selain bank konvesional kini lahir juga bank digital yang diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum. Layanan bank digital ini menawarkan layanan yang cepat dan mudah, akan tetapi dengan lahirnya bank digital muncul juga berbagai tantangan dan risiko baru yang akan di hadapi terutama dalam masalah perlindungan data pribadi, keamanan siber, dan kebocoran data nasabah. Pesatnya perkembangan fintech di Indonesia telah mengubah perilaku masyarakat dalam transaksi keuangan yang semakin beralih ke platform digital terutama sejak pandemic COVID-19 pada tahun 2020 yang memaksa masyarakat mengurangi transaksi fiksi. Penelitian ini menggunakan metode penelitian normatif, yaitu dengan mengkaji norma, prinsip dan peraturan hukum yang sudah ada. Dalam penelitian hukum normatif, sumber-sumber

hukum seperti undang-undang, buku, jurnal, berita dan literatur hukum lainnya menjadi objek utama dalam kajian ini. Berdasarkan hasil penelitian, pengaturan hukum yang terkait dengan data dan privasi nasabah bank digital di Indonesia perlu diperkuat karena masih bersifat parsial. Pengaturan hukum harus bersifat komprehensif dan mencakup aspek-aspek yang terkait dengan pengumpulan, penyimpanan, penggunaan, dan keamanan data pribadi nasabah. Untuk memperkuat pengaturan hukum tersebut, perlu dilakukan harmonisasi peraturan perundang-undangan yang terkait. Selain itu, perlu juga dilakukan sosialisasi dan edukasi kepada masyarakat dan bank digital terkait pentingnya perlindungan data dan privasi.

How to cite: Yolanda, E., Sewu, P. L. S. & Andersen, C., (2024). Analisis Hukum Tantangan Bank Digital Dihubungkan dengan Perlindungan Hukum bagi Nasabah Berdasarkan Perundang-Undangan di Indonesia. *Jurnal Ilmiah Global Education*, 5(4), 2876-2886. https://doi.org/10.55681/jige.v5i4.3592

PENDAHULUAN

Bank di Indonesia merupakan salah satu komponen penting karena bank merupakan penghubung masyarakat dalam melaksanakan berbagai jenis transaksi. Peranannya mencakup penyelenggaraan sistem pembayaran, pemberian kredit sebagai sumber modal, elemen utama dalam kegiatan bisnis dan ekonomi, serta sarana penyimpanan uang bagi nasabah. Saat ini, layanan perbankan di Indonesia tidak hanya terbatas pada bank konvensional, tetapi juga mencakup kehadiran Bank Digital yang muncul akibat kemajuan teknologi dan informasi.

Kemajuan dalam teknologi informasi dan komunikasi telah secara drastis mengubah cara masyarakat menjalani interaksi, pekerjaan, dan transaksi. Sebagai salah satu pilar utama dalam sektor keuangan, bank memainkan peran kunci dalam menciptakan ekosistem ekonomi yang beradaptasi dengan transformasi digital. Oleh sebab itu, transformasi dalam sektor perbankan menjadi suatu keharusan. Pertumbuhan fintech yang pesat di Indonesia telah memengaruhi pola transaksi masyarakat, mempercepat adopsi transaksi digital, terutama dengan semakin meluasnya platform e-commerce. Selain itu, pandemi COVID-19 pada tahun 2020 memaksa masyarakat untuk beraktivitas dari rumah, mendorong kebiasaan baru yang berorientasi pada digitalisasi dan mengurangi ketergantungan pada transaksi fisik.

Dibalik kemajuan pertumbuhan bank digital ada kekhawatiran serius terkait tantangan dan risiko yang akan dihadapi perbankan di Era Digital, tantangan dan risiko tersebut terdiri dari risiko perlindungan data pribadi, risiko strategis investasi di bidang IT, risiko serangan siber, kesiapan organisasi, risiko kebocoran data nasabah, risiko penyalahgunaan teknologi, risiko penggunaan pihak ketiga, risiko regulasi perbankan dari pemerintah, dan risiko infrastruktur jaringan komunikasi. Namun risiko utama yang banyak terjadi di Indonesia ada tiga poin utama yaitu terkait perlindungan data pribadi, serangan siber, dan kebocoran data nasabah. Berdasarkan jurnal paradigma hukum pembangunan pada tahun 2022 hanya menjelaskan perihal implementasi aturan perlindungan data pribadi. Fokus penelitian ini bukan hanya membahas aturan perlindungan data pribadi saja namun membahas juga perihal serangan siber dan kebocoran data nasabah. Hal ini dilakukan ini dilakukan karena pelanggaran keamanan data mengenai data pribadi, serangan siber, dan kebocoran data nasabah banyak terjadi di Indonesia. Para pelanggar mencuri data privasi seseorang dengan cara akses tidak sah. Dengan terus berkembangnya teknologi dan informasi maka pelanggaran keamanan data juga terus berkembang dimana

pelanggaran tersebut membuat kerangka hukum semakin rumit, contohnya bagaimana hukum mengatur perihal teknologi cloud computing dimana data disimpan didalam cloud yang melibatkan pihak ketiga yang dapat menimbulkan risiko terkait kontrol, dan keamanan data nasabah. Mengidentifikasi dan memahami kerangka hukum perlindungan privasi, serangan siber, kebocoran data nasabah dalam era digital adalah kunci untuk mengatasi tantangan ini. Penelitian mendalam serta analisis yang komprehensif terhadap regulasi, kepatuhan, tanggung jawab, dan pendekatan inovatif menjadi kunci dalam memperkuat keamanan data pribadi, mengatasi ancaman siber, dan mencegah kebocoran informasi nasabah. Untuk menciptakan lingkungan digital yang aman dan terpercaya bagi individu maupun organisasi, diperlukan kerja sama yang erat antara sektor publik dan swasta, didukung oleh partisipasi aktif dari seluruh pemangku kepentingan.

Dasar Hukum Informasi dan Transaksi Elektronik di atur dalam Undang – Undang Nomor 11 Tahun 2008 lalu di ubah dan di rancang dalam Undang – Undang Nomor 19 Tahun 2016 dengan memberikan landasan hukum terkait masalah pelanggaran informasi dan transaksi elektronik, namun belum cukup mendalami tantangan unik dan kompleks yang dihadapi oleh bank digital. Dengan demikian, fokus utama dari penelitian ini dirumuskan untuk menganalisis hukum dalam tantangan dan risiko penyelenggaraan bank digital di Indonesia serta menganalisis perlindungan hukum bagi nasabah terkait risiko penyelenggaraan bank digital.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu dengan cara meneliti bahan pustaka atau data sekunder. Penulis menggunakan data sekunder berupa buku, jurnal, berita dan peraturan perundang-undangan yang berkaitan dengan layanan perbankan digital dan perlindungan terhadap nasabah layanan perbankan digital.

HASIL DAN PEMBAHASAN

TANTANGAN DAN RISIKO PENYELENGGARAAN LAYANAN BANK DIGITAL DI INDONESIA

Penyelenggaraan bank digital di Indonesia menghadirkan peluang signifikan untuk meningkatkan inklusi keuangan dan aksesibilitas layanan perbankan bagi masyarakat luas. Konsep bank digital dan bank konvesional memiliki perbedaan dalam model layanan dan infrastruktur yang mereka usung, bank digital sebagai manifestasi dari transformasi digital dalam sektor perbankan mempunyai teknologi yang memiliki kemampuan untuk nasabah dapat melakukan aktifitas perbankan melalui perangkat elektronik seperti smartphone tanpa perlu melakukan transaksi fisik.

Namun, di balik potensi yang menjanjikan ini, terdapat berbagai tantangan dan risiko yang perlu diperhatikan oleh para pemangku kepentingan. Terdapat sembilan klasifikasi risiko dan tantangan bank digital yaitu perlindungan data pribadi, strategis investasi di bidang IT, serangan siber, kebocoran data nasabah, regulasi perbankan dari pemerintah, penyalahgunaan teknologi, penggunaan pihak ketiga, kesiapan organisasi, dan infrastruktur jaringan komunikasi. Namun dalam penelitian ini hanya membahas risiko utama yang terbesar dan banyak terjadi di Indonesia yaitu perlindungan data pribadi, serangan siber, dan kebocoran data nasabah. Tantangan ini dikutip dari Website BRI Api yang juga mengutip berdasarkan keterangan Otoritas Jasa Keuangan.

1. **Perlindungan Data Pribadi** diklasifikasikan menjadi data umum dan data khusus serta

menerapkan prinsip-prinsip perlindungan data yang ketat, regulasi ini bertujuan untuk melindungi hak individu terkait dengan data pribadi mereka, meningkatkan rasa kepercayaan masyarakat terhadap penggunaan data pribadi, serta menjamin kepatuhan terhadap standar perlindungan data internasional. Pengaturan perlindungan data pribadi dapat bervariasi antar negara, pada umumnya, kebijakan tersebut mengacu pada prinsip perlindungan data yang serupa. Rezim perlindungan data di banyak negara terinspirasi oleh pedoman OECD 1980 mengenai *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* yang menerapkan prinsip pertama privasi yang diakui secara internasional (OECD, 2013). Menganalisis perlindungan data pribadi perlu dilakukan pembandingan regulasi yang berlaku di Indonesia dengan kerangka hukum international, khususnya General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa. Prinsip dalam GDPR memiliki regulasi yang lebih komprehensif dan rinci dibandingkan dengan Undang-Undang Perlindungan Data Pribadi (UU PD) Nomor 27 Tahun 2022. Regulasi yang bersifat parsial di Indonesia memengaruhi kepercayaan masyarakat terhadap layanan bank digital. Hal ini menciptakan celah bagi kebocoran data nasabah, karena bank belum diwajibkan menerapkan standar keamanan yang seketat GDPR. Di Indonesia, harmonisasi peraturan diperlukan agar lebih efektif menangani tantangan ini. Digitalisasi Sistem Perbankan harus disertai dengan audit berkala dan penerapan teknologi seperti enkripsi end-to-end sehingga risiko akses tidak sah dapat dicegah atau diminimalkan.Kelebihan dari GDPR antara lain adalah :

a) Prinsip Transparansi dan Akuntabilitas dimana setiap organisasi diwajibkan untuk memberikan informasi yang jelas tentang Bagaimana data dikumpulkan, diproses, dan disimpan
b) Hak Subjek Data dimana GDPR memberikan hak akses, hak untuk dilupakan (right to be forgotten), serta hak probabilitas data kepada pemilik data.
c) Denda dan sanksi tegas terhadap pelanggaran pada GDPR.

Perkembangan teknologi dan informasi memberikan peluang bagi pemerintah untuk melakukan inovasi pembangunan aparatur negara melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) atau *E-Government*, Dimana penyelenggaraan ini memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada instansi pemerintah, aparatur sipil negara, pelaku bisnis, dan masyarakat. Melalui penerapan SPBE, pemerintah juga berupaya untuk memanfaatkan berbagai teknologi baru seperti *big data*, *Internet of Things*, *Artificial Intelligence*, dan lain sebagainya. Pemanfaatan teknologi baru mempunyai tantangan dan risiko tersendiri, terutama dengan isu privasi dan perlindungan data pribadi. Sumber risiko perlindungan data pribadi dapat berasal dari kerentanan teknologi infrastruktur, penggunaan data tanpa persetujuan yang jelas, akses tidak sah. Dalam perkembangan teknologi dan informasi, ada teknologi yang bernama *cloud computing* dimana teknologi ini menyediakan infrastruktur dasar seperti server, penyimpanan, dan jaringan sehingga dapat digunakan untuk menyimpan data dalam skala besar tanpa harus mengelola server fisik. Pencegahan Risiko dapat dilakukan dengan cara mengimplementasikan teknologi keamanan dengan menggunakan algoritma enkripsi untuk melindungi data dalam perjalanan dan saat disimpan, menerapkan firewall untuk mencegah akses tidak sah, dan menggunakan sistem deteksi dan pencegahan intrusi untuk memantau dan merespon aktivitas mencurigakan. Perlindungan data pribadi termasuk dalam perlindungan konsumen, beberapa tantangan perlindungan konsumen di era digital di antara lain adalah maraknya penipuan dan pelanggaran keamanan data, rendahnya literasi konsumen, dan penyampaian informasi yang tidak jelas (Praktik

pemasaran yang buruk). Tantangan-tantangan tersebut menyebabkan *misleading information, misselling,* dan *overdebtness* yang berdampak langsung terhadap konsumen. Dalam perlindungan konsumen terdapat dua istilah hukum yakni *consumer law* dan *comsumer protection law* yang merupakan bidang hukum baru dalam akademik dan praktik penegakan hukum di Indonesia. Data pribadi adalah hak dasar setiap individu yang perlu dilindungi melalui peraturan yang ditetapkan dalam undang-undang yang memiliki kekuatan hukum dan mengikat. Peraturan terkait keamanan data dan perlindungan data pribadi di Indonesia masih tersebar dan bersifat parsial dan belum komprehensif.

2. **Serangan Siber** dalam perbankan digital mengacu pada potensi kerugian atau kerusakan yang mungkin dialami oleh individu, organisasi, atau sistem sebagai akibat dari serangan siber. Serangan siber adalah upaya yang disengaja untuk merusak, mengakses secara tidak sah, atau mencuri data dan informasi melalui jaringan komputer atau internet. Risiko ini mencakup berbagai aspek termasuk finansial, operasional, reputasi, dan hukum. Risiko serangan siber menuntut penguatan kapasitas keamanan melalui standar autentikasi, enkripsi, dan firewall. Dalam konteks hukum, kewajiban pelaporan dan transparansi yang diatur dalam SEOJK No. 12/SEOJK.03/2023 perlu ditegaskan untuk mendorong kepatuhan bank digital dalam melaporkan insiden. Di Indonesia, serangan siber menjadi isu yang semakin penting. Keamanan siber di Indonesia saat ini berada pada titik rawan dengan risiko yang terus meningkat, hal ini disebabkan oleh lonjakan volume lalu lintas informasi internasional yang masuk ke dalam sistem jaringan informasi nasional. Banyaknya serangan ke sistem informasi Indonesia adalah karena kesadaran akan ancaman siber dan regulasi atau aturan belum kuat di Indonesia, hal ini karena para penentu kebijakan masih awam terhadap informasi terkait siber. Ada juga faktor internal dan eksternal, faktor eksternal mencakup pesatnya perkembangan teknologi yang telah mengubah pola perilaku dan struktur sosial masyarakat. Dengan akses informasi yang hampir tak terbatas, muncul peluang untuk melakukan tindak kejahatan dari berbagai lokasi, bahkan dari dalam rumah, sementara itu faktor internal biasanya terkait dengan demografi pelaku. Data menunjukkan bahwa sebagian besar pelaku kejahatan siber berada dalam rentang usia 17 hingga 20 tahun, di mana dorongan untuk bereksperimen dengan teknologi cenderung lebih tinggi. Laporan dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2022 mencatat bahwa serangan malware dan ransomware pada sektor perbankan meningkat hingga 35% dibanding tahun sebelumnya. Ini menunjukkan perlunya investasi teknologi keamanan siber yang lebih canggih, seperti penguatan autentikasi berbasis biometrik. Keamanan Siber menjadi kunci untuk melindungi data ini dari potensi serangan yang dapat merugikan konsumen dan merusak citra penyelenggara sistem elektronik. Sumber risiko serangan siber dapat berasal dari penggunaan perangkat tidak aman oleh nasabah, malware, ransomware, dan phising. Terkait sumber risiko serangan siber dapat dilakukan pencegahan dengan Penguatan Autentikasi Multi-Faktor (MFA) misalnya menggunakan OTP (One-Time Password), autentikasi biometric, atau autentikasi dua factor yang berbasis aplikasi, Segmentasi Jaringan dan Pemulihan Bencana dengan cara memisahkan sistem operasi kristis dari sistem yang terhubung ke internet, bank dapat meminimalisir dampak malware dan ransomware yang mungkin menyebar, Edukasi berkelanjutan dan Simulasi Phising yang konsisten terhadap nasabah mengenai ancaman phising melalui berbagai media (email, notifikasi aplikasi, dan media sosial). Dengan strategi pencegahan yang komprehensif dan peningkatan kesadaran pengguna, risiko serangan siber dalam bank digital dapat diminimalkan. Implementasi harus terus dievaluasi agar dapat menyesuaikan dengan dinamika ancaman siber yang terus berkembang. Evaluasi berkelanjutan dapat membantu

organisasi untuk mengidentifikasi dan memahami kelemahan dalam sistem mereka yang dapat diekploitasi.

3. **Kebocoran Data Nasabah** merupakan masalah besar yang dihadapi di era teknologi modern. Data yang dicuri dapat berdampak buruk dan merugikan banyak pihak. Peraturan Pemerintah Nomor 71 Tahun 2019 mengatur penyelenggaraan sistem elektronik, namun penerapan mekanisme pemulihan dan perbaikan pasca insiden kebocoran data perlu dioptimalkan melalui audit berkala dan monitoring keamanan. Diperlukan perlindungan untuk mengurangi risiko kebocoran data pribadi agar tidak disalahgunakan karena data pribadi yang sudah diunggah ke sistem elektronik memiliki rekaman digital yang tidak dapat dihapus. Akan tetapi, karena sistem perlindungan yang tidak memadai, masih terjadi kesalahan secara tidak sengaja di lapangan. Ini memungkinkan perampok informasi pribadi orang lain dibobol, diperjualbelikan, atau digunakan untuk tujuan ilegal. Hal ini menekankan pentingnya evaluasi menyeluruh terhadap protokol keamanan bank digital, serta penyusunan rencana respons insiden yang cepat dan efektif untuk meminimalkan dampak jangka panjang terhadap kepercayaan nasabah. Risiko kebocoran data nasabah dapat berasal dari pengelolaan data yang buruk, terdapat celah pada keamanan data, proses otentikasi yang lemah, semakin lemah sebuah sistem maka semakin mudah sistem tersebut disusupi, maka dari itu harus ada upaya pencegahan yang dilakukan seperti mengelola akses data dengan ketat menggunakan metode autentikasi yang aman seperti autentikasi dua faktor, implementasi keamanan berlapis seperti firewall dan enkripsi data, lalu melakukan audit dan monitoring berkala terhadap sistem keamanan dan aktivitas jaringan untuk mendeteksi potensi ancaman lebih awal. Kebocoran Data ini berdampak terhadap kepercayaan konsumen terhadap keamanan data yang akan dibagikan. Akibatnya, Bank akan menghadapi beberapa jenis risiko antara lain risiko stratejik, risiko operasional, risiko hukum dan resiko reputasi, Salah satu faktor yang menjadi pertimbangan konsumen untuk membagikan data pribadi adalah kepercayaan terhadap perusahaan. Rusaknya kinerja perusahaan, seperti terjadi kasus kebocoran data, dapat mengakibatkan hilangnya konsumen dan turunnya pendapatan, bahkan didenda. Ketika konsumen kehilangan kepercayaan pada perusahaan, mereka mulai mencari alternatif. Hal ini bisa mengarahkan mereka kepada pesaing yang tidak mengalami serangan cyber. Pemulihan reputasi membutuhkan upaya dan biaya yang besar untuk membangun kembali kepercayaan konsumen, insiden pelanggaran data tidak hanya masalah keamanan informasi tetapi juga berdampak pada stabilitas finansial, operasional, dan reputasi organisasi. Hal ini menekankan pentingnya langkah pencegahan serta respon cepat dalam menghadapi insiden tersebut.

PERLINDUNGAN HUKUM TERKAIT RISIKO DAN TANTANGAN BANK DIGITAL

Perlindungan hukum adalah upaya melalui instrumen hukum untuk menjamin bahwa hak-hak individu dapat terlindungi dan tidak dilanggar. Perlindungan hukum juga dapat diartikan sebagai upaya untuk memberikan rasa aman kepada masyarakat, baik secara fisik maupun pikiran dari berbagai ancaman dan gangguan. Perlindungan Hukum dapat dibagi menjadi dua bentuk utama, yaitu:

1) Perlindungan Hukum Preventif, yang mencakup peraturan pencegahan yang berfungsi sebagai standar untuk setiap tindakan masyarakat, mencakup semua aspek tindakan manusia.
2) Perlindungan Hukum Represif, berupa tindakan korektif setelah terjadinya pelanggaran terhadap hak seseorang atau kelompok dimana badan-badan hukum yang mengurus dalam upaya penyelesaian sengketa.

Terminologi Hukum mencakup beberapa konsep dan mekanisme yang digunakan dalam sistem hukum nasional untuk melindungi hak-hak warga negara. Terminologi ini membentuk dasar dari sistem perlindungan hukum yang efektif, dimana setiap individu memiliki hak untuk dilindungi oleh hukum dan mendapatkan keadilan melalui prosedur yang ditetapkan. Dalam konteks ini, negara memegang peran penting sebagai pelindung utama melalui institusi-institusi seperti pengadilan, polisi, dan lembaga hak asasi manusia. Namun perlindungan hukum juga dapat dilakukan oleh organisasi non-pemerintah, pengacara, dan lembaga internasional yang berfokus pada advokasi dan perlindungan hak- hak individu. Secara keseluruhan, perlindungan hukum adalah salah satu pilar utama dalam sistem hukum yang berfungsi untuk menjaga keadilan, ketertiban, dan keamanan dalam masyarakat. Dibawah ini terdapat perlindungan hukum terkait risiko yang dibahas pada pembahasan sebelumnya:

1. **Perlindungan Hukum Risiko Perlindungan Data Pribadi** dalam konteks bank digital dan pengaturannya dalam peraturan perundang-undanganya di Indonesia. Hukum Perlindungan Data Pribadi memerlukan dasar teoritis untuk memastikan dicapainya stabilitas (*stability*), dapat memprediksi (*predictability*), dan keadilan (*fairness)* dalam keseluruhan system hukum, ekonomi, dan teknologi terhadap peradaban manusia Adaptasi Kehidupan Baru.Hukum Perlindungan Data Pribadi adalah konseptual *Sui General Lex Habeas* (Bersumber dari Buku yang Berjudul "Hukum Perlindungan Data Pribadi dan Data Nasional" Karya Danrivanto Budhijanto) dengan yuridiksi teritorial dan virtual. Ada Prinsip Utama yang mengatur perlindungan data pribadi yaitu:
   a) Pengumpulan dan Pemrosesan Data yang harus dilakukan secara sah, transparan, dan sesuai dengan tujuan yang jelas serta sah. Setiap data pribadi yang dikumpulkan harus relevan dan terbatas pada apa yang diperlukan untuk tujuan pemrosesan tertentu. Dalam proses ini, organisasi harus memastikan bahwa pemilik data memahami alasan pengumpulan data, serta hak-hak mereka terkait data pribadi tersebut.
   b) Inovasi Terbaru Layanan Digital yang harus terus berkembang, karena organisasi perlu mengikuti inovasi teknologi terbaru untuk memastikan data pribadi konsumen tetap aman dan memberikan transparasi bagi pengguna sehingga pengguna mempunyai kontrol yang lebih besar atas data mereka pribadi.
   c) Peningkatan Kapasitas Keamanan Data yang melibatkan teknologi enkripsi, autentikasi ganda, firewall, dan sistem pemantauan keamanan yang dapat mendeteksi aktivitas mencurigakan. Selain mengembangkan teknologi, diperlukan pelatihan bagi karyawan dalam menangani data pribadi dengan aman.
   d) Adaptasi Terhadap Perkembangan Teknologi Terbaru dengan cara menyesuaikan kebijakan dan prosedur perlindungan data dengan kemajuan teknologi terbaru. Adaptasi ini meliputi pengintegrasian solusi berbasis kecerdasan buatan, big data, internet of things, dan cloud computing. Akan tetapi organisasi juga wajib mengantisipasi risiko baru yang muncul akibat perkembangan teknologi tersebut.

Sebelum UU PDP disahkan, perlindungan data pribadi di Indonesia diatur oleh berbagai peraturan perundang-undangan yang bersifat sektoral, seperti:

a) Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik mengubah beberapa ketentuan dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang- Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Perubahan dalam UU ini termasuk penyempurnaan definisi dan aturan mengenai pengelolaan data pribadi serta sanksi yang lebih jelas bagi pelanggaran terhadap privasi dan keamanan data tersebut.
b) Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (KIP), yang mengatur tentang hak setiap orang untuk memperoleh informasi publik, dengan tetap memperhatikan perlindungan data pribadi

c) Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, yang mengakui hak atas privasi sebagai salah satu hak asasi manusia

d) Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022, yang mengatur perlindungan data pribadi mewajibkan bagi pengendali data pribadi seperti menjaga keamanan dan kerahasiaan data, serta memastikan akurasi data yang diproses, dan Undang-Undang ini juga mengatur sanksi pidana dan perdata bagi pelanggaran terhadap ketentuan perlindungan data pribadi.

2. **Perlindungan Hukum Risiko Serangan Siber** dalam konteks Bank Digital dan pengaturan perundang-undangannya di Indonesia. Bank Digital mengelola data sensitive dan aset finansial nasabah yang sangat rentan terhadap berbagai ancaman siber. Regulasi mengenai keamanan siber dalam konteks bank digital harus dirancang untuk menghadirkan perlindungan yang menyeluruh, mencakup aspek territorial dan virtual, dan menjangkau seluruh sistem perbankan digital. Prinsip Utama yang mengatur risiko serangan siber, yaitu:

   a) Edukasi dan Kesabaran Siber adalah hal dasar dalam pencegahan serangan siber. Organisasi perlu memastikan bahwa seluruh karyawan memiliki pemahaman yang kuat tentang risiko siber dan langkah-langkah pencegahan yang harus diambil. Edukasi terhadap konsumen juga merupakan hal penting agar konsumen memiliki pemahaman terkait ancaman siber.

   b) Inovasi berkelanjutan di Bidang Keamanan Siber dengan cara organisasi harus berkomitmen pada inovasi berkelanjutan dalam teknologi keamanan siber mengingat metode serangan siber juga semakin canggih. Organisasi secara aktif berinvestasi dalam riset dan pengembangan sistem keamanan yang lebih tangguh. Inovasi ini memungkinkan organisasi selalu siap menghadapi ancaman-ancaman baru.

   c) Penginkatan Kapasitas Keamanan Siber meliputi penguatan infrastruktur, peralatan, dan kemampuan teknologi untuk melindungi sistem dari berbagai ancaman. Disamping teknologi, perlu adanya peningkatan dalam prosedur keamanan yang mencakup respon cepat, pemantauan real-time, dan mekanisme pemulihan data setelah serangan.

   d) Kewajiban Pelaporan dan Transparasi merupakan prosedur keamanan yang penting. Organisasi harus memiliki prosedur yang jelas dan tertata untuk melaporkan setiap insiden serangan siber, baik ke dalam organisasi maupun kepada otoritas terkait. Transparasi dalam proses keamanan siber meningkatkan kepercayaan publik dan memungkinan pihak eksternal, seperti regulator dan mitra bisnis.

Untuk mengantisipasi dan memitigasi risiko serangan siber, pemerintah Indonesia telah memperbaharui beberapa peraturan perundang-undangan dan mengeluarkan undang- undang baru di tahun 2024 yang memberikan perlindungan hukum lebih komprehensif bagi perbankan digital. Berikut beberapa landasan hukum utamanya:

a) Peraturan Otoritas Jasa Keuangan No. 24/POJK.03/2023 yang meliputi tentang Peningkatan Standar Keamanan, Manajemen Risiko Siber, Kewajiban Pelaporan, dan Kolaborasi dan Pemantauan.

b) Surat Edaran Otoritas Jasa Keuangan (SEOJK) No. 12/SEOJK.03/2023 yang memperbaharui dan memperluas ketentuan terkait Peningkatan Kapasitas Keamanan Siber, Manajemen Risiko Siber yang Lebih Baik, Audit dan Pemantauan Berlanjut, dan Peningkatan Pelaporan Insiden Siber.

c) Pasal 35 Undang-Undang ITE yang menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar dianggap seolah-olah data yang otentik, Dapat dipidana.

3. **Perlindungan Hukum Risiko Kebocoran Data Nasabah** dalam konteks Bank Digital dan pengaturan perundang-undangannya di Indonesia. Kebocoran data nasabah adalah peristiwa

di mana informasi pribadi atau sensitif milik nasabah diakses, diungkapkan, atau disalahgunakan tanpa izin. Perlindungan hukum terhadap risiko kebocoran data nasabah semakin mendesak di era perbankan digital untuk menjamin keamanan data dan kepercayaan masyarakat. Sistem hukum yang kuat diperlukan untuk memastikan bahwa aturan yang berlaku bersifat stabil dan dapat diandalkan. Prinsip Utama yang mengatur risiko kebocoran data nasabah yaitu:

a) Kerahasiaan dan Integritas Data dipertahankan dengan menerapkan pengawasan ketat untuk mendeteksi perubahan yang mencurigakan. Kerahasiaan data harus dipastikan bahwa data nasabah hanya dapat diakses oleh pihak berwenang, dan integritas data memastikan bahwa data tersebut tetap akurat, lengkap, dan tidak mengalami perubahan yang tidak sah
b) Tanggung Jawab dan Akuntabilitas berarti setiap organisasi memiliki kewajiban untuk melindungi data nasabah dan bertanggung jawab atas segala potensi kebocoran dan pelanggaran yang terjadi alam hal terjadi insiden kebocoran data, organisasi wajib melakukan pelaporan dan menjalankan prosedur yang tepat untuk memperbaiki situasi
c) Perlindungan Hak Nasabah untuk memastikan bahwa nasabah memiliki kontrol dan hak atas data pribadi mereka yang disimpan oleh bank. Hak-hak ini meliputi hak akses, hak untuk mengubah data, hak atas transparansi penggunaan data, serta hak untuk menghapus data pribadi jika tidak diperlukan lagi. Dengan memberikan hak-hak tersebut, bank digital tidak hanya memenuhi standar hukum, tetapi juga meningkatkan rasa aman nasabah
d) Pemulihan dan Perbaikan memastikan bahwa ketika terjadi insiden kebocoran data, organisasi memiliki rencana pemulihan dan perbaikan yang cepat dan efektif. Pemulihan meliputi tindakan langsung untuk menghentikan kebocoran, memberitahukan nasabah yang terdampak, serta memberikan langkah mitigasi yang dapat diambil oleh nasabah. Selain itu, perbaikan juga melibatkan evaluasi dan pembaruan sistem keamanan untuk mencegah terulangnya insiden serupa di masa mendatang

Perlindungan hukum terhadap risiko kebocoran data nasabah dalam perbankan digital di Indonesia telah menjadi fokus utama seiring dengan perkembangan teknologi dan digitalisasi di sektor perbankan. Untuk mengantisipasi dan memitigasi risiko kebocoran data nasabah, Berikut adalah landasan perlindungan hukum yang diatur berdasarkan undang-undang:

a) Peraturan Otoritas Jasa Keuangan No. 24/POJK.03/2023 yang meliputi tentang Peningkatan Standar Keamanan, Manajemen Risiko Siber, Kewajiban Pelaporan, dan Kolaborasi dan Pemantauan
b) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
c) Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022, yang mengatur perlindungan data pribadi mewajibkan bagi pengendali data pribadi seperti menjaga keamanan dan kerahasiaan data, serta memastikan akurasi data yang diproses, dan Undang-Undang ini juga mengatur sanksi pidana dan perdata bagi pelanggaran terhadap ketentuan perlindungan data pribadi.

KESIMPULAN

Kesimpulan penelitian ini menegaskan bahwa transformasi digital di sektor perbankan menawarkan peluang besar, namun tantangan yang menyertainya masih belum sepenuhnya teratasi. Masalah-masalah seperti perlindungan data pribadi, serangan siber, dan kebocoran data nasabah menunjukkan bahwa langkah-langkah saat ini belum cukup untuk memberikan jaminan keamanan yang komprehensif. Dalam penelitian ini, beberapa solusi telah diidentifikasi yaitu Harmonisasi dan penyempurnaan kerangka hukum, Implementasi teknologi canggih seperti autentikasi berbasis biometrik dan pemantauan berbasis AI, Edukasi Masyarakat, Kolaborasi Antar-Pemangku Kepentingan. Dengan implementasi langkah-langkah tersebut, meskipun belum

sepenuhnya menyelesaikan masalah, penelitian ini memberikan dasar bagi pengembangan solusi yang lebih menyeluruh. Pendekatan ini diharapkan mampu mendorong transformasi digital di sektor perbankan secara aman, transparan, dan berkelanjutan.

DAFTAR PUSTAKA

Danrivanto Budhijanto. (2023). *Hukum Perlindungan Data Pribadi di Indonesia*, Bandung: Refika Aditama.

Bayu Perwira Hie. (2021). *Transformasi Digital Bank di Indonesia: Konsep dan Praktek dalam Memimpin Transformasi Total.* Malang: Media Nusa Creative.

Uly Handayani Mukhra, dkk. (2024). *Mobile Banking dalam Presepsi Nasabah, Aceh*: Syiah Kuala University Press.

Jamal Wiwoho, Pujiyono, Irwan Trinugroho, Dona Budi Kharisma. (2023). *Hukum Ekonomi Digital.* Yogyakarta : Thafa Media.

Yusuf Shofie. (2021). *Tanggungjawab Korporasi dalam Hukum Perlindungan Konsumen di Indonesia*. Bandung : PT Citra Aditya Bakti.

Beridiansyah. (2021). *Kejahatan Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia*. Aceh : Syiah Kuala University Press

Eliani Bate'e, dkk. (2024). *Tindak Pidana Informasi Teknologi Cyber Crime.* Ponorogo : Uwais Inspirasi Indonesia.

FA Suharno. (2024). *Manajemen Strategi Menghadapi Peperangan Cyber.* Yogyakarta : AG Publishing,.

Made Sudarma. (2024). *Manajemen Data.* Jambi : PT Sonpedia Publishing Indonesia.

Suharbi, M. A., & Margono. H., (2022). "Kebutuhan transformasi bank digital Indonesia di Era Revolusi Industri 4.0" *Jurnal Ilmiah Akuntansi dan Keuangan*, 4 (10).

Siti Yuniarti (2019). "PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA" *Business Economic, Communication, and Social Science Journal*, 1(1).

Faiz Rahman (2021). "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia" *Jurnal Legislasi Indonesia*. 3(2).

Yusuf Daeng dkk (2023). "Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi", *Journal Of Social Science Research.* 3 (6).

Wenderlin Koswara (2022). "Implementasi Aturan Perlindungan Data Pribadi Oleh Penyelenggara Sistem Elektronik Dikaitkan Dengan Teori Keadilan dan Kepastian Hukum" *Jurnal Paradigma Hukum Pembangunan*. 7(2).

Kusuma, A.C & Rahmani, A.D. *"*Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)*" SUPREMASI JURNAL HUKUM*, 5(1).

Abubakar, L., & Handayani, T. (2022). *"*PENGUATAN REGULASI: UPAYA PERCEPATAN TRANSFORMASI DIGITAL PERBANKAN DI ERA EKONOMI DIGITAL*" Jurnal Masalah-Masalah Hukum,* 51(3).

Setiawan, H.B., & Najicha, F.U. 2022. "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data" *Jurnal Kewarganegaraan*, 6(1).

Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik mengubah beberapa ketentuan dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (KIP), yang mengatur tentang hak setiap orang untuk memperoleh informasi publik, dengan tetap memperhatikan perlindungan data pribadi

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, yang mengakui hak atas privasi sebagai salah satu hak asasi manusia.

Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022

Peraturan Otoritas Jasa Keuangan No. 24/POJK.03/2023 yang meliputi tentang Peningkatan Standar Keamanan, Manajemen Risiko Siber, Kewajiban Pelaporan, dan Kolaborasi dan Pemantauan

Surat Edaran Otoritas Jasa Keuangan (SEOJK) No. 12/SEOJK.03/2023

Undang – Undang ITE Pasal 35

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

BRI api, Tantangan Perbankan di Era Digital, https://developers.bri.co.id/id/news/9-tantangan- perbankan-di-era-digital-dan-cara-briapi-meresponnya

Website Kompas, "Kenali Jenis Jenis Kejahatan Siber di Sektor Perbankan", https://money.kompas.com/read/2021/11/10/071027026/kenali-jenis-jenis-kejahatan-siber-di- sektor-perbankan