

ANALISIS SANKSI PIDANA TERHADAP PEGAWAI BANK YANG DENGAN SENGAJA MEMBOCORKAN DATA REKENING NASABAH DI INDONESIA

Jesica Yuliana Silaen ¹, Sidi Ahyar Wiraguna ²
Fakultas Hukum, Hukum, Universitas Esa Unggul

Correspondence		
Email: jesikayuliana05@gmail.com	No. Telp:	
Submitted 25 Mei 2025	Accepted 28 Mei 2025	Published 29 Mei 2025

ABSTRACT

In this digitalization era, the personal data is something that must be made by all humans, no exeception also for Indonesia people the submission of personal data such as ID cards, email addresses and so on to certain parties to be accessed, allows humans to live an easily, effectively and efficiently life. However, the level of crime that takes advantage of the convenience inthe increasingly high digitalization era has forced the country to immediately make rules that regulate, both regulations and sanctions for anyone who unlawfully uses other people’s personal data for profit, which makes Indonesia citizens can live a good life and get legal guarantees regarding the confidentiality of their personal data.

Keywords: Confidential, data Protection.

ABSTRAK

Di era digitalisasi ini, data pribadi merupakan suatu hal yang wajib dimiliki oleh seluruh manusia, tidak terkecuali bagi masyarakat Indonesia penyampaian data pribadi seperti KTP, alamat email dan lain sebagainya kepada pihak-pihak tertentu untuk dapat diakses, memungkinkan manusia untuk menjalani kehidupan dengan mudah, efektif dan efisien. Namun, tingkat kejahatan yang memanfaatkan kemudahan di era digitalisasi yang semakin tinggi ini telah memaksa negara untuk segera membuat peraturan yang mengatur, baik peraturan perundang-undangan maupun sanksi bagi siapa saja yang secara melawan hukum menggunakan data pribadi orang lain untuk mendapatkan keuntungan, yang membuat warga negara Indonesia dapat hidup dengan baik dan mendapatkan jaminan hukum mengenai kerahasiaan data pribadinya.

Kata Kunci: Rahasia, Perlindungan Data.

1. Pendahuluan

A. Latar Belakang

Perlindungan kepada nasabah bank terhadap kebocoran data menjadi semakin krusial seiring dengan pesatnya perkembangan teknologi digital. Dalam era digital ini, bank menghadapi banyak tantangan-tantangan yang besar untuk menjaga data pribadi nasabah (Shafa Salsabila, 2025). Salah satunya digital banking, digital banking menawarkan kemudahan dan aksesibilitas, tetapi tidak menutup kemungkinan bisa mengalami kebocoran data. Adanya kebocoran data dapat berakibat fatal, tidak hanya bagi individu, tetapi juga bagi reputasi lembaga perbankan itu sendiri. Oleh karena itu, bank perlu menerapkan berbagai langkah proaktif untuk melindungi informasi sensitif yang dimiliki. Regulasi dan kebijakan yang ketat harus diterapkan untuk memberikan kerangka hukum yang jelas dalam pengelolaan data nasabah. Semua ini bertujuan untuk menciptakan kepercayaan di kalangan nasabah dan menjaga integritas sistem perbankan. Isu kebocoran data telah menjadi perhatian utama di seluruh dunia, termasuk Indonesia (Khetrina Maria Angnesia, 2025). Dalam beberapa tahun terakhir, sejumlah kasus kebocoran data di sektor perbankan telah mengungkapkan betapa rentannya informasi pribadi nasabah. Kebocoran ini sering kali disebabkan oleh serangan siber, kurangnya keamanan sistem, atau bahkan kelalaian dari pihak internal bank. Ketika data sensitif seperti nomor rekening, password, dan informasi pribadi lainnya bocor, dampaknya bisa sangat merugikan bagi nasabah (Berto Purnomo Sidik, 2025). Kerugian finansial, pencurian identitas, dan penurunan kepercayaan terhadap lembaga keuangan adalah beberapa konsekuensi yang sering terjadi. Selain itu, lembaga perbankan yang mengalami kebocoran data juga berisiko menghadapi sanksi dari regulator dan kerugian reputasi yang sulit

dipulihkan. Ini menggarisbawahi pentingnya perlindungan data yang efektif dan berkelanjutan. (Anwar, 2020)

Salah satu contoh nyata dari isu kebocoran data di sektor perbankan adalah kasus yang melibatkan Bank Syariah Indonesia (BSI). Pada tanggal 8 Mei 2023, seluruh layanan BSI terhenti akibat serangan siber, yang membuat nasabah tidak dapat melakukan transaksi apapun. Penutupan layanan ini berdampak luas, termasuk pada jaringan ATM, mobile banking, dan kantor cabang. Setelah penyelidikan, terungkap bahwa insiden tersebut berkaitan dengan serangan dari kelompok hacker LockBit 3.0. Mereka berhasil mengakses dan mengenkripsi data nasabah, sehingga menyebabkan kebocoran informasi sensitif. Banyak nasabah mengeluh kehilangan dana dan merasa terancam akibat kebocoran data ini. Kasus ini menyadarkan betapa pentingnya tindakan pencegahan dan respons cepat dalam menghadapi ancaman siber. Menurut Alfons, peretasan ini kemungkinan dilakukan lebih awal, yakni saat libur Idul Fitri. Alfons mengatakan insiden itu mungkin terjadi sebelum tanggal 8 Mei 2023, karena disaat itu data-data dari pelanggan BSI sudah berhasil disalin dan dienkripsi. Kebocoran data ini menimbulkan kerugian terhadap nasabah selain kebocoran data nasabah juga kehilangan dananya (Muryani Verina Dwi, 2025). Saya memilih kasus ini untuk menelusuri lebih dalam mengenai perlindungan hukum bagi nasabah ketika terjadi kebocoran data, serta untuk mengeksplorasi upaya bank dalam menjaga kerahasiaan data nasabah. (Alfons, 8 Mei 2023).

RUMUSAN MASALAH

1. Bagaimana penerapan sanksi pidana terhadap pegawai bank yang secara sengaja dan melawan hukum membocorkan data rekening Nasabah di Indonesia?
2. Apa saja jenis pelanggaran yang dilakukan oleh pegawai bank dalam kebocoran data rekening nasabah menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)?
3. Bagaimana efektivitas sanksi pidana yang diatur dalam UU PDP dalam mencegah kebocoran data rekening nasabah oleh pegawai bank?

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini berbasis pada teknik studi kepustakaan (literature review) yang merupakan sumber sekunder dengan menggunakan pendekatan yuridis empiris. Undang undang yang dijadikan sumber utama dalam penelitian ini adalah Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan sebagaimana telah diubah dengan 10 Tahun 1998, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik (ITE) Nomor 11 Tahun 2008 sebagaimana telah diubah dalam Undang-Undang Nomor 19 Tahun 2016. Perubahan peraturan perundang-undangan sebagai berikut: Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016, POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, Peraturan Pemerintah No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Selain itu, sumber-sumber sekunder dalam penelitian ini memuat referensi dan/atau rujukan seperti buku-buku, artikel, jurnal serta media lain yang berkaitan dengan batasan-batasan ruang lingkup Hukum Perbankan di Indonesia. Berdasarkan sumber dari bahan materi tersebut akan dianalisis dengan pengolahan metode kualitatif. (Papendang, 2016)

HASIL DAN PEMBAHASAN

Konsep regulasi dan/atau peraturan terkait peninjauan kegiatan Bank diatur dalam perundang undangan Indonesia Hubungan hukum antara bank dan konsumen tidak secara khusus diatur oleh ketentuan dalam UU Perbankan. Hubungan ini lebih dari sekedar hubungan kreditur-debitur, melainkan hubungan yang dibangun atas dasar kepercayaan (Mugiono Mugiono, 2025). Sesuai dengan UU Perbankan, hubungan hukum antara bank dan nasabah

penyimpanan dana memiliki ciri-ciri khusus dan termasuk ke dalam perjanjian tidak bernama karena tidak dapat disebut sebagai perjanjian penitipan, perjanjian pemberian kuasa, atau bahkan perjanjian pinjam-meminjam uang. Secara teoritis, bank mengelola dana konsumen dan menyalurkannya kepada konsumen yang menunggak, menjalankan peran sebagai perantara. “Hubungan antara bank dan nasabah didasarkan pada hubungan kepercayaan,” demikian penjelasan Pasal 29 ayat (3) dan (4) UU Perbankan. Hubungan kehati-hatian dan hubungan rahasia adalah dua bagian dari hubungan kepercayaan ini. Hubungan hukum antara bank dengan nasabahnya didasarkan pada suatu perjanjian, yang bahkan dapat dikatakan sebagai perjanjian baku yang dibuat secara sepihak oleh bank, sebagaimana dinyatakan dalam Pasal 1 angka 6, 7, 8, 9, dan 14 UU Perbankan. Selama tidak melanggar hukum, ketertiban umum, atau kesusilaan, KUH Perdata memberikan fleksibilitas yang tinggi kepada masyarakat untuk menyepakati apa yang mereka inginkan. Perjanjian yang memenuhi asas-asas dan syarat-syarat sahnya perjanjian mengikat hubungan hukum antara bank dengan nasabahnya. Perjanjian nasabah-bank tampaknya melanggar persyaratan keabsahan perjanjian, khususnya asas kesepakatan, jika dilihat dari sudut pandang praktik perbankan. Meskipun demikian, hal ini dapat ditafsirkan sebagai perjanjian jika terbukti bahwa kedua belah pihak menerima perjanjian tersebut melalui tanda tangan. Dengan demikian, nasabah dan bank memiliki perjanjian yang sah.

Kewajiban Bank

Selanjutnya terkait kewajiban bank sebagai pelaku usaha, selain mengelola dana nasabah dengan baik, juga ditentukan dalam Pasal 7 Undang-Undang Perlindungan Konsumen, sebagai berikut: a. Beritikad baik dalam melakukan kegiatan usahanya, b. Memberikan kondisi dan jaminan barang dan atau jasa serta memberi penjelasan penggunaan, perbaikan dan pemeliharaan, c. Memperlakukan atau melayani konsumen secara benar dan jujur serta tidak diskriminatif, d. Menjamin mutu barang dan atau jasa yang diproduksi dan atau diperdagangkan ketentuan standar mutu barang dan atau jasa yang berlaku, e. Memberi kesempatan kepada konsumen untuk menguji dan atau mencoba barang dan atau jasa tertentu serta memberi jaminan dan atau garansi atas barang yang dibuat dan atau jasa yang diperdagangkan, f. Memberi kompensasi, ganti rugi dan atau penggantian atas kerugian akibat penggunaan, pemakaian dan pemanfaatan barang dan atau jasa yang diperdagangkan, g. Memberi kompensasi, ganti rugi dan atau penggantian apabila barang dan atau jasa yang diterima atau dimanfaatkan tidak sesuai dengan perjanjian. (Nurhayati, 2020, November, pp. 50-56)

Rahasia Dagang Bank

Menurut Pasal 1 angka 28 Undang-undang Nomor 10 Tahun 1998 Tentang Perbankan, yang dimaksud dengan rahasia Bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai menyatakan bahwa Rahasia Dagang adalah segala sesuatu yang berhubungan dengan keuangan dan hal-hal lain dari nasabah bank yang menurut kelaziman dunia perbankan wajib dirahasiakan. Selain itu ketentuan dalam Pasal 40 ayat 1 Undang-Undang Nomor 7 Tahun 1992 yang telah diubah oleh Undang-Undang no 10 Tahun 1998 Tentang Perbankan, selanjutnya disebut dengan UU Perbankan, menyatakan bahwa Bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41 A, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44 A.

Sementara itu Penjelasan atas Pasal 40 ayat 1 UU Perbankan menguraikan bahwa apabila nasabah bank adalah nasabah penyimpan yang sekaligus juga sebagai nasabah debitur, bank wajib tetap merahasiakan keterangan tentang nasabah dalam kedudukannya sebagai nasabah penyimpan. Keterangan mengenai nasabah selain sebagai nasabah penyimpan, bukan merupakan keterangan yang wajib dirahasiakan bank.

Berdasarkan pasal yang terkait dengan rahasia bank dalam UU Perbankan tersebut diatas, maka dapat disimpulkan bahwa ruang lingkup rahasia bank terbatas hanya terhadap identitas nasabah penyimpan di samping keadaan simpanan nasabah penyimpan yang bersangkutan. Adapun ruang lingkup dari rahasia bank, antara lain: 1. Menyangkut keterangan mengenai nasabah penyimpan dan simpanannya. Ini berarti tidak termasuk keterangan mengenai nasabah debitur dan pinjamannya; dan 2. Situasi tertentu dalam mana informasi mengenai nasabah penyimpan beserta dengan simpanannya dibolehkan, dimungkinkan atau dibenarkan saja diberikan oleh pihak yang terkena larangan jika informasi tersebut tergolong pada informasi yang dikecualikan atau informasi nasabah penyimpan dan simpanannya tidak termasuk dalam kualifikasi kerahasiaan bank.

Merujuk pada Pasal 47 ayat (2) UU Perbankan menyatakan bahwa pihak-pihak yang berkewajiban untuk merahasiakan keadaan keuangan nasabah penyimpan dan simpanannya, yaitu: 1. Anggota Dewan Komisaris Bank; 2. Direksi Bank; 3. Pegawai Bank; dan 4. Pihak Terafiliasi lainnya dari Bank.

Penjelasan Pasal 47 ayat 2 menyatakan bahwa yang dimaksud dengan pegawai bank adalah semua pejabat dan karyawan bank. Sehingga semua pegawai bank dapat termasuk dalam pernyataan ini, walaupun pegawai bank tersebut tidak memiliki akses sama sekali terhadap atau tidak mempunyai hubungan sama sekali dengan nasabah penyimpan dan simpanannya. (Sjahdeni, 2006)

Etika Bank dalam Menjaga Data Nasabah

Ketentuan pelaksanaan dari rahasia bank dalam Undang-Undang Perbankan, untuk melindungi kerahasiaan dan keamanan data pribadi nasabah Lembaga Otoritas Jasa Keuangan menerbitkan Peraturan Otoritas Jasa Keuangan (POJK) Nomor 1/ POJK.07/2013 Tahun 2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan.

Peraturan POJK ini, dalam Pasal 31 ayat (1) dan (2) ditentukan bahwa pelaku usaha jasa keuangan dilarang dengan cara apapun memberikan data dan/atau informasi mengenai konsumennya kepada pihak ketiga. Larangan tersebut dikecualikan dalam hal: 1. Konsumen memberikan persetujuan tertulis; dan/atau 2. Diwajibkan oleh peraturan perundang-undangan.

Pembocoran data nasabah oleh pegawai bank merupakan pelanggaran terhadap rahasia bank. Pelanggaran terhadap rahasia bank tersebut meskipun dilakukan oleh pegawai bank, tetapi juga dapat dipertanggungjawabkan kepada bank sebagai pihak yang berkewajiban untuk menjaga kerahasiaan data nasabah. Bank sebagai pelaku jasa keuangan dapat dikenai sanksi dalam Pasal 53 POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Sanksi yang dapat diberikan terhadap bank sebagai pelaku jasa keuangan yang melanggar ketentuan dalam Peraturan Otoritas Jasa Keuangan tersebut dikenakan sanksi administratif antara lain berupa: a. Peringatan tertulis; b. Denda yaitu kewajiban untuk membayar sejumlah uang tertentu; c. Pembatasan kegiatan usaha; d. Pembekuan kegiatan usaha; dan e. Pencabutan izin kegiatan usaha.

Pegawai bank yang membocorkan data pribadi nasabah kepada pihak ketiga yang tidak berkepentingan tanpa persetujuan tertulis dari pihak nasabah adalah pelanggaran terhadap rahasia bank. Dalam ilmu hukum dikenal konsep kewajiban hukum yang berkaitan tanggung jawab hukum yakni seseorang dikatakan secara hukum bertanggung jawab untuk suatu perbuatan tertentu adalah bahwa dia dapat dikenakan suatu sanksi dalam kasus perbuatan yang berlawanan.

Perwujudan bank melindungi data nasabah dilaksanakan dengan merahasiakan seluruh informasi mengenai klien, tidak menggunakan tanpa persetujuan, melakukan penyimpanan, mengenkripsikan serta menciptakan sistem otentikasi dan bertindak lanjut jika terdapat pengaduan dari klien. Keseluruhan informasi di dalam Bank sangat rentan terhadap serangan siber yang tentunya merugikan berbagai pihak dari nasabah. (Munir, 2003, p. 88)

Analisis Kasus kebocoran data di sektor perbankan yang melibatkan Bank Syariah Indonesia (BSI)

Kasus ini bermula dari adanya kesalahan sistem yang mengakibatkan baik nasabah maupun kantor cabang tidak dapat melakukan transaksi melalui ATM maupun BSI Mobile. pada tanggal 8 Mei 2023, lewat akun instagram Pihak BSI mengumumkan adanya kendala dan gangguan pada sistem perbankan BSI karena sedang adanya pemeliharaan sistem berupa perbaikan dan migrasi sistem namun gangguan ini terus terjadi selama sehari-hari.

Pada tanggal 10 Mei 2023, Menteri BUMN Erick Thohir mengajukan pertanyaan mengenai potensi serangan siber yang mungkin terjadi. Satu hari setelahnya, pihak Bank Syariah Indonesia (BSI) mengadakan konferensi pers, di mana mereka mengonfirmasi adanya serangan siber yang mengakibatkan gangguan pada layanan perbankan mereka. Meskipun layanan BSI berhasil pulih pada hari yang sama, pihak bank belum memberikan penjelasan mengenai jenis serangan siber yang dialami, karena masih memerlukan proses audit dan forensik digital untuk memperoleh bukti yang lebih jelas.

Pada 12 Mei 2023, Beredar sebuah klaim mengenai adanya gangguan pada layanan BSI terjadi karena adanya aktivitas dari peretas. Kelompok peretas yang dikenal dengan nama LockBit mengklaim bahwa mereka telah berhasil menyerang sistem BSI menggunakan ransomware LockBit 3.0. Informasi mengenai klaim ini pertama kali disampaikan kepada publik melalui akun Twitter @darktracer_int pada 13 Mei 2023. Menurut data yang diklaim, Data sensitif baik milik nasabah maupun perusahaan yang telah dicuri berukuran 1.5TB (terabyte) dari 9 pusat data (database) yang berisikan 15 juta data nasabah dan karyawan, data sensitif yang dimaksud diantaranya: 1. Nomor Telepon, 2. Alamat Lengkap, 3. Nama Lengkap, 4. Rincian dokumen, 5. Informasi Saldo bank, nomor kartu riwayat transaksi, serta dokumen-dokumen finansial, 6. Surat hukum, dan perjanjian kerahasiaan (NDA). 7. Data kata sandi untuk semua layanan internal dan eksternal yang digunakan oleh bank.

Peretas juga mengancam akan membocorkan data nasabah dengan memberikan waktu 72Jam untuk menghubunginya sebagai jalan penyelesaian masalah namun tidak ada respon yang diberikan sehingga pada tanggal 16 Mei pada pukul 7 pagi peretas membocorkan data yang telah dicuri di situs dark web karena tidak mencapai kesepakatan yang ditawarkan. Peretas meminta BSI membayar tebusan sebesar 20 juta Dolar AS (Rp 296.4 Miliar) kemudian ditawarkan dengan nominal 100 Ribu dan 10 Juta dollar AS namun keduanya ditolak oleh peretas. (Sudarmanto, 2021)

Analisis Hukum

Dalam kasus ini terdapat beberapa pelanggaran yang dilakukan oleh bank BSI dan dapat dibedakan dengan dilihat berdasarkan Undang Undang yang relevan.

a. UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Berdasarkan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi pada pasal 57 ayat 1 menjelaskan terkait dengan pelanggaran yang dapat dikenakan sanksi, dan dalam kasus ini pelanggaran pada pasal 20. Pada pasal 20 ayat 2 dijelaskan beberapa ketentuan dasar yang menjadi dasar dalam melakukan pemrosesan data pribadi dan dalam kasus ini pihak bank BSI tidak berhasil memenuhi hal tersebut dengan bocornya data pribadi nasabah yang merupakan hak subjek data pribadi, hal ini diperjelas dengan pasal 4 ayat 2 huruf yang menegaskan bahwa data keuangan pribadi merupakan data spesifik yang melekat kepada subjek data dalam hal ini adalah nasabah. Dampak dari tidak dipenuhinya kewajiban ini dijelaskan pada pasal 57 ayat 1, 2 dan 3 yang masing masing menjelaskan tentang pelanggaran pasal, sanksi administratif dan denda administratif yang dapat dijatuhkan

b. UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Berdasarkan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pada pasal 30 ayat 1, 2, dan 3 menjelaskan terkait dengan adanya kesenjangan seseorang dan tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik untuk

mendapatkan informasi. Dalam hal ini peretas berhasil masuk kedalam sistem elektronik bank BSI dengan cara menyusupkan malware LockBit 3.0. Dan ini berhasil melampaui sistem keamanan bank BSI dengan cara menerobos dan menjebol sistem keamanan yang ada. Menurut pasal 46 ayat 1,2 dan 3. Ketentuan pidana yang dapat diberikan adalah penjara paling lama 6 sampai 8 tahun dan denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah) sampai Rp800.000.000,00 (delapan ratus juta rupiah). Pada pasal 32 ayat 1, 2 dan 3 menjelaskan terkait dengan adanya pengubahan atau perpindahan data secara melawan hukum dari/oleh orang yang tidak berhak melakukan perpindahan. Dalam kasus ini sebanyak 15 juta datanasabah berhasil dipindahkan dari 9 pusat data dan kemudian digunakan tidak sebagaimana mestinya dalam kasus ini dijual kepada publik lewat situs dark web seharga 20 juta Dolar AS. Menurut pasal 48 ayat 1,2 dan 3. Ketentuan pidana yang dapat diberikan adalah penjara paling lama 8 sampai 10 tahun dan denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah) sampai Rp5.000.000.000,00 (lima miliar rupiah).

Pada pasal 33 menjelaskan terkait dengan adanya gangguan dalam sistem elektronik yang menyebabkan tidak dapat bekerja sebagaimana mestinya. Dalam kasus ini adanya serangan yang terjadi menyebabkan layanan BSI mulai dari perbankan sampai bank online terganggu selama beberapa hari. menurut pasal 49 ketentuan pidana yang dapat diberikan adalah penjara paling lama 10 tahun dan denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah) Pada pasal 33 menjelaskan terkait dengan adanya gangguan dalam sistem elektronik yang menyebabkan tidak dapat bekerja sebagaimana mestinya. Dalam kasus ini adanya serangan yang terjadi menyebabkan layanan BSI mulai dari perbankan sampai bank online terganggu selama beberapa hari. menurut pasal 49 ketentuan pidana yang dapat diberikan adalah penjara paling lama 10 tahun dan denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah). (undang-undang, 2008)

Ruang Lingkup Tanggung Jawab Hukum Bank

Bank memiliki kewajiban hukum untuk melindungi keamanan dan kerahasiaan data nasabah. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan memberikan perlindungan terhadap dana nasabah, tetapi perlindungan terhadap data nasabah masih memerlukan perhatian yang lebih mendalam.¹ Berikut adalah penjelasan mengenai tiga aspek utama tersebut: tanggung jawab administratif, perdata, dan pidana.

a. Tanggung Jawab Administratif

Tanggung jawab administratif diatur oleh Otoritas Jasa Keuangan (OJK) melalui Peraturan OJK No. 38/POJK.03/2016 mengenai Manajemen Risiko Teknologi Informasi.² Peraturan ini mengharuskan bank untuk menerapkan kebijakan keamanan informasi yang ketat dan melakukan pengawasan terhadap sistem pengelolaan data nasabah. Apabila terjadi kebocoran data akibat kelalaian dalam pengelolaan sistem keamanan informasi, OJK berhak memberikan sanksi administratif kepada bank, yang dapat berupa denda, teguran tertulis, atau pembatasan kegiatan usaha.

b. Tanggung Jawab Perdata

Tanggung jawab perdata adalah tanggung jawab hukum yang muncul akibat perbuatan melawan hukum (onrechtmatige daad) yang diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPperdata).³ Pasal ini menyatakan bahwa "setiap tindakan melawan hukum yang mengakibatkan kerugian bagi orang lain, mengharuskan pihak yang menyebabkan kerugian tersebut untuk memberikan ganti rugi." Dalam konteks kebocoran data nasabah, jika bank terbukti lalai dalam menjaga kerahasiaan dan keamanan data nasabah sehingga mengakibatkan kerugian bagi nasabah, maka nasabah dapat mengajukan gugatan perdata terhadap bank. Contoh kasus yang sering terjadi adalah ketika data nasabah bocor dan digunakan untuk kegiatan penipuan atau penyalahgunaan informasi, nasabah yang dirugikan dapat menuntut bank untuk memberikan ganti rugi atas kerugian materiil dan imateriil yang

diderita. Kerugian materiil meliputi kehilangan dana atau akses yang tidak sah ke rekening nasabah, sedangkan kerugian imateriil dapat berupa gangguan privasi dan rasa aman nasabah.

c. Tanggung Jawab Pidana

Selain tanggung jawab perdata, bank juga dapat menghadapi tanggung jawab pidana jika terbukti melanggar hukum yang berkaitan dengan perlindungan data nasabah. Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), terdapat sanksi pidana bagi individu atau pihak yang dengan sengaja atau karena kelalaian membocorkan data pribadi tanpa izin.⁴ Pasal 65 UU PDP mengatur bahwa setiap orang atau pihak yang mengakses, mengumpulkan, atau menyebarkan data pribadi tanpa izin dapat dikenakan hukuman penjara dan/atau denda yang signifikan. Misalnya, jika ada bukti bahwa pegawai bank secara sengaja menjual data nasabah kepada pihak ketiga untuk keuntungan pribadi, maka pegawai tersebut dapat dikenai sanksi pidana sesuai ketentuan dalam UU PDP. Bank sebagai institusi juga dapat dikenakan denda jika terbukti gagal mengimplementasikan sistem perlindungan data yang memadai.

2. Mekanisme Perlindungan Data Nasabah

Perlindungan data nasabah merupakan aspek penting dalam menjaga kepercayaan dan integritas di sektor keuangan. Dalam dunia yang semakin digital, pengelolaan data pribadi nasabah harus dilakukan dengan standar keamanan tinggi untuk mencegah penyalahgunaan, pencurian data, dan pelanggaran privasi. Dalam Pasal 40 dari UU No. 10 Tahun 1998 tentang Perbankan ditegaskan bahwa bank memiliki kewajiban untuk menjaga kerahasiaan informasi mengenai nasabahnya, termasuk data simpanan maupun transaksi nasabah. Prinsip kerahasiaan bank ini bertujuan melindungi kepercayaan nasabah terhadap lembaga perbankan. Kewajiban tersebut hanya dapat dikesampingkan dalam keadaan tertentu yang diatur oleh undang-undang, seperti untuk kepentingan perpajakan, penyidikan pidana, atau permintaan pengadilan.

Perlindungan data nasabah dapat dilakukan dengan langkah-langkah berikut. Pertama, Penerapan teknologi keamanan yang merupakan fondasi utama dalam melindungi data nasabah, terutama di sektor perbankan. Berbagai teknologi canggih, seperti enkripsi, firewall, dan sistem deteksi intrusi, digunakan untuk menjaga kerahasiaan serta integritas data nasabah yang tersimpan di server. Teknologi ini juga memastikan data tetap aman selama proses transmisi melalui jaringan. Selain itu, bank harus menerapkan autentikasi berlapis untuk meningkatkan perlindungan. Contohnya, penggunaan metode verifikasi biometrik seperti sidik jari atau pengenalan wajah⁸ dan penggunaan kode *One-Time Password* (OTP) menjadi langkah wajib untuk memverifikasi identitas pengguna. Penggunaan sistem ini bertujuan untuk memastikan hanya pihak berwenang yang dapat mengakses informasi sensitif. Dengan demikian dapat mengurangi risiko kebocoran atau penyalahgunaan data. Penggunaan teknologi keamanan yang tepat tidak hanya melindungi data nasabah, tetapi juga membangun kepercayaan terhadap layanan perbankan digital yang semakin berkembang di era modern ini.

Kedua, Pengaturan kebijakan internal yang ketat juga merupakan aspek penting dalam perlindungan data nasabah. Lembaga keuangan harus menyusun kebijakan yang membatasi akses data hanya kepada karyawan yang memiliki wewenang sesuai tugas dan tanggung jawabnya. Langkah ini memastikan bahwa data sensitif tidak disalahgunakan oleh pihak yang tidak berwenang. Selain itu, pelatihan dan edukasi rutin bagi karyawan tentang pentingnya menjaga kerahasiaan data nasabah menjadi keharusan. Edukasi ini bertujuan untuk meningkatkan kesadaran terhadap risiko keamanan dan meminimalkan potensi pelanggaran akibat kelalaian. Dengan kebijakan internal yang kuat, risiko ancaman dari pihak internal dapat ditekan secara signifikan.

Ketiga, kepatuhan terhadap regulasi menjadi kewajiban yang tidak dapat diabaikan oleh lembaga keuangan dalam melindungi data nasabah. Di Indonesia, sejumlah peraturan menjadi

landasan hukum utama. Salah satunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mengatur prinsip-prinsip pengelolaan data seperti keharusan memperoleh persetujuan eksplisit dari pemilik data sebelum pengolahan dilakukan dan memastikan hak pemilik data termasuk pada hak untuk mengakses, memperbarui, dan menghapus data pribadi mereka. Selain itu POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan yang mengatur mengenai transparansi, kerahasiaan data, dan mekanisme pengaduan. Regulasi ini dirancang untuk menjaga kepercayaan nasabah serta memastikan pengelolaan data dilakukan sesuai standar hukum yang berlaku.

Keempat, penerapan transparansi dan tanggung jawab memperkuat kepercayaan nasabah. Lembaga keuangan harus memberikan informasi yang jelas mengenai cara data nasabah dikelola dan tujuan penggunaannya.¹⁰ Jika terjadi kebocoran data, bank wajib memberikan notifikasi kepada nasabah yang terdampak serta melaporkan insiden tersebut kepada Otoritas Jasa Keuangan (OJK) dalam waktu 24 jam sesuai ketentuan regulasi. Prosedur ini penting untuk menjaga transparansi dan meminimalkan dampak yang mungkin timbul. Selain itu, bank harus memiliki protokol penanganan insiden yang komprehensif dan rencana pemulihan yang jelas, mencakup langkah-langkah pemulihan data, penyelidikan forensik, serta tindakan pencegahan untuk mencegah kejadian serupa di masa mendatang. Implementasi langkah-langkah ini menunjukkan komitmen bank dalam menjaga kepercayaan nasabah dan mematuhi regulasi yang berlaku.

KESIMPULAN

Penelitian ini mengungkapkan bahwa tanggung jawab hukum bank dalam kasus kebocoran data nasabah bersifat kompleks dan berlapis, mencakup aspek administratif, perdata, dan pidana. Hasil analisis menunjukkan bahwa meskipun telah ada kerangka hukum yang mengatur perlindungan data nasabah, implementasinya masih menghadapi tantangan signifikan akibat pesatnya perkembangan teknologi dan semakin canggihnya ancaman siber. Studi kasus yang dilakukan mengungkapkan bahwa kebocoran data sering terjadi akibat kombinasi kelemahan sistem keamanan dan faktor human error, yang menggarisbawahi pentingnya pendekatan komprehensif dalam perlindungan data. Untuk memperkuat sistem perlindungan data nasabah, diperlukan pembaruan regulasi yang lebih responsif terhadap perkembangan teknologi, peningkatan standar keamanan teknis, dan penguatan kapasitas sumber daya manusia di sektor perbankan. Harmonisasi regulasi antar lembaga terkait dan kerjasama internasional dalam penanganan kejahatan siber juga menjadi faktor krusial dalam membangun sistem perlindungan data yang lebih efektif dan terpercaya

SARAN

Berdasarkan analisis yang telah dilakukan, Penulis dapat merekomendasikan beberapa hal, antara lain:

1. Penguatan Regulasi Internal dan Teknologi:
 - a. Implementasi sistem keamanan berlapis dengan autentikasi ganda untuk akses data sensitif.
 - b. Audit berkala terhadap aktivitas pegawai yang memiliki kewenangan tinggi.
2. Peningkatan Edukasi dan Pelatihan Pegawai. Pegawai bank perlu diberikan pelatihan intensif tentang etika kerja, hukum perlindungan data, dan ancaman hukum atas pelanggaran
3. Kolaborasi dengan Pemerintah. Bank Jago harus bekerja sama dengan OJK dan lembaga terkait untuk memperketat regulasi di sektor perbankan digital, termasuk pengawasan terhadap kejahatan siber dan
4. Perbaikan Sistem Transparansi kepada Konsumen Bank perlu menyediakan informasi kepada nasabah mengenai langkah-langkah yang dilakukan untuk meningkatkan keamanan data.

DAFTAR PUSTAKA

- Berto Purnomo Sidik, S. A. (2025). Tinjauan Hukum terhadap Aplikasi Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, 219-232.
- Khetrina Maria Angnesia, S. A. (2025). Analisis Pertanggungjawaban Hukum Pemerintah dalam Menegakkan Pelindungan Data Pribadi di Era Digital. *Perspektif Administrasi Publik dan hukum*, 176-187.
- Mugiono Mugiono, S. A. (2025). Between Ease and Vulnerability: Juridical Analysis of Population Identity Data Protection in Digital Applications. *COSMOS: Jurnal Ilmu Pendidikan, Ekonomi dan Teknologi*, 684-691.
- Muryani Verina Dwi, W. S. (2025). EFEKTIVITAS UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DALAM MENJAWAB TANTANGAN KEAMANAN SIBER DI INDONESIA. *Causa: Jurnal Hukum dan Kewarganegaraan*, 81-90.
- Shafa Salsabila, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, 145-157.
- Artha, Yohana, "Layanan BSI "Error", Erick Thohir Akui Ada Serangan Siber", <https://money.kompas.com/read/2023/05/10/140408326/layanan-bsi-errorerick-thohir-akui-ada-serangan-siber>
- Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132-142
- Anwar, M. (2020). "Perlindungan Hukum Terhadap Nasabah Bank Dalam Kasus Kebocoran Data Pribadi." *Jurnal Hukum & Pembangunan*, 50(1), 123-138.
- Bank Syariah Indonesia, <https://www.instagram.com/p/CrMIIari8H/>
- Jailani, A. (2019). Perlindungan Hukum Bagi Nasabah Terkait Dengan Rahasia Bank. *Dinamika Hukum*, 25(2).
- Jurnal Syntax Admiration. (n.d.). Analisis yuridis perlindungan hukum data.
- Kian, A. M. L. (2015). Tindak Pidana Credit/Debit Card Fraud dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia. *Hasanuddin Law Review*, 1(1), 47-60.
- Krismen, Y. (2014). Pertanggungjawaban Pidana Korporasi Dalam Kejahatan Ekonomi. *Jurnal Ilmu Hukum*, 5(1), 61-70.
- Kumar, V., & Singh, M. (2022). "Analysis of Recent Data Breaches in Banking Sector". *Journal of Information Security*, 13(2), 45-60.
- Nurhayati, I., & Farida, R. (2020). "Hak Dan Kewajiban Hukum Dalam Hubungan Antara Nasabah Dengan Bank. In *Prosiding Seminar Nasional Terapan Riset Inovatif (Sentrinov)*", (Vol. 6, No. 2, Pp. 50-56).
- Otoritas Jasa Keuangan Republik Indonesia, Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, POJK 6/POJK.07/2022 LN. No. 99 Tahun 2022, TLN No. 6788
- Prasetyo, A. (2021). "Kebocoran Data Nasabah dan Implikasinya Terhadap Kepercayaan Publik." *Jurnal Perbankan dan Hukum*, 7(2), 67-82.
- Papendang, A. A. (2016). "Hak Dan Kewajiban Nasabah Bank Serta Perlindungan Hukum Menurut Undang-Undang Nomor 10 Tahun 1998". *Lex Administratum*, 4(3).
- Peraturan Otoritas Jasa Keuangan No. 1/Pojk.07/2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan.

- Peraturan Pemerintah No. 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.
- Sutan Remy Sjahdeni, (2006), "Rahasia Bank : Berbagai Masalah Di Sekitarnya Dalam Hukum Perbankan", Program Pascasarjana Universitas Indonesia.
- Sari, R.(2019)."Tanggung Jawab Hukum Bank Dalam Melindungi Data Pribadi Nasabah."Jurnal Hukum dan Teknologi, 8(1), 45-58.
- Saputra, F. D., & Zubaedah, R. (2023). Eksplorasi Kebutuhan Dan Harapan Debitur Terhadap Perlindungan Data Pribadi Dalam Industri Keuangan. *Jurnal Ilmiah Wahana Pendidikan*, Juli, 2023(14), 297–306.
- Tambing, F., Yusuf, M., Fitriadi, M., & Nadzirin Anshari Nur, M. (2023). Keamanan Data Nasabah di Bank dan Perlindungan Otoritas Jasa Keuangan. *Journal Sultra Research of Law*, 5(1).
- Undang-undang (UU) Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
- Undang-undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Wijayanto, K. (2015). Pengaruh kualitas pelayanan terhadap kepuasan dan loyalitas nasabah bank.*Jurnal Manajemen Daya Saing*,17(1), 38-45.
- Wulandari, T. (2023). "Analisis Perlindungan Hukum Nasabah Terhadap Kebocoran Data." *Jurnal Hukum dan Kebijakan Publik*, 12(4), 333-348.
- Yohana, Y., Syahrin, A., Hamdan, M., & Siregar, M. (2014). Pertanggungjawaban Pidana dalam Kejahatan Perbankan.*USU Law Journal*,2(3), 221-237
- Yustianti, S., & Roesli, M. (2018). Bank Indonesia Policy in the National Banking Crisis Resolution.*YURISDIKSI: Jurnal Wacana Hukum Dan Sains*,11(2), 77-90.
- Yetno, A. (2024). Tanggung Jawab Bank Dalam Menjaga Keamanan Dan Kerahasiaan Data Nasabah Perbankan Di Indonesia. *Morality: Jurnal Ilmu Hukum*, 10(1), 67–76. <http://dx.doi.org/10.52947/morality.v10i1.424>.

1.