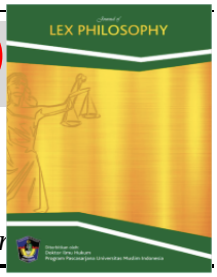
Journal of Lex Philosophy (JLP)
Volume 6, Nomor 1, Desember 2025
P-ISSN: 2722-1237, E-ISSN: 2722-2020
Website: http: pasca-umi.ac.id/index.php/jlp
This work is licensed under a Creative Commons Attribution 4.0 International Licer



Perlindungan Hukum Kerahasiaan Data Pribadi Nasabah Pada Perbankan Di Indonesia

Ferdiansyah[1], Zainuddin[2] & Andi Risma[2]

[1]*Magister Ilmu Hukum, Universitas Muslim Indonesia*
[2]*Fakultas Hukum, Universitas Muslim Indonesi*
[*]*Koresponden Penulis, E-mail*: ferdiansyah.ferdiansyah@umi.ac.id

Submitted: 28 Mei 2025; Revised: 17 Juni 2025; Accepted: 27 Juni 2025

ABSTRAK
Penelitian ini bertujuan untuk menganalisis penerapan dan tanggung jawab hukum perbankan dalam menjaga kerahasiaan data pribadi nasabah di Indonesia, seiring dengan meningkatnya risiko kebocoran data di era digital. Perlindungan terhadap data pribadi nasabah merupakan bagian dari hak privasi yang dijamin dalam berbagai instrumen hukum, termasuk Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian ini menggunakan pendekatan normatif-yuridis dengan metode studi pustaka yang menelaah ketentuan peraturan perundang-undangan, doktrin hukum, dan putusan pengadilan terkait. Hasil penelitian menunjukkan bahwa meskipun regulasi telah mengatur prinsip kerahasiaan, namun masih terdapat celah implementasi yang memungkinkan terjadinya pelanggaran hak privasi nasabah. Oleh karena itu, dibutuhkan harmonisasi regulasi serta peningkatan pengawasan dan keamanan sistem teknologi informasi di sektor perbankan. Tanggung jawab hukum bank tidak hanya terbatas pada aspek preventif, tetapi juga harus mencakup tindakan korektif dan pemulihan bagi nasabah yang dirugikan akibat kebocoran data. Penelitian ini merekomendasikan pembentukan mekanisme pengawasan khusus dan peningkatan literasi hukum data pribadi dalam praktik perbankan.

Kata Kunci: *Perlindungan Hukum; Data Pribadi, Kerahasiaan; Perbankan*

ABSTRACT
This study aims to analyze the application and legal responsibilities of banks in protecting customers' personal data confidentiality in Indonesia, amidst the growing risks of data breaches in the digital era. Protection of customers' personal data is part of the right to privacy guaranteed by several legal instruments, including Law No. 10 of 1998 on Banking and Law No. 27 of 2022 on Personal Data Protection. This research employs a normative-juridical approach by examining statutory regulations, legal doctrines, and relevant court decisions. The findings indicate that, although regulations uphold the principle of confidentiality, there are still implementation gaps that may lead to violations of customer privacy rights. Therefore, regulatory harmonization as well as enhanced supervision and information technology system security in the banking sector are essential. The bank's legal responsibility should not only be preventive but also include corrective actions and compensation for customers affected by data breaches. This study recommends the establishment of a specialized oversight mechanism and increased legal literacy on personal data protection in banking practices.

Keywords: *Legal Protection; Personal Data; Confidentiality; Banking.*

PENDAHULUAN

Perbankan merupakan lembaga keuangan utama dalam struktur perekonomian suatu negara. Fungsi bank yang sangat strategis menjadikannya sebagai motor penggerak pembangunan nasional (Damayanti, Pamungkas & Lestari, 2023). Sebagaimana diatur dalam Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perbankan, bank memiliki peran vital dalam menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkan kembali dana tersebut kepada pihak yang membutuhkan. Dalam rangka mewujudkan tujuan pembangunan nasional sebagaimana amanat Pembukaan UUD 1945, perbankan menjadi instrumen penting dalam mendorong pertumbuhan ekonomi dan menciptakan stabilitas keuangan. Oleh karena itu, integritas dan kepercayaan masyarakat terhadap lembaga perbankan harus dijaga, salah satunya melalui perlindungan atas data pribadi nasabah.

Perbankan dituntut untuk bekerja secara profesional, dapat membaca dan menganalisis seluruh kegiatan ekonomi nasional. Maka dari itu, pengawasan dan pembinaan terhadap perbankan menjadi penting agar dapat bekerja efisien, wajar, dan sehat (Siregar, 2024). Perlindungan terhadap data nasabah merupakan bagian integral dari prinsip kehati-hatian dalam operasional bank.

Kerangka hukum perbankan di Indonesia berlandaskan pada beberapa regulasi utama, di antaranya Undang-Undang Nomor 10 Tahun 1998 dan Undang-Undang Nomor 7 Tahun 1992 yang menjadi dasar legal institusi perbankan. Selain itu, penguatan aspek perlindungan konsumen serta tata kelola keuangan ditopang oleh Undang-Undang Nomor 4 Tahun 2023 tentang Penguatan dan Pengembangan Sektor Keuangan (UU PPSK).

Perlindungan terhadap data pribadi secara umum diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. UU ini menjadi tonggak penting dalam era digital yang mengatur tata kelola data pribadi serta menjamin hak warga negara atas privasi dan keamanan informasi pribadinya.

Lembaga perbankan wajib menjaga kerahasiaan data nasabahnya. Pasal 40 ayat (1) UU Perbankan menyatakan bahwa bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya. Pelanggaran terhadap ketentuan ini dapat menyebabkan hilangnya kepercayaan publik terhadap sistem perbankan (UU No. 10 Tahun 1998).

Konsep rahasia bank sebagaimana dijelaskan dalam Pasal 1 angka 28 UU No. 10 Tahun 1998 menyatakan bahwa rahasia bank mencakup seluruh informasi terkait nasabah penyimpan dan simpanannya. Perlindungan ini tidak hanya bersifat hukum, namun juga menyangkut etika profesional perbankan.

Perlindungan hukum data pribadi juga diperkuat melalui UU ITE, khususnya Pasal 26 yang mewajibkan penyelenggara sistem elektronik untuk menjaga kerahasiaan dan integritas data pengguna (UU No. 19 Tahun 2016). Data pribadi tidak dapat digunakan tanpa persetujuan eksplisit dari pemilik data.

UU ITE menekankan dua dasar legitimasi dalam pemrosesan data pribadi, yaitu persetujuan (consent) dan dasar hukum yang sah. Ketentuan ini penting untuk memberikan perlindungan hukum bagi nasabah dalam lingkungan digital yang

rentan terhadap penyalahgunaan data (Safitri, 2022). Dalam konteks pengawasan sektor keuangan, UU OJK Nomor 21 Tahun 2011 memberikan kewenangan kepada OJK untuk melindungi konsumen, termasuk ketika terjadi pelanggaran atas privasi data oleh lembaga keuangan. OJK dapat melakukan tindakan hukum atas nama konsumen yang dirugikan (Putra, 2023).

Peraturan OJK No. 1/POJK.07/2013 dan SEOJK No. 14/SEOJK.07/2014 mengatur secara spesifik kewajiban bank untuk menjaga keamanan data nasabah dan melarang pemberian informasi kepada pihak ketiga tanpa persetujuan tertulis. Ketentuan ini menjadi penting dalam membangun sistem keamanan informasi yang kuat di sektor perbankan.

Namun, dalam praktiknya, perlindungan data nasabah masih menghadapi tantangan besar. Kasus kebocoran data BRI pada Januari 2022, yang mengungkap informasi seperti nomor rekening dan saldo, menunjukkan lemahnya sistem keamanan digital bank (Yudistira & Ramadani, 2023).

Kasus serangan ransomware terhadap BSI oleh LockBit 3.0 pada Mei 2023 menjadi sorotan publik. Kebocoran 1,5 TB data dari 15 juta nasabah menjadi ancaman serius, terutama ketika sebagian data dijual di dark web. Ini membuktikan perlunya penguatan sistem keamanan siber di perbankan (Endrosava & Afiliasi, 2024).

Selain itu, insiden kebocoran data Bank Jatim yang dijual oleh kelompok peretas di forum daring menambah deretan kasus serupa. Diperlukan tanggung jawab dan tindakan nyata dari bank dan otoritas untuk menangani serta mencegah insiden semacam ini terulang kembali.

Kasus-kasus tersebut mengindikasikan bahwa meskipun telah ada regulasi, implementasi perlindungan data pribadi belum optimal. Bank harus meningkatkan kapasitas teknologi, audit keamanan, serta pelatihan SDM guna menghadapi ancaman siber yang semakin canggih.

Perlindungan data pribadi di sektor perbankan tidak hanya terkait pada kepatuhan terhadap undang-undang, tetapi juga menjadi bagian dari tanggung jawab sosial institusi keuangan kepada nasabah. Kepercayaan nasabah adalah aset utama bank, dan harus dijaga melalui komitmen tinggi terhadap kerahasiaan informasi.

Dalam konteks globalisasi dan digitalisasi, data pribadi menjadi komoditas berharga. Oleh karena itu, regulasi nasional harus terus diperbarui agar sejalan dengan perkembangan teknologi dan praktik keamanan data secara internasional.

Diperlukan sinergi antara regulator, pelaku usaha perbankan, dan masyarakat dalam membangun kesadaran serta sistem perlindungan data yang tangguh. Pendekatan hukum harus disertai dengan pendekatan teknologi dan edukasi publik agar perlindungan data menjadi budaya bersama.

Berdasarkan paparan tersebut, maka urgensi hukum perlindungan data nasabah di sektor perbankan menjadi sangat penting. Ke depan, upaya harmonisasi hukum nasional dengan standar internasional, serta penguatan pengawasan oleh OJK, menjadi langkah strategis dalam menjamin keamanan data nasabah.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum yang bersifat normatif-yuridis, yaitu penelitian yang menitikberatkan pada kajian terhadap norma-norma hukum positif yang berlaku. Fokus utama dari penelitian ini adalah mengkaji urgensi perlindungan hukum terhadap kerahasiaan data nasabah dalam sektor perbankan. Isu ini menjadi sangat relevan seiring dengan meningkatnya digitalisasi layanan perbankan dan potensi kebocoran data pribadi yang dapat merugikan nasabah. Penelitian ini tidak hanya bertujuan untuk menggambarkan kondisi normatif yang berlaku, tetapi juga untuk mengidentifikasi kelemahan dalam regulasi yang ada dan memberikan alternatif solusi guna memperkuat rezim perlindungan data di sektor keuangan.

Pendekatan yang digunakan dalam penelitian ini terdiri atas dua pendekatan utama. Pertama, pendekatan perundang-undangan (statute approach), yaitu dengan menelaah seluruh peraturan perundang-undangan yang berkaitan dengan perlindungan kerahasiaan data nasabah, baik yang bersumber dari undang-undang perbankan, perlindungan data pribadi, maupun ketentuan Otoritas Jasa Keuangan (OJK). Pendekatan ini digunakan untuk memahami filosofi serta rasio legis di balik pembentukan norma hukum tersebut. Kedua, pendekatan konseptual (conceptual approach), yaitu dengan mengkaji konsep-konsep dasar dalam ilmu hukum yang relevan, seperti hak atas privasi, prinsip kehati-hatian (prudential principle), dan asas kerahasiaan. Melalui pendekatan ini, diharapkan lahir analisis hukum yang memiliki landasan teori yang kuat dan mampu memberikan rekomendasi kebijakan yang tepat dan aplikatif.

PEMBAHASAN

A. Penerapan Perlindungan Hukum Kerahasiaan Data Pribadi Nasabah Perbankan di Indonesia

1. Membangun Kepercayaan Masyarakat

Perkembangan teknologi informasi dalam sektor perbankan telah menghadirkan berbagai kemudahan dalam aktivitas transaksi keuangan, tetapi juga menyimpan risiko baru terkait kerahasiaan data pribadi nasabah. Kepercayaan masyarakat menjadi faktor kunci yang menentukan keberlanjutan operasional perbankan, dan salah satu indikator utama dari kepercayaan ini terletak pada sejauh mana bank mampu menjaga kerahasiaan data pribadi nasabah. Undang-Undang Republik Indonesia No. 7 Tahun 1992 yang telah diperbarui melalui Undang-Undang No. 10 Tahun 1998 tentang Perbankan (UU Perbankan), serta Undang-Undang No. 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) dan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi fondasi yuridis utama dalam mengatur aspek perlindungan data di sektor ini (Yuniarti, 2019; Damayanti, Pamungkas & Lestari, 2023).

Pasal 14 angka 27 UU P2SK yang mengubah Pasal 40 ayat (1) UU Perbankan secara eksplisit mengatur bahwa bank dan pihak terafiliasi wajib menjaga rahasia nasabah penyimpan, termasuk pegawai dan pejabat bank. Namun, terdapat pengecualian tertentu atas kewajiban tersebut, misalnya dalam perkara perdata atau pidana, permintaan pengadilan niaga, persetujuan tertulis dari nasabah, permintaan ahli waris, serta untuk kepentingan negara atau instansi resmi lainnya yang diatur dalam

ketentuan hukum positif. Oleh karena itu, kerangka hukum ini menunjukkan adanya keseimbangan antara prinsip kerahasiaan dan kebutuhan hukum atau administratif yang sah.

Perlindungan hukum terhadap data pribadi nasabah mencakup identitas, alamat, nomor rekening, hingga riwayat transaksi. UU PDP mengatur prinsip-prinsip pemrosesan data seperti legalitas, transparansi, akuntabilitas, dan persetujuan (consent) eksplisit dari pemilik data (Ramadhani & Wiraguna, 2025). Bank dilarang membocorkan data nasabah tanpa persetujuan tertulis kecuali diatur oleh undang-undang atau diperintahkan oleh pengadilan. Hal ini mempertegas bahwa kerahasiaan data merupakan prinsip mendasar dalam layanan perbankan.

Penerapan perlindungan hukum ini penting untuk mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab seperti penipuan, pencurian identitas, atau pemasaran tanpa izin. Bank harus menerapkan sistem keamanan yang komprehensif dan melakukan edukasi publik kepada nasabah mengenai pentingnya menjaga data pribadi mereka. Jika perlindungan ini dilakukan secara konsisten, akan terbentuk loyalitas dan kepercayaan dari masyarakat terhadap lembaga keuangan.

Bank yang konsisten dalam menjaga kerahasiaan data akan menikmati reputasi yang baik di masyarakat. Hal ini berdampak langsung pada pertumbuhan bisnis, loyalitas nasabah, dan kemampuan untuk mengembangkan layanan inovatif secara berkelanjutan. Oleh karena itu, keamanan data bukan sekadar kewajiban hukum, tetapi merupakan strategi bisnis jangka panjang yang efektif.

2. Perlindungan Data Pribadi Nasabah dari Kejahatan Siber

Ancaman kejahatan siber menjadi tantangan besar dalam upaya melindungi data pribadi nasabah perbankan. Data seperti nama, NIK, nomor rekening, dan informasi keuangan menjadi target utama pelaku kejahatan digital. Oleh karena itu, keberadaan UU PDP dan regulasi turunan seperti Peraturan OJK Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum sangat krusial dalam memperkuat proteksi terhadap ancaman tersebut (OJK, 2023).

Peraturan OJK Nomor 44 Tahun 2024 tentang Rahasia Bank mempertegas bahwa penyampaian informasi nasabah kepada pihak ketiga harus dilandasi oleh persetujuan atau dasar hukum yang sah. Ancaman siber yang umum mencakup phishing, malware, ransomware, spoofing, keylogger, pharming, skimming, sniffing, carding, hingga penipuan OTP. Setiap metode ini dirancang untuk mencuri data pribadi dengan teknik manipulatif atau teknologi canggih (Yudistira & Ramadani, 2023).

Kasus serangan ransomware terhadap Bank Syariah Indonesia pada tahun 2023 menjadi pelajaran penting. Serangan ini menginfeksi sistem dan mengekspos data 15 juta nasabah, mengakibatkan gangguan layanan selama hampir satu minggu. Survei Kominfo (2021) juga menunjukkan bahwa 12,1% responden pernah mengalami kebocoran data finansial, dengan kerugian berupa pengurangan saldo tabungan dan e-wallet.

Bank wajib menerapkan langkah-langkah teknologi seperti enkripsi, sistem deteksi intrusi, dan autentikasi multifaktor untuk menghindari kebocoran data. Selain itu, bank harus membangun sistem manajemen risiko yang mampu mengenali dan

merespons potensi ancaman siber secara real time. Ini menjadi bagian dari tanggung jawab hukum sekaligus bentuk perlindungan terhadap kepercayaan publik.

3. Kepatuhan pada Regulasi

Kepatuhan terhadap regulasi merupakan pilar utama dalam menjamin keamanan dan kerahasiaan data pribadi nasabah. Fungsi kepatuhan (compliance function) di dalam lembaga perbankan bertugas memastikan bahwa seluruh kegiatan operasional, termasuk pemrosesan data pribadi, dilaksanakan sesuai dengan hukum dan prinsip kehati-hatian (Siregar, 2024).

Peraturan OJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat menggantikan POJK sebelumnya, dan menjadi kerangka hukum utama dalam perlindungan konsumen sektor keuangan. Peraturan ini mewajibkan bank memiliki pengendalian internal dan prosedur kepatuhan yang memadai, termasuk dalam hal perlindungan data. Selain itu, Bank Indonesia melalui Peraturan Nomor 4 Tahun 2025 juga menetapkan standar keamanan dalam sistem pembayaran digital.

Bank juga diwajibkan untuk melakukan audit internal secara berkala, mengadopsi teknologi yang aman, dan membangun sistem kontrol akses yang membatasi akses data hanya pada pihak yang berwenang. Fungsi kepatuhan memastikan seluruh perangkat dan sistem informasi perbankan berjalan sesuai standar keamanan data yang ditetapkan (BI, 2025).

Good Corporate Governance (GCG) menjadi dasar tata kelola perlindungan data yang mendorong akuntabilitas dan transparansi dalam setiap lini manajemen. Dengan penerapan GCG, pengelolaan risiko kebocoran data dapat terintegrasi dalam sistem manajemen risiko secara keseluruhan. Regulasi seperti POJK Nomor 4 Tahun 2025 tentang Penyelenggara Agregasi Jasa Keuangan juga memperkuat pentingnya manajemen risiko perlindungan data di era digital.

Peraturan OJK Nomor 46/POJK.03/2017 tentang Fungsi Kepatuhan Bank Umum memberikan landasan kuat bagi fungsi kepatuhan untuk menjalankan pengawasan internal, menangani pelanggaran, dan merekomendasikan tindakan korektif. Fungsi ini menjadi benteng utama dalam menghadapi ancaman terhadap kerahasiaan data nasabah.

Penting juga bagi bank untuk terus melakukan pelatihan dan edukasi kepada seluruh pegawai mengenai pentingnya perlindungan data pribadi. Hal ini bertujuan membangun budaya kepatuhan yang kuat dan mencegah pelanggaran yang disebabkan oleh kelalaian manusia. Dengan sistem yang kuat dan SDM yang sadar hukum, perlindungan data nasabah dapat terjaga secara maksimal.

B. Tanggung Jawab Hukum Perbankan Dalam Menjaga Kerahasiaan Data Pribadi Nasabah di Indonesia

1. Tanggung Jawab Administratif

Bank memiliki tanggung jawab hukum yang signifikan dalam menjaga keamanan dan kerahasiaan data pribadi nasabahnya. Tanggung jawab ini diatur dalam berbagai regulasi, termasuk Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Regulasi tersebut mewajibkan bank untuk memiliki dan menerapkan sistem keamanan informasi yang memadai agar data pribadi nasabah

terlindungi dari kebocoran maupun penyalahgunaan oleh pihak yang tidak berwenang.

Dalam konteks administratif, Otoritas Jasa Keuangan (OJK) memiliki kewenangan dalam mengatur dan mengawasi pelaksanaan perlindungan data oleh institusi keuangan melalui sejumlah regulasi. Misalnya, Peraturan OJK No. 38/POJK.03/2016 tentang Manajemen Risiko Teknologi Informasi dan POJK No. 77/POJK.01/2016 tentang Inovasi Keuangan Digital mengatur bagaimana bank wajib menerapkan kebijakan keamanan informasi yang ketat. OJK juga mewajibkan bank untuk melakukan audit berkala terhadap sistem manajemen data nasabah.

Sanksi administratif dapat dijatuhkan terhadap bank yang gagal menjalankan kewajiban perlindungan data nasabah, seperti denda, pencabutan izin usaha, atau penghentian sebagian aktivitas bisnis. POJK No. 22/2023 memberikan dasar hukum atas penjatuhan sanksi administratif tersebut (Supangkat, 2025). SEOJK No. 14/2014 turut memberikan panduan lebih lanjut mengenai keamanan informasi dan kerahasiaan data nasabah (Djafar, 2019).

Setiap proses pengumpulan, penyimpanan, dan pemrosesan data pribadi nasabah harus dilakukan berdasarkan prinsip-prinsip perlindungan data. Prinsip tersebut antara lain mencakup persetujuan eksplisit dari nasabah, kerahasiaan data, serta pemberian hak akses kepada nasabah untuk melakukan koreksi atau penghapusan data. Implementasi prinsip ini menjadi dasar penting dalam membangun transparansi dan meningkatkan kepercayaan publik.

Kebocoran data akibat kelalaian sistem keamanan bank dapat dikenai sanksi administratif oleh regulator. Sanksi tersebut termasuk denda, teguran tertulis, hingga pencabutan izin operasional, tergantung pada tingkat pelanggaran. Tanggung jawab bank juga mencakup tindakan pegawai atau mitra pihak ketiga yang menyebabkan kebocoran data.

Pengendalian internal yang efektif menjadi kewajiban bank, termasuk kebijakan keamanan informasi, audit internal berkala, serta mitigasi risiko serangan siber. Transparansi informasi kepada nasabah harus dijalankan secara konsisten. Bila terjadi insiden keamanan data, bank wajib memberikan notifikasi kepada nasabah dan melaporkannya kepada OJK.

Ketentuan Pasal 40 UU No. 10 Tahun 1998 menegaskan bahwa bank wajib menjaga rahasia nasabah, kecuali dalam keadaan tertentu sebagaimana diatur oleh undang-undang. Dalam kerja sama dengan pihak ketiga, bank juga wajib memastikan bahwa pihak yang memiliki akses terhadap data nasabah tunduk pada regulasi perlindungan data.

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan mempertegas pentingnya perlindungan konsumen, termasuk aspek keamanan data pribadi. Pelaku usaha sektor jasa keuangan diwajibkan untuk menerapkan prinsip dasar perlindungan data sesuai standar hukum yang berlaku.

2. Tanggung Jawab Perdata

Tanggung jawab perdata dalam sektor perbankan bersumber dari hubungan kontraktual antara bank dan nasabah. Hubungan hukum ini mengandung prinsip kepercayaan, di mana nasabah menyerahkan data pribadinya dengan keyakinan

bahwa data tersebut akan dijaga kerahasiaannya. Pelanggaran terhadap prinsip kepercayaan ini dapat menimbulkan gugatan ganti rugi berdasarkan wanprestasi atau perbuatan melawan hukum.

Landasan hukum bagi tanggung jawab perdata bank tercantum dalam Undang-Undang No. 10 Tahun 1998 dan UU PDP. Dalam hal bank menyalahgunakan atau lalai menjaga data pribadi nasabah, maka nasabah berhak menuntut kompensasi atas kerugian yang diderita.

Kasus wanprestasi dapat terjadi apabila terdapat pelanggaran terhadap perjanjian layanan, khususnya mengenai perlindungan data. Dalam hal perbuatan melawan hukum, bank dapat digugat apabila terjadi kelalaian atau tindakan menyimpang yang menimbulkan kerugian, baik oleh pegawai maupun pihak ketiga yang bekerja sama dengan bank. Salah satu bentuk tanggung jawab bank adalah menyediakan jalur penyelesaian sengketa, seperti pengaduan konsumen, mediasi melalui LAPS SJK (Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan), maupun gugatan ke pengadilan.

Putusan No. 3/PDT.Sus-BPSK/2022/PN LSM menjadi contoh konkret mengenai kelalaian bank dalam menjaga data pribadi yang menyebabkan kerugian material dan immaterial bagi nasabah. Bank dalam kasus tersebut dikenai ganti rugi, yang menunjukkan pentingnya penguatan regulasi dan sistem perlindungan data.

Pasal 1367 KUHPerdata mengatur pertanggungjawaban vicarious liability, di mana bank dapat dimintai tanggung jawab atas perbuatan melawan hukum yang dilakukan oleh pegawai dalam lingkup tugasnya. Hal ini menegaskan pentingnya pelatihan dan pengawasan terhadap sumber daya manusia di lingkungan bank.

Peraturan OJK juga memperkuat tanggung jawab perdata dengan menetapkan bahwa bank bertanggung jawab atas kerugian nasabah akibat tindakan atau kelalaian pegawai atau pihak ketiga. Oleh karena itu, bank perlu merancang sistem perlindungan data secara menyeluruh dan proaktif.

3. Tanggung Jawab Pidana

Aspek pidana dalam perlindungan data pribadi nasabah menjadi elemen penting dalam kerangka hukum perlindungan konsumen sektor keuangan. Tanggung jawab ini muncul ketika terjadi pelanggaran hukum pidana yang merugikan nasabah. UU PDP, terutama Pasal 65, menetapkan bahwa setiap pihak yang secara melawan hukum mengakses, menyebarluaskan, atau menyalahgunakan data pribadi dapat dikenai hukuman pidana. Ancaman pidana meliputi pidana penjara dan denda. Pegawai bank yang dengan sengaja membocorkan data nasabah dapat diproses secara pidana.

Bank sebagai entitas korporasi juga dapat dikenai pertanggungjawaban pidana jika terbukti lalai dalam menerapkan sistem perlindungan data. Ketentuan ini sejalan dengan prinsip corporate criminal liability atau pertanggungjawaban pidana korporasi. UU No. 10 Tahun 1998 mengatur bahwa hanya dalam kondisi tertentu dan berdasarkan hukum, data nasabah dapat dibuka. Jika bank melanggar ketentuan tersebut, maka dapat dijatuhi sanksi pidana sesuai hukum yang berlaku.

Manajemen bank yang lalai dalam mengawasi penerapan kebijakan perlindungan data dapat turut dimintai pertanggungjawaban pidana. Kegagalan menerapkan

sistem pengawasan internal yang memadai menjadi faktor pemberat dalam proses hukum. Kebocoran data yang terjadi secara sistemik akibat lemahnya sistem keamanan siber dan ketiadaan audit internal menunjukkan adanya kelalaian struktural. Dalam hal ini, tidak hanya pelaku langsung, namun juga pengambil kebijakan di lembaga tersebut dapat dijerat hukum.

Pemahaman dan kepatuhan terhadap hukum perlindungan data harus menjadi bagian dari budaya organisasi perbankan. Pelatihan rutin, evaluasi risiko, serta penerapan teknologi mutakhir merupakan langkah-langkah preventif yang wajib dilakukan. Proses pelaporan oleh nasabah atas pelanggaran data kepada lembaga penegak hukum perlu difasilitasi secara jelas dan efisien. Kepastian hukum dan rasa keadilan menjadi tolok ukur efektivitas penegakan hukum.

Sanksi pidana juga dapat disertai denda administratif sebagaimana diatur dalam UU PDP. Hal ini menunjukkan bahwa suatu pelanggaran dapat dikenai sanksi secara simultan dari sisi pidana maupun administratif. Keberhasilan penegakan hukum dalam konteks pidana sangat dipengaruhi oleh koordinasi antara OJK, Kominfo, dan aparat penegak hukum. Penguatan sinergi antar lembaga menjadi kunci utama dalam menciptakan sistem perlindungan yang efektif.

Penegakan tanggung jawab pidana dalam perlindungan data pribadi nasabah berperan besar dalam menjaga kepercayaan masyarakat terhadap sistem perbankan. Selain sebagai bentuk kepatuhan hukum, hal ini juga merupakan bagian dari strategi membangun stabilitas sektor keuangan.

KESIMPULAN

1. Penerapan perlindungan hukum terhadap kerahasiaan data pribadi nasabah perbankan di Indonesia telah mengalami kemajuan yang signifikan dengan hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang memberikan kerangka hukum umum dalam melindungi hak-hak subjek data, termasuk nasabah bank. Di sektor perbankan, ketentuan tersebut diperkuat dengan berbagai regulasi sektoral seperti Undang-Undang Perbankan, Peraturan Otoritas Jasa Keuangan (POJK), serta kebijakan internal masing-masing bank yang mewajibkan prinsip transparansi, persetujuan, dan akuntabilitas dalam pengelolaan data.
2. Perbankan di Indonesia memikul tanggung jawab hukum yang signifikan dalam menjaga kerahasiaan data pribadi nasabah, sebagaimana diatur dalam berbagai peraturan perundang-undangan seperti Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kewajiban ini mencakup pengamanan data sejak proses pengumpulan, penyimpanan, hingga pemusnahan, serta pencegahan akses ilegal oleh pihak ketiga. Apabila terjadi pelanggaran terhadap kewajiban tersebut, bank dapat dikenakan sanksi administratif maupun pidana, yang pada gilirannya akan berdampak terhadap reputasi dan keberlangsungan usaha perbankan.

SARAN

1. **Penguatan Regulasi dan Pengawasan Terintegrasi:** Pemerintah bersama otoritas sektor keuangan, seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI),

perlu memperkuat harmonisasi regulasi antara Undang-Undang Perbankan dan Undang-Undang Perlindungan Data Pribadi dengan menetapkan peraturan turunan yang jelas, operasional, dan adaptif terhadap perkembangan teknologi digital. Selain itu, pengawasan perlu dilakukan secara berkala dan menyeluruh dengan melibatkan audit independen untuk memastikan bahwa setiap lembaga perbankan menerapkan standar keamanan informasi dan perlindungan data pribadi secara optimal.

2. **Peningkatan Kapasitas SDM dan Teknologi Keamanan Data:** Setiap lembaga perbankan di Indonesia perlu berinvestasi dalam peningkatan kualitas sumber daya manusia (SDM) yang kompeten di bidang keamanan siber dan perlindungan data pribadi. Selain itu, bank juga perlu menerapkan teknologi enkripsi terkini, sistem deteksi dini kebocoran data (intrusion detection system), dan prosedur tanggap insiden yang efektif. Langkah ini tidak hanya akan mencegah kebocoran data nasabah, tetapi juga memperkuat kepercayaan publik terhadap sistem perbankan nasional.

DAFTAR PUSTAKA

Bank Indonesia. (2025). *Peraturan Bank Indonesia Nomor 4 Tahun 2025 tentang Kebijakan Sistem Pembayaran*. Jakarta: Bank Indonesia. (belum tercatat dalam LNRI, karena masih tahun berjalan).

Damayanti, A. N., Pamungkas, Z. B., & Lestari, T. I. (2023). Perlindungan Hukum Terhadap Konsumen Pengguna Jasa Perbankan. In *Prosiding Seminar Nasional Hukum, Bisnis, Sains Dan Teknologi* (Vol. 3, No. 1, pp. 487-496).

Djafar, W. (2019, August). Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. In *Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM* (Vol. 26, pp. 1-14).

Endrosava, A. A., & Afiliasi, S. (2024). Peran Regulasi Modern dalam Menjaga Integritas Sistem Hukum Perbankan Digital. *Jurnal Multidisiplin Ilmu Akademik*, *1*(6), 228-235.

Munawarah, H., Yusuf, M., & Komarudin, P. (2022). *Bank digital syariah: analisis cyber security menurut hukum positif di Indonesia dan hukum ekonomi syariah*. PT. Borneo Development Project.

Otoritas Jasa Keuangan. (2016). *Peraturan OJK Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 38.

Otoritas Jasa Keuangan. (2016). *Peraturan OJK Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 77.

Otoritas Jasa Keuangan. (2023). *POJK Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 22.

Otoritas Jasa Keuangan. (2014). *SEOJK Nomor 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data Nasabah*. Tidak dimuat dalam Lembaran Negara, sumber internal OJK.

Ramadhani, W. K. S., & Wiraguna, S. A. (2025). Implementasi pelindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan. *Perspektif Administrasi Publik dan hukum*, *2*(2), 158-175.

Republik Indonesia. (1998). *Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan*. Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 238, Tambahan Lembaran Negara Republik Indonesia Nomor 6845.

Republik Indonesia. (2023). *Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 20, Tambahan Lembaran Negara Republik Indonesia Nomor 6859.

Republik Indonesia. (2023). *Kitab Undang-Undang Hukum Perdata (BW)*. *Staatsblad Tahun 1847 Nomor 23*.

Siregar, F. S. (2024). Peran Fungsi Kepatuhan Dalam Memitigasi Risiko Reputasi Di Perbankan Syariah. *Jurnal Ekonomi, Sosial & Humaniora*, *6*(02), 211-214.

Yudistira, M., & Ramadani, R. (2023). Tinjauan yuridis terhadap efektivitas penanganan kejahatan siber terkait pencurian data pribadi menurut undang-undang no. 27 tahun 2022 oleh kominfo. *UNES Law Review*, *5*(4), 3917-3929.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147-154

.