KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.2, No.1 Februari 2025
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 103-114
DOI: https://doi.org/10.61722/jmia.v2i1.3180

Kerahasiaan Bank vs Hak Atas Informasi: Mengurai Konflik Kepentingan dalam Perlindungan Data Pribadi

Widiya Dwi Novarianti
Universitas Negeri Semarang
Athalia Pranata Putri S Meliala
Universitas Negeri Semarang
Nova Arini Stevia Yusuf
Universitas Negeri Semarang
Bintang Naharika Citra Melati
Universitas Negeri Semarang
Fakultas Hukum Universitas Negeri Semarang
Kampus Sekaran, Gedung K, Gunungpati, Kota Semarang,
Jawa Tengah, Indonesia 50229
Korespondensi penulis : widiyadwinovarianti@students.unnes.ac.id

Abstrak. *Bank confidentiality and the right to information are two principles that often have the potential to conflict, especially in the context of personal data protection. Bank have an obligation to maintain the confidentiality of customer data in accordance with the principles of bank secrecy regulated in the banking law, but on the other hand, they are also required to provide information to the authorities based on certain statutory regulations, such as tax law, anti money laundering and eradication. Terrorism. This conflict creates challenges in ensuring the protection of customers personal data without violating the public's right to information. In the context of Indonesian law, regulations regarding through harmonization of regulations which prioritize the principles of proportionality and public interest. This research outlines the efforts that banks can make to maintain a balance between these two obligations, including the implementation of data security technology, internal supervision, and compliance with the relevant legal framework. This strategy is expected while fulfilling banking legal obligations.*
Keywords : Bank confidentiality, Protection of personal data, Legal compliance.

Abstrak. Kerahasiaan bank dan hak atas informasi merupakan dua prinsip yang kerap berpotensi berbenturan, terutama dalam konteks perlindungan data pribadi. Bank memiliki kewajiban menjaga kerahasiaan data nasabah sesuai dengan prinsip kerahasiaan bank yang diatur dalam Undang-undang perbankan, namun di sisi lain, mereka juga diwajibkan memberikan informasi kepada pihak berwenang berdasarkan peraturan perundang-undangan tertentu, seperti hukum perpajakan, anti pencucian uang, dan pemberantasan terorisme. Konflik ini menimbulkan tantangan dalam memastikan perlindungan data pribadi nasabah tanpa melanggar hak masyarakat hak atas informasi. Dalam konteks hukum indonesia, pengaturan mengenai hal ini diatur melalui harmonisasi regulasi yang mengedepankan asas proporsionalitas dan kepentingan publik. Penelitian ini mengurai upaya yang dapat dilakukan bank untuk menjaga keseimbangan antara kedua kewajiban tersebut, termasuk implementasi teknologi keamanan data, pengawasan internal, serta kepatuhan terhadap kerangka hukum yang relevan. Strategi ini diharapkan dapat melindungi kepentingan nasabah sekaligus memenuhi kewajiban hukum perbankan.
Kata Kunci : Kerahasiaan bank, Perlindungan data pribadi, Kepatuhan hukum.

PENDAHULUAN

Kerahasiaan data pribadi nasabah adalah salah satu pilar utama dalam menjaga kepercayaan publik terhadap institusi perbankan. Bank memegang peranan strategis dalam menjaga stabilitas ekonomi, yang sebagian besar bergantung pada kepercayaan nasabah terhadap integritas dan profesionalisme lembaga keuangan tersebut. Prinsip kerahasiaan ini diatur secara tegas dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang mengangkut

Received September 30, 2024; Revised Oktober 30, 2024;Desember 10, 2024
* Widiya Dwi Novarianti, *widiyadwinovarianti@students.unnes.ac.id*

identitas, transaksi keuangan, maupun informasi lain yang diperoleh melalui hubungan nasabah dengan bank. Kegagalan bank dalam menjaga kerahasiaan ini tidak hanya akan merusak reputasi lembaga keuangan, tetapi juga berpotensi menimbulkan kerugian bagi nasabah dan melemahkan kepercayaan terhadap sistem perbankan secara keseluruhan. Namun di sisi lain, tuntutan untuk memberikan informasi yang relevan kepada masyarakat juga merupakan hak yang dijamin oleh konstitusi dan berbagai peraturan perundang-undangan. Yakni Undang-undang Nomor 14 Tahun 2008 tentang keterbukaan informasi publik mengatur bahwa informasi yang bersifat strategis atau berkaitan dengan kepentingan publik harus dapat diakses oleh masyarakat luas. Dalam konteks perbankan, kebutuhan untuk mengungkap informasi tertentu sering kali muncul dalam situasi-situasi seperti pengungkapan tindak pidana korupsi, pencucian uang, atau pendanaan terorisme. Tuntutan ini menciptakan dilema hukum ketika kewajiban menjaga kerahasiaan data pribadi nasabah harus berhadapan dengan hak atas informasi yang bersifat publik. Konflik antara kedua kepentingan ini semakin kompleks dengan hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU DP). Undang-undnag ini memberikan perlindungan komprehensif terhadap data pribadi serial individu, termasuk nasabah bank, sekaligus mewajibkan pengendali data untuk transparansi dalam pengelolaanya. UU PDP juga memperkenalkan konsep yang lebih spesifik terkait pengendalian data, batasan-batasan pemrosesan data, serta hak-hak subjek data pribadi., seperti hak untuk mengakses, mengoreksi dan menghapus data mereka. Ketentuan ini, meskipun bertujuan memberikan perlindungan yang lebih baik bagi privasi individu, dapat memperumit pengaturan hukum terkait kewajiban bank dalam memberikan informasi kepada pihak berwenang, seperti penyidik atau aparat hukum. Dalam praktiknya, menjaga keseimbangan antara kerahasiaan dan hak atas informasi tidak hanya melibatkan persoalan hukum, tetapi juga berdampak pada aspek teknis, manarjal dan etika. Kerahasiaan data pribadi nasabah, misalnya tidak boleh digunakan sebagai dalih untuk menutup-nutupi informasi yang relevan dalam pengungkapan tindak pidana atau penyelamatan kepentingan publik. Sebaliknya tuntutan atas keterbukaan informasi juga harus diatur secara hati-hati agar tidak menimbulkan pelanggaran privasi yang dapat merugikan individu maupun perusahaan. Dengan kata lain, baik kerahasiaan maupun keterbukaan harus dikelola dalam kerangka hukum yang seimbang dan saling melengkapi, bukan saling bertentangan. Dalam hal ini menunjukkan perlunya pengaturan hukum yang lebih terintegrasi dan meminimalkan konflik antara prinsip dan hak atas informasi. Beberapa negara telah mengembangkan pendekatan yang lebih matang dalam menyelesaikan konflik ini, seperti dengan menetapkan batasan yang jelas mengenai jenis informasi yang dapat diakses publik, menciptakan prosedur ketat untuk proses pengungkapan informasi, serta menerapkan mekanisme akuntabilitas yang memastikan data rahasia hanya diakses oleh pihak yang berwenang. Di indonesia, meskipun sudah ada berbagai aturan hukum yang mengatur kerahasiaan data nasabah dan hak atas informasi, kenyataan implementasi di lapangan seringkali menghadapi berbagai tantangan. Salah satu masalah utama adalah kurangnya koordinasi antara lembaga yang terlibat dalam pengaturan dan pengawasan, sehingga menyebabkan kebijakan yang tumpang tindih. Selain itu, secara teknis, banyak bank belum sepenuhnya siap untuk mengelola data sesuai dengan standar keamanan dan transparansi yang diharapkan, sehingga menciptakan potensi hukum yang lebih besar. Dalam beberapa situasi, seperti kasus penyidikan tindak pidana keuangan, bank sering mendapat tekanan dari pihak berwenang untuk memberikan data atau informasi yang seharusnya dirahasiakan. Tekanan semacam ini menjadi semakin intensif dalam kondisi krisis, misalnya ketika ada skandal keuangan besar atau ancaman terhadap stabilitas ekonomi nasional. Jika bank tidak hati-hati dalam memberikan informasi, ini dapat menimbulkan pelanggaran privasi yang merugikan

nasabah, sekaligus merusak reputasi lembaga perbankan itu sendiri. Namun, jika bank terlalu tertutup, masyarakat bisa kehilangan kepercayaan karena dianggap menyembunyikan fakta yang sebenarnya penting untuk diketahui. Ketiadaan transparansi dalam pengelolaan informasi publik juga bisa menjadi masalah yang serius. Misalnya, jika data yang relevan tidak disampaikan kepada masyarakat secara akurat, ini dapat memunculkan spekulasi negatif yang semakin memperkeruh situasi. Hal ini pada akhirnya bisa berdampak buruk terhadap kepercayaan masyarakat terhadap bank dan bahkan sistem perbankan secara keseluruhan. Oleh karena itu, penting bagi bank untuk menemukan cara agar dapat menyeimbangkan kedua prinsip ini yakni menjaga kerahasiaan data pribadi nasabah sekaligus memenuhi kewajiban memberikan informasi kepada publik atau pihak yang berkepentingan. Penelitian ini berfokus untuk menjawab tantangan tersebut dengan menguraikan konflik kepentingan yang muncul di antara kewajiban bank untuk menjaga kerahasiaan data nasabah dan tuntutan akan keterbukaan informasi. Penelitian ini juga bertujuan untuk menawarkan solusi berbasis hukum yang tidak hanya relevan dengan konteks nasional tetapi juga mempertimbangkan praktik-praktik terbaik dari negara lain. Harapannya, hasil penelitian ini dapat menjadi dasar bagi pengembangan kebijakan yang lebih seimbang, adil, dan berkelanjutan dalam menghadapi era keterbukaan informasi dan perlindungan data pribadi. Dengan pendekatan yang lebih praktis dan adaptif, penelitian ini tidak hanya ingin mengidentifikasi permasalahan tetapi juga memberikan kontribusi nyata dalam menciptakan pengaturan hukum yang lebih baik di Indonesia. Ini penting, terutama di tengah perkembangan teknologi yang semakin cepat dan kebutuhan akan regulasi yang mampu menjawab tantangan zaman.

KAJIAN TEORI

1. Kepastian Hukum

Kepastian hukum adalah konsep mendasar dalam dunia hukum yang menekankan pentingnya kejelasan dan konsistensi dalam aturan-aturan yang berlaku. Dengan adanya kepastian hukum, setiap individu dapat memahami dengan jelas ini dan maksud dari suatu peraturan, serta mampu memprediksi konsekuensi dari tindakan yang mereka lakukan. Dalam konsep ini juga memberikan rasa aman bagi masyarakat, karena hukum ditegakkan secara adil dan tidak berubah. Dalam konteks ini, kepastian hukum menjadi landasan utama dalam menciptakan tatanan masyarakat yang tertib, dimana hak dan kewajiban setiap orang dapat dijalankan dengan baik tanpa adanya ambiguitas atau ketidak jelasan dalam penerapan hukum. Menurut Gustav Radbruch menyatakan bahwa kepastian hukum adalah salah satu tujuan utama yang ingin dicapai oleh sistem hukum. Menurutnya, kepastian hukum berfungsi sebagai landasan bagi individu untuk dapat memperkirakan dampak dari tindakan yang mereka ambil dalam konteks hukum.[1] Dengan adanya kepastian hukum, masyarakat dapat memahami dengan jelas batasan dan konsekuensi yang diatur oleh hukum, sehingga tercipta rasa aman dalam bertindak. Selain itu, kepastian hukum juga menjadi prasyarat penting untuk menegakkan prinsip non diskriminasi, dimana setiap individu harus mendapatkan perlakuan yang setara dihadapan hukum tanpa kecuali. Tanpa adanya kepastian hukum, masyarakat tidak memiliki acuan yang tegas untuk bertindak sesuai aturan.

Dalam konteks perlindungan data pribadi, kepastian hukum menjadi penting bagi lembaga keuangan untuk memahami dan menjalankan kewajiban mereka sesuai dengan kerangka hukum yang berlaku. Undang-undang terkait perlindungan data, seperti General Data Protection

[1] Haprabu, P. S. (2023). *PENERAPAN ASAS KEPASTIAN HUKUM PENYELESAIAN KERUGIAN NASABAH BANK DALAM PENGGUNAAN UANG ELEKTRONIK (BRIZZI)* (Doctoral dissertation, FAKULTAS HUKUM UNIVERSITAS PASUNDAN).

Regulation (GDPR) di tingkat internasional atau regulasi setara di Indonesia seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), memberikan pedoman yang pasti bagi bank untuk menjaga kerahasiaan data nasabah. Hal ini selaras dengan prinsip kepastian hukum yang mendorong semua pihak untuk mengetahui dan mematuhi aturan yang ada.[2] Di sisi lain, hak masyarakat untuk mendapatkan informasi, terutama yang berkaitan dengan kebijakan publik dan transparansi operasi lembaga keuangan, juga harus di akomodasi. Dalam hal ini, bank menghadapi tantangan untuk menyeimbangkan dua kewajiban hukum: menjaga kerahasiaan data pribadi dan memenuhi prinsip keterbukaan informasi. Menurut Radbruch, kepastian hukum membantu menghindari ambiguitas dalam pelaksanaan kewajiban ini dengan menyediakan batasan dan mekanisme yang jelas mengenai bagaimana kedua hal tersebut dapat dikelola secara harmonis tanpa saling bertentangan.

2. Keseimbangan Kepentingan

Keseimbangan kepentingan (*balancing of interests*) adalah kerangka teori yang digunakan untuk menilai dan mengharmonisasikan berbagai kepentingan yang saling bertentangan dalam suatu konteks hukum atau sosial. Dalam konteks kerahasiaan bank dan hak atas informasi, teori ini menjadi relevan untuk mengurai konflik antara kepentingan perlindungan data pribadi nasabah dan kebutuhan akan transparansi atau keterbukaan informasi. Kerahasiaan bank bertujuan melindungi privasi dan kepercayaan nasabah terhadap institusi perbankan, sementara hak atas informasi mendorong akses terhadap data yang mungkin diperlukan untuk tujuan hukum, pengawasan, atau publikasi tertentu. Keseimbangan antara kedua kepentingan ini harus mempertimbangkan prinsip proporsionalitas, di mana kepentingan yang lebih besar atau yang mendesak diberikan prioritas tanpa mengabaikan nilai penting dari kepentingan lainnya. Dalam praktiknya, pendekatan ini melibatkan analisis kontekstual terhadap dampak perlindungan data pribadi terhadap kebebasan informasi, termasuk menilai tujuan penggunaan data, risiko terhadap hak individu, dan manfaat sosial yang dihasilkan. Dengan demikian, penerapan teori keseimbangan kepentingan memungkinkan pengambilan keputusan yang adil, akuntabel, dan berbasis pada prinsip perlindungan hak asasi manusia.

3. Kepatuhan Hukum

Pada penelitian terdahulu yang ditulis oleh Natanael Rolas Midian Simbolon (2023). Mengkaji mengenai perlindungan kerahasiaan bank di Indonesia, yang diatur dalam Pasal 40 UU No. 10 Tahun 1998 tentang Perbankan, memiliki peran penting dalam menjaga privasi nasabah, yang pada gilirannya memelihara kepercayaan publik terhadap sistem perbankan. Salah satu penelitian yang relevan adalah mengenai kepatuhan bank terhadap prinsip kerahasiaan yang diatur oleh undang-undang dan peraturan sektoral lain, seperti POJK terkait perlindungan konsumen. Penelitian ini menunjukkan bahwa bank memiliki kewajiban untuk menjaga informasi nasabah sebagai bagian dari tanggung jawab mereka terhadap privasi dan keamanan data, serta menumbuhkan kepercayaan nasabah terhadap lembaga keuangan.[3] Kemudian penelitian yang ditulis oleh Merta (2021). Menjelaskan mengenai Undang-Undang Perlindungan Konsumen mengatur hak dan kewajiban baik bagi konsumen maupun pelaku usaha dalam transaksi barang atau jasa. Pemerintah melalui BPSK (Badan Penyelesaian Sengketa Konsumen) telah menyediakan sarana untuk menyelesaikan sengketa antara konsumen dan pelaku usaha, yang

[2] Hendri, H., Suriyanto, S., & Pranacitra, R. (2023). Kepastian Dan Perlindungan Hukum Terhadap Data Pribadi Pengguna Fintech Peer To Peer Lending. *Jurnal Ilmiah Universitas Batanghari Jambi*, *23*(1), 848-854.
[3] Simbolon, N. R. M. (2023). PENEGAKAN HUKUM TERHADAP PENYALAHGUNAAN DATA NASABAH BANK DI ERA KETERBUKAAN INFORMASI. *Jurnal Darma Agung*, *31*(6), 49-62.

hingga kini terus beroperasi. [4]Meskipun BPSK berfokus pada penyelesaian sengketa untuk kepentingan konsumen, terkadang hak-hak pelaku usaha tidak selalu dilindungi dengan baik, dan konsumen sering kali diuntungkan dalam beberapa kasus. Salah satu contoh kasus yang diteliti menunjukkan bahwa BPSK menawarkan dua solusi penyelesaian, yaitu perdamaian, di mana kerugian konsumen dibagi dua dengan pihak bank. Pihak Maybank menyatakan bahwa mereka akan menanggung kerugian nasabah selama penyelidikan yang dilakukan oleh kepolisian, sesuai dengan ketentuan dalam Undang-Undang Nomor 8 Tahun 1999 dan peraturan hukum yang berlaku.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif analitis. Pendekatan ini digunakan untuk mendalami isu konflik kepentingan antara kerahasiaan data nasabah dan hak atas informasi, serta untuk memahami dan menganalisis pengaturan hukum yang relevan di Indonesia. Proses penelitian dilakukan melalui pengumpulan data sekunder yang meliputi dokumen hukum, literatur akademik, laporan penelitian sebelumnya serta publikasi resmi dari institusi terkait. dan analisis data secara sistematis, dengan tujuan menghasilkan rekomendasi. Penelitian ini berfokus pada pengaturan hukum di indonesia dengan analisis terhadap lembaga perbankan nasional,regulasi sektor keuangan dan sistem hukum yang berlaku.

HASIL PENELITIAN DAN PEMBAHASAN

1.1. Bagaimana Bank Dapat Menjaga Kerahasiaan Data Pribadi Nasabah Tanpa Mengabaikan Hak Masyarakat Atas Informasi yang Diatur Dalam Peraturan Perundang-Undangan

Lembaga keuangan, termasuk bank, harus memperhatikan perlindungan data pribadi dalam era digital yang semakin berkembang. Seiring dengan peningkatan kekhawatiran masyarakat tentang potensi penyalahgunaan data pribadi, bank memiliki tanggung jawab yang besar untuk menjaga kerahasiaan dan keamanan data pribadi nasabah. Sebaliknya, masyarakat juga berhak atas informasi. Peraturan perundang-undangan mengatur informasi terkait kebijakan publik dan transparansi operasi lembaga keuangan. Oleh karena itu, salah satu masalah utama yang dihadapi oleh bank adalah menjaga keseimbangan antara kewajiban mereka untuk melindungi data pribadi pelanggan dan hak masyarakat untuk mendapatkan informasi dengan cara yang sesuai dengan peraturan.Untuk melakukannya, bank harus membuat kebijakan yang memungkinkan keduanya berjalan secara proporsional. Pertama, bank harus menerapkan sistem keamanan yang canggih untuk melindungi data pribadi nasabah, seperti enkripsi data, kontrol akses yang ketat, dan pelatihan staf tentang keamanan data. Selain itu, bank harus memastikan bahwa informasi pelanggan hanya digunakan untuk tujuan yang sah dan dengan persetujuan nasabah, dan tidak diberikan kepada pihak ketiga tanpa izin yang jelas kecuali dalam kasus yang diatur oleh hukum. Sebaliknya, bank harus mematuhi prinsip transparansi yang diatur oleh peraturan perundang-undangan; misalnya, mereka dapat menyediakan laporan tahunan yang menunjukkan kinerja dan kesehatan finansial mereka, tetapi tidak mencakup informasi yang dapat mengidentifikasi nasabah atau mengungkapkan data pribadi mereka. Untuk menghormati hak privasi individu dan

[4] Merta, M., & Sudiro, A. (2021). Pertanggungjawaban Bank Atas Pelanggaran Kerahasiaan Data Pribadi Milik Nasabah Yang Dilakukan Pegawai Bank Berdasarkan Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan. *Jurnal Hukum Adigama*, *4*(1), 824-844.

memenuhi kewajiban transparansi masyarakat, proses pengelolaan informasi ini harus dilakukan dengan hati-hati dan bertanggung jawab.

Bank dapat menjalankan kebijakan dan praktik yang sesuai dengan peraturan perundang-undangan dengan pendekatan yang holistik ini untuk memastikan bahwa kedua kepentingan—perlindungan data pribadi nasabah dan hak masyarakat untuk mendapatkan informasi—dapat tercapai tanpa saling bertentangan. Hanya melibatkan dua aspek penting yaitu, perlindungan data pribadi dan transparansi informasi publik, keduanya harus dikelola dengan hati-hati untuk memastikan bahwa kepentingan individu dan masyarakat dapat berjalan beriiringan. Sesuai Pasal 40 ayat (1) UU No. 10 Tahun 1998 tentang Perbankan 'bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya

Bank juga harus mematuhi prinsip-prinsip yang ditetapkan dalam Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019). Dalam peraturan ini, bank wajib menerapkan kebijakan keamanan informasi berbasis risiko yang mencakup prosedur deteksi dini terhadap ancaman kebocoran data pribadi. Misalnya, sistem monitoring dan audit berkala dapat membantu mengidentifikasi potensi kerentanan sebelum terjadi insiden. Di samping itu, bank dapat memanfaatkan teknologi blockchain untuk meningkatkan keamanan data nasabah karena sifatnya yang transparan dan sulit diubah. Teknologi ini dapat menjadi solusi tambahan untuk memperkuat kepercayaan masyarakat terhadap perlindungan data pribadi[5].

Selain langkah-langkah teknis, penting bagi bank untuk membangun budaya keamanan informasi di antara seluruh karyawan. Sosialisasi dan pelatihan yang berkelanjutan perlu dilakukan untuk meningkatkan kesadaran akan pentingnya menjaga kerahasiaan data pribadi nasabah. Misalnya, karyawan harus memahami konsekuensi hukum yang diatur dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), terutama Pasal 32 yang mengatur tentang perlindungan data elektronik. Langkah ini dapat mencegah kebocoran data yang diakibatkan oleh human error, salah satu penyebab utama insiden keamanan informasi[6].

Bank juga harus memiliki mekanisme pengaduan yang mudah diakses oleh masyarakat jika terjadi pelanggaran perlindungan data pribadi. Layanan ini dapat berupa pusat layanan pelanggan atau platform online yang dirancang khusus untuk menerima keluhan terkait keamanan data. Sesuai dengan amanat Pasal 26 UU ITE, nasabah memiliki hak untuk mengajukan gugatan hukum apabila data pribadinya disalahgunakan. Dengan memberikan akses mudah untuk melaporkan insiden, bank dapat menunjukkan komitmen mereka terhadap akuntabilitas dan perlindungan hak nasabah.

Di sisi lain, bank harus memperhatikan bahwa tidak semua informasi dapat dirahasiakan sepenuhnya, terutama jika informasi tersebut menyangkut kebijakan publik. Sebagai contoh, Otoritas Jasa Keuangan (OJK) mengatur kewajiban transparansi melalui Peraturan OJK No. 32/POJK.03/2016 tentang Transparansi dan Publikasi Laporan Bank. Peraturan ini mewajibkan bank untuk menyampaikan laporan tahunan yang memuat kinerja keuangan, tata kelola, dan langkah-langkah manajemen risiko. Informasi ini dapat diakses oleh masyarakat

[5] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (*https://jdih.setneg.go.id/*).
[6] UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (*https://jdih.kominfo.go.id/*).

tanpa mengungkapkan data nasabah secara spesifik, sehingga tetap memenuhi prinsip perlindungan privasi[7].

Bank perlu bekerja sama dengan regulator, seperti OJK dan Bank Indonesia, untuk memastikan kebijakan dan prosedur mereka sejalan dengan regulasi yang berlaku. Kemitraan ini dapat mencakup audit berkala oleh pihak ketiga, penyusunan pedoman tata kelola data, dan adopsi standar internasional seperti ISO 27001 untuk manajemen keamanan informasi. Langkah-langkah ini akan memastikan bahwa perlindungan data pribadi nasabah berjalan seiring dengan keterbukaan informasi kepada masyarakat, sehingga menciptakan ekosistem perbankan yang aman, transparan, dan terpercaya.

1.2. Tantangan yang dihadapi Oleh Bank dalam Menjaga Kerahasiaan Nasabah dalam Menghadapi Perkembangan Teknologi dan Keamanan Siber

Dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, bank didefinisikan sebagai suatu badan usaha yang bertugas mengumpulkan dana dari masyarakat dalam bentuk simpanan, kemudian menyalurkannya kembali kepada masyarakat dalam bentuk kredit atau bentuk lainnya guna meningkatkan kesejahteraan masyarakat[8]. Kepercayaan nasabah terhadap bank akan terbangun kuat jika mereka merasa informasi pribadi dan keuangan mereka aman, menjaga kerahasiaan data nasabah juga merupakan bentuk komitmen bank terhadap integritas lembaga dan kepatuhan terhadap regulasi. Sebagai lembaga keuangan yang tunduk pada hukum, bank memiliki kewajiban untuk menjaga kerahasiaan data nasabah demi menjaga kepercayaan publik dan kelangsungan bisnisnya[9]. Pada Pasal 40 UU. 10/1998 tentang Perbankan menegaskan kewajiban bank untuk menjaga kerahasiaan data nasabah, termasuk informasi terkait simpanan dan aktivitas rekening. Ketentuan ini mengatur bahwa bank dilarang memberikan informasi mengenai nasabah kepada pihak ketiga kecuali dalam keadaan tertentu yang telah diatur dalam undang-undang. Pengecualian ini mencakup permintaan data oleh otoritas yang berwenang, seperti aparat penegak hukum atau pengadilan, untuk keperluan penegakan hukum. Prinsip ini bertujuan untuk melindungi privasi nasabah sekaligus menjaga kepercayaan masyarakat terhadap sistem perbankan. Pelanggaran terhadap pasal ini dapat dikenakan sanksi sesuai dengan ketentuan yang berlaku, menegaskan pentingnya kepatuhan bank terhadap aturan kerahasiaan data nasabah.[10]

Kemajuan dan perkembangan teknologi digital telah mendorong perubahan signifikan dalam perilaku dan gaya hidup masyarakat dalam menjaga data pribadinya. Sebagaimana konsekuensinya, penggunaan data pribadi menjadi suatu komoditas berharga dalam berbagai interaksi di dunia digital, penggunaan data yang tidak bertanggung jawab dapat menimbulkan berbagai risiko termasuk penyalahgunaan

---

[7] Peraturan Otoritas Jasa Keuangan No. 32/POJK.03/2016 tentang Transparansi dan Publikasi Laporan Bank (*https://www.ojk.go.id/*).

[8] Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

[9] Don Rade, Stefanus, Dhey W. Tadeus, and Gana Gana. 2021. "Kerahasiaan Bank Sebagai Bentuk Perlindungan Data Nasabah (Kasus Pada PT. Bank Cimb Niaga Tbk)". Jurnal Sosial Dan Sains 1 (8):892-909. https://doi.org/10.59188/jurnalsosains.v1i8.183.

[10] CRP, H. S. M. S. (2021). *Manajemen perbankan.* Gramedia Widiasarana Indonesia.

identitas dan pelanggaran privasi[11]. Hal ini juga menjadi tugas dan bagian penting bagi perbankan dalam menjaga data nasabahnya sebagai unsur kerahasiaan bank. Kewajiban bank dalam menjaga rahasia keterangan mengenai nasabahnya merupakan prinsip dasar dalam dunia perbankan yang sangat penting[12]. Meningkatnya ancaman siber menjadi tantangan signifikan bagi sektor perbankan. Sebagai tindakan untuk menanggulanginya, berbagai strategi keamanan siber yang komprehensif telah dan terus dikembangkan untuk melindungi kerahasiaan data nasabah. Keamanan siber pada sektor keuangan seperti perbankan memiliki perhatian utama untuk menanggulangi tindakan melawan hukum terhadap nasabahnya. Dampak risiko serangan siber terhadap perkembangan perbankan digital di Indonesia meliputi kerugian yang dapat diukur secara konkret dan langsung mempengaruhi operasional bank, yang dikenal sebagai kerugian langsung[13]. Kemajuan teknologi juga menciptakan tantangan baru berupa serangan siber yang semakin canggih, seperti phishing, malware, dan ransomware.

Menurut laporan yang diterbitkan oleh Bank Indonesia, serangan siber pada sektor keuangan telah meningkat dalam beberapa tahun terakhir, seiring dengan meningkatnya adopsi teknologi digital oleh masyarakat. Untuk menanggulangi ancaman ini, bank perlu mengimplementasikan sistem keamanan yang terintegrasi, termasuk pemantauan berbasis kecerdasan buatan dan enkripsi data tingkat lanjut. Langkah ini memungkinkan deteksi dan pencegahan serangan sebelum data nasabah terekspos atau disalahgunakan melalui Peraturan OJK No. 38/POJK.03/2016[14]. Penggunaan teknologi inovatif ini juga memerlukan investasi besar dan pelatihan intensif bagi staf untuk memastikan efektivitasnya. Keamanan siber memegang peranan penting dalam melindungi data dari ancaman serangan yang berpotensi merusak integritas dan kerahasiaannya, ketidakcukupan sistem keamanan dapat menyebabkan kebocoran data nasabah, yang tidak hanya merugikan pelanggan tetapi juga berisiko mencemarkan reputasi bank[15]. Keamanan siber memiliki peran yang sangat penting dalam melindungi data nasabah dari ancaman siber, terutama dalam industri perbankan yang bergantung pada kepercayaan dan integritas sistem informasi. Bank menyimpan sejumlah besar data sensitif, termasuk informasi pribadi, riwayat transaksi, dan data keuangan nasabah, yang menjadi sasaran empuk bagi pelaku kejahatan siber. Serangan seperti phishing, malware, ransomware, dan pencurian identitas dapat mengakibatkan kebocoran data nasabah, yang tidak hanya merugikan individu secara finansial tetapi juga berpotensi menurunkan kepercayaan masyarakat terhadap lembaga keuangan tersebut. Selain itu, pelanggaran keamanan

[11] Suari, Kadek Rima Anggen, and I. Made Sarjana. "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia." Jurnal Analisis Hukum 6, no. 1 (2023): 132-142.
[12] Pasal 40 Undang-Undang Nomor 10 Tahun 1998
[13] Satrya, Ilham Zharfan. "Serangan Siber dalam Perkembangan Perbankan Digital di Indonesia." Journal-article. Syntax Literate. Vol. 9–9, October 2024. http://dx.doi.org/10.36418/syntax-literate.v9i10.
[14] Bank Indonesia. (2021). *The state of cybersecurity in Indonesia*. Digital Indonesia. De Gruyter.
[15] Vebrianty, Annisa. "PERLINDUNGAN HUKUM PEMBUKAAN REKENING SECARA ONLINE DALAM LAYANAN PERBANKAN DIGITAL PADA PT BANK CENTRAL ASIA Tbk." Bachelor's thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, 2021.

siber dapat menyebabkan kerugian finansial yang signifikan bagi bank akibat denda regulasi, tuntutan hukum, dan biaya pemulihan sistem. Dalam konteks regulasi, bank diwajibkan mematuhi berbagai undang-undang, seperti Pasal 40 UU No. 10 Tahun 1998, yang mengatur kewajiban bank menjaga kerahasiaan data nasabah. Ketidakpatuhan terhadap regulasi ini dapat memicu sanksi hukum sekaligus mencoreng reputasi institusi.[16] Oleh karena itu, penerapan teknologi keamanan mutakhir seperti enkripsi data, autentikasi multifaktor, serta deteksi ancaman berbasis kecerdasan buatan menjadi langkah strategis yang tidak hanya melindungi data nasabah tetapi juga menjaga keberlanjutan operasional dan kepercayaan publik terhadap lembaga perbankan.

Pemerintah bertanggung jawab untuk membangun sistem keamanan siber yang mampu menyediakan perlindungan data yang aman sekaligus mendukung prinsip demokrasi bagi seluruh warga negara Indonesia[17]. Mekanisme perlindungan data nasabah oleh perbankan pada aspek hukum dan kepatuhan diwujudkan melalui implementasi regulasi yang ketat serta pengawasan berkelanjutan oleh otoritas terkait. Bank wajib mematuhi Pasal 40 UU No. 10 Tahun 1998, yang mewajibkan kerahasiaan data nasabah, dan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengatur prinsip-prinsip pengelolaan data, termasuk persetujuan nasabah dalam pengumpulan, penyimpanan, dan pengelolaan data mereka. Selain itu, peraturan OJK, seperti POJK No. 38/POJK.03/2016 tentang Manajemen Risiko dalam Penggunaan Teknologi Informasi, mewajibkan bank untuk menerapkan kebijakan mitigasi risiko teknologi informasi, termasuk pengamanan data nasabah. Penjahat siber cenderung memanfaatkan kelemahan dalam sistem untuk meretasnya dengan mudah dan melakukan manipulasi terhadap data atau laporan yang ada[18]. Bank juga diwajibkan melakukan audit internal dan eksternal secara berkala untuk memastikan kepatuhan terhadap standar keamanan dan mengidentifikasi potensi pelanggaran. Kerja sama dengan pihak ketiga diatur melalui kontrak yang mencakup klausul kerahasiaan data dan audit keamanan. Untuk memastikan kepatuhan ini, regulator seperti OJK dan Bank Indonesia melakukan pengawasan rutin, termasuk inspeksi lapangan dan sanksi administratif terhadap pelanggaran. Langkah-langkah ini memastikan bahwa data nasabah dilindungi sesuai standar hukum yang berlaku.

Selain serangan siber, tantangan lain yang dihadapi bank adalah risiko kebocoran data akibat kesalahan manusia (human error). Berdasarkan data yang dirilis oleh Badan Siber dan Sandi Negara (BSSN), sebagian besar insiden kebocoran data disebabkan oleh kelalaian karyawan dalam menangani informasi sensitif (BSSN,

[16] Jan, T. S. (2022). *Kerahasiaan Bank dan Perpajakan*. Penerbit Alumni.
[17] Aji, Muhammad Prakoso. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]." Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional 13, no. 2 (January 4, 2023): 222–38. https://doi.org/10.22212/jp.v13i2.3299.
[18] Silalahi, Putri Hasian, Fiorella Angella Dameria, and Fiorella Angella Dameria. "Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional." Wajah Hukum 7, no. 2 (November 1, 2023): 614. https://doi.org/10.33087/wjh.v7i2.1244.

2022). Untuk mengurangi risiko ini, bank dapat menyusun pedoman tata kelola data yang ketat dan mengadakan pelatihan rutin tentang keamanan informasi. Penerapan mekanisme seperti autentikasi dua faktor (2FA) untuk akses internal dapat menjadi langkah penting dalam mencegah kebocoran data akibat akses yang tidak sah (PP No. 71 Tahun 2019, Pasal 22).[19]

Di sisi lain, regulasi internasional seperti General Data Protection Regulation (GDPR) telah mempengaruhi standar perlindungan data di Indonesia. Peraturan ini mendorong bank untuk mengadopsi prinsip perlindungan data yang lebih ketat, seperti transparansi dalam pengelolaan data nasabah dan hak untuk dilupakan (right to be forgotten). Di Indonesia, prinsip ini diakomodasi dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP, 2022). Bank harus mematuhi aturan ini dengan menetapkan kebijakan yang memastikan nasabah dapat mengelola persetujuan mereka atas penggunaan data pribadi. Kebijakan ini juga mencakup pemberitahuan kepada nasabah jika terjadi pelanggaran data, sehingga dapat meminimalkan dampaknya.

Kolaborasi antara bank dengan otoritas terkait, seperti OJK dan BSSN, juga menjadi aspek penting dalam menghadapi tantangan keamanan data. Melalui inisiatif seperti Financial Services Cybersecurity Framework yang dikeluarkan oleh OJK, bank dapat mengadopsi pendekatan berbasis risiko dalam mengelola keamanan siber (OJK, 2022). Kolaborasi ini mencakup berbagi informasi tentang ancaman terbaru, audit keamanan berkala, dan uji penetrasi untuk mengevaluasi kerentanan sistem. Langkah ini memungkinkan bank untuk merespons serangan siber secara proaktif dan terkoordinasi.

Terakhir, dalam era transformasi digital, edukasi masyarakat juga menjadi kunci untuk melindungi data pribadi nasabah. Bank dapat menyelenggarakan kampanye literasi digital yang bertujuan untuk meningkatkan kesadaran masyarakat tentang pentingnya menjaga keamanan data pribadi, seperti tidak membagikan informasi sensitif kepada pihak ketiga yang tidak terpercaya (Bank Indonesia, 2022)[20]. Edukasi ini juga dapat mencakup panduan untuk mengidentifikasi upaya phishing atau serangan sosial lainnya yang sering menjadi pintu masuk bagi penjahat siber. Dengan pendekatan ini, bank tidak hanya melindungi nasabah tetapi juga membangun hubungan yang lebih kuat dengan masyarakat.

KESIMPULAN

Bank memiliki tanggung jawab penting untuk menjaga keseimbangan antara kerahasiaan data pribadi nasabah dan pemenuhan hak masyarakat atas informasi sesuai dengan peraturan perundang-undangan. Dalam menghadapi perkembangan teknologi dan ancaman keamanan siber yang semakin kompleks, bank perlu menerapkan langkah-langkah komprehensif, termasuk teknologi keamanan canggih, kebijakan tata kelola data yang ketat, dan kolaborasi dengan regulator. Pelatihan staf, sosialisasi kepada nasabah, dan penerapan regulasi nasional maupun

[19] Badan Siber dan Sandi Negara (BSSN). (2022). *Laporan Kebocoran Data di Indonesia*. Jakarta: BSSN.
[20] Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko pada Sistem Informasi Bank. Otoritas Jasa Keuangan.

standar internasional seperti GDPR menjadi elemen kunci dalam menciptakan ekosistem perbankan yang aman dan transparan. Selain itu, bank harus menjaga kepercayaan masyarakat dengan menyediakan akses informasi publik yang tidak mengorbankan privasi individu. Pendekatan holistik ini memastikan bahwa prinsip kerahasiaan data dan keterbukaan informasi dapat berjalan seiring, mendukung keberlanjutan operasional perbankan serta kepercayaan masyarakat terhadap lembaga keuangan.

DAFTAR PUSTAKA

Artikel Jurnal

Aji, M. P. (2023). "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective. *Jurnal Politika Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional 13*, 222-38.

Don Rade, S. D. (2021). "Kerahasiaan Bank Sebagai Bentuk Perlindungan Data Nasabah (Kasus Pada PT. Bank Cimb Niaga Tbk)". *Jurnal Sosial Dan Sains*, 1 (8):892-909.".

Hendri, H. S. (2023). Kepastian Dan Perlindungan Hukum Terhadap Data Pribadi Pengguna Fintech Peer To Peer Lending. *Jurnal Ilmiah Universitas Batanghari Jambi*, 23(1), 848-854.

Merta, M. &. (2021). Pertanggungjawaban Bank Atas Pelanggaran Kerahasiaan Data Pribadi Milik Nasabah Yang Dilakukan Pegawai Bank Berdasarkan Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. *Jurnal Hukum Adigama*, 4(1), 842-844.

Satrya, I. Z. (2024). Serangan Siber dalam Perkembangan Perbankan Digital di Indonesia. *Journal-article. Syntax Literate.* , 9-9.

Silalahi, P. H. (2023). "Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional. *Wajah Hukum 7*, 614. .

Simbolon, N. R. (2023). PENEGAKAN HUKUM TERHADAP PENYALAHGUNAAN DATA NASABAH BANK DI ERA KETERBUKAAN INFORMASI. *Jurnal Darma Agung*, 31(6), 49-62.

Suari, K. R. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum 6, no. 1* , 132-142.".

Vebrianty, A. (2021). "PERLINDUNGAN HUKUM PEMBUKAAN REKENING SECARA ONLINE DALAM LAYANAN PERBANKAN DIGITAL PADA PT BANK CENTRAL ASIA Tbk. *Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta,*, 67-69.

Undang – Undang

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Elektronik. (n.d.). UU No. 11 Tahun 2008 tentang Informasi dan Transaksi.

Pemerintah, P. (n.d.). No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Disertasi/Tesis/Paper Kerja

Haprabu, P. S. (2023). PENERAPAN ASAS KEPASTIAN HUKUM PENYELESAIAN KERUGIAN NASABAH BANK DALAM PENGGUNAAN UANG ELEKTRONIK (BRIZZI) . *Doctoral dissertation, FAKULTAS HUKUM UNIVERSITAS PASUNDAN).*, 65-69.

Vebrianty, A. (2021). PERLINDUNGAN HUKUM PEMBUKAAN REKENING SECARA ONLINE DALAM LAYANAN PERBANKAN DIGITAL PADA PT BANK CENTRAL ASIA Tbk." . *Bachelor's thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta,*, 57-60.

Buku Teks

CRP, H. S. (2021). *Manajemen perbankan.* Gramedia Widiasarana Indonesia.

Indonesia., B. (2021). *The state of cybersecurity in Indonesia.* . Digital Indonesia. De Gruyter.

Jan, T. S. (2022). *Kerahasiaan Bank dan Perpajakan.* Penerbit Alumni.

Laporan Instansi/Lembaga/Organisasi/Perusahaan

Bank. (2021). *Peraturan Otoritas Jasa Keuangan No. 32/POJK.03/2016 tentang Transparansi dan Publikasi Laporan.*

BSSN. (2022). *Laporan Kebocoran Data di Indonesia.* Jakarta: BSSN.

OJK. (2022). *Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko pada Sistem Informasi Bank. Otoritas Jasa Keuangan.* Otoritas Jasa Keuangan.