Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 90-97

# ANALISIS SANKSI ADMINISTRASI TERHADAP BANK YANG GAGAL MELINDUNGI DATA REKENING NASABAH DI INDONESIA

**Fathan Al Majid [1], Sidi Ahyar Wiraguna [2]**
[1, 2] Fakultas Hukum Universitas Esa Unggul Tangerang
fathnmjd@gmail.com

**Abstract (English)**

*The digitalization of the banking sector has enhanced the efficiency of financial services but simultaneously introduced significant risks to the security of customers' personal data. This study aims to analyze the legal responsibilities of banks and the effectiveness of administrative sanctions based on Law No. 27 of 2022 on Personal Data Protection (PDP Law), particularly in cases where banks fail to safeguard customer account data. The research employs a normative juridical method, using statutory and conceptual approaches. The findings reveal that banks, as data controllers, are legally obligated to obtain explicit consent and implement both technical and administrative measures to secure customer data. However, case studies involving Bank Syariah Indonesia (BSI) and Bank Jago expose major weaknesses in internal security systems and oversight, leading to large-scale data breaches. While the PDP Law comprehensively regulates administrative sanctions—including fines, written warnings, and license revocations—the effectiveness of its enforcement remains limited due to weak institutional oversight, the absence of an independent supervisory authority, and low levels of digital literacy among the public and industry players. This research recommends strengthening regulatory institutions, implementing periodic compliance audits, improving public digital literacy, and harmonizing cross-sector regulations to enhance personal data protection in the banking industry. Data protection should not only be seen as a technical issue but as a fundamental manifestation of the right to privacy as part of human rights.*

**Article History**
Submitted: 21 Mei 2025
Accepted: 24 Mei 2025
Published: 25 Mei 2025

**Key Words**
*Personal data protection, bank, PDP Law, administrative sanctions, digital security*

**Abstrak (Indonesia)**

*Digitalisasi sektor perbankan telah meningkatkan efisiensi layanan keuangan, namun juga memunculkan risiko signifikan terhadap keamanan data pribadi nasabah. Penelitian ini bertujuan untuk menganalisis bentuk tanggung jawab hukum bank dan efektivitas penerapan sanksi administratif berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), khususnya ketika bank gagal melindungi data rekening nasabah. Metode yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa bank sebagai pengendali data memiliki kewajiban teknis dan administratif yang tegas untuk memperoleh persetujuan eksplisit dan menjamin keamanan data nasabah. Namun, studi kasus terhadap Bank Syariah Indonesia (BSI) dan Bank Jago mengungkap lemahnya sistem keamanan internal dan pengawasan yang mengakibatkan kebocoran data berskala besar. UU PDP telah mengatur sanksi administratif secara komprehensif, termasuk denda, teguran, hingga pencabutan izin. Akan tetapi, efektivitas implementasinya masih terbatas akibat lemahnya pengawasan, belum adanya lembaga pengawas independen, serta rendahnya literasi digital di kalangan masyarakat dan pelaku industri. Penelitian ini merekomendasikan penguatan kelembagaan, audit kepatuhan berkala, peningkatan literasi digital, dan harmonisasi regulasi antar sektor sebagai langkah strategis untuk memperkuat perlindungan data pribadi di sektor perbankan. Perlindungan data bukan hanya aspek teknis, tetapi juga bentuk konkret dari penghormatan terhadap hak privasi sebagai bagian dari hak asasi manusia.*

**Sejarah Artikel**
Submitted: 21 Mei 2025
Accepted: 24 Mei 2025
Published: 25 Mei 2025

**Kata Kunci**
*Perlindungan data pribadi, bank, UU PDP, sanksi administratif, keamanan digital*

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 90-97

**Pendahuluan**

Kebocoran data nasabah, baik melalui serangan siber maupun kelalaian internal, menjadi tantangan besar dalam era digital ini. Contohnya, serangan LockBit 3.0 terhadap Bank Syariah Indonesia (BSI) pada Mei 2023 menyebabkan lebih dari 15 juta data pribadi nasabah bocor dan berdampak besar pada kepercayaan publik terhadap sistem perbankan(Raudhin Zulfikar et al., 2024). Selain itu, kasus pembobolan rekening oleh pegawai Bank Jago juga menunjukkan lemahnya pengawasan internal dan pelanggaran terhadap kerahasiaan data pribadi (Wicaksana et al., 2024). Perkembangan teknologi digital dalam sektor perbankan telah mengubah secara fundamental cara masyarakat mengakses dan menggunakan layanan keuangan. Di Indonesia, pertumbuhan digitalisasi perbankan meningkat pesat seiring adopsi mobile banking dan digital banking yang menjangkau masyarakat luas secara real time dan efisien (Yuspin et al., 2023). Namun, di balik kemudahan tersebut, muncul pula risiko signifikan terhadap keamanan data pribadi nasabah, khususnya data yang berkaitan dengan rekening perbankan.

Dalam konteks hukum, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menegaskan bahwa bank memiliki kewajiban menjaga kerahasiaan data nasabah sebagai bentuk perlindungan hukum dan etika perbankan. Namun, transformasi digital menuntut pembaruan dan penguatan regulasi karena praktik pengelolaan data di era digital jauh lebih kompleks dan rentan (Sibagariang & Parhusip, 2024). Untuk itu, hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam memberikan kepastian hukum terhadap perlindungan data di berbagai sektor, termasuk perbankan. UU PDP memberikan dasar hukum yang kuat dalam mengatur hak subjek data, kewajiban pengendali data, serta jenis-jenis sanksi administratif dan pidana atas pelanggaran data pribadi (Agustina & Wiraguna, 2025). Dalam konteks perbankan, bank dikategorikan sebagai pengendali data yang wajib menerapkan langkah-langkah teknis dan administratif untuk melindungi data pribadi yang mereka kelola. Pelanggaran terhadap ketentuan ini dapat berakibat pada pemberian sanksi administratif berupa teguran, denda administratif, penghentian sementara pemrosesan data, bahkan pencabutan izin operasional bank (Syarifah et al., 2024).

Namun demikian, pelaksanaan sanksi administratif di sektor perbankan masih menghadapi berbagai tantangan. Salah satunya adalah lemahnya pengawasan dari otoritas terkait seperti Otoritas Jasa Keuangan (OJK), serta minimnya literasi digital di kalangan masyarakat dan bahkan pelaku industri sendiri (Rifa & Hidayati, 2024). Banyak bank belum sepenuhnya mematuhi ketentuan Pasal 20 dan 21 UU PDP, yang mengharuskan adanya persetujuan eksplisit dan pemberian informasi menyeluruh kepada nasabah sebelum data mereka diproses (Syarifah et al., 2024). Selain faktor internal, tantangan eksternal berupa lemahnya koordinasi antar lembaga pengawas, terbatasnya wewenang penyelesaian sengketa non-litigasi oleh otoritas pengawas data, dan ketentuan waktu yang tidak adaptif dengan corak bisnis masing-masing sektor turut memperumit implementasi perlindungan hukum secara efektif (Rifa & Hidayati, 2024). Bahkan, dalam banyak kasus, bank tidak memiliki standar keamanan digital yang memadai, sehingga rawan menjadi target kejahatan siber, terutama dengan berkembangnya metode peretasan yang semakin canggih (Agustina & Wiraguna, 2025).

Fenomena kebocoran data nasabah tidak hanya merugikan individu, tetapi juga merusak reputasi institusi keuangan dan menurunkan tingkat kepercayaan masyarakat terhadap sistem perbankan. Hal ini berdampak sistemik pada stabilitas sektor keuangan nasional. Oleh karena itu, perlindungan data nasabah bukan hanya menjadi isu teknis, tetapi juga menyangkut aspek hak asasi manusia, khususnya hak atas privasi sebagaimana diatur dalam Pasal 28G ayat (1) UUD 194

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 90-97

(Agustina & Wiraguna, 2025) 5. Hak atas privasi menjadi landasan moral dan hukum bagi negara untuk memberikan jaminan perlindungan yang kuat bagi warganya dalam era digital.

Tujuan dari penelitian ini adalah untuk menganalisis bentuk tanggung jawab hukum dan penerapan sanksi administratif terhadap bank yang terbukti lalai dalam menjaga keamanan data rekening nasabah. Penelitian ini menekankan pentingnya implementasi ketentuan UU PDP dan Undang-Undang Perbankan secara konsisten, serta menilai efektivitas mekanisme pengawasan dan penegakan hukum yang tersedia.

**Metode Penelitian**

Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan yang menelaah norma hukum positif melalui studi terhadap peraturan perundang-undangan, literatur hukum, dan putusan-putusan yang relevan (Sidi Ahyar, 2025). Metode ini dipilih karena fokus utama penelitian adalah menganalisis tanggung jawab hukum bank serta penerapan sanksi administratif dalam kasus kegagalan melindungi data rekening nasabah. Dengan menggabungkan pendekatan perundang-undangan dan konseptual, penelitian ini bertujuan memberikan pemahaman komprehensif terhadap mekanisme perlindungan hukum atas data pribadi nasabah dalam sektor perbankan.

Sumber data yang digunakan adalah data sekunder berupa bahan hukum tertulis, seperti Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain itu, ditelusuri pula peraturan pelaksana seperti ketentuan dari Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), untuk mengetahui bagaimana regulasi tersebut diterapkan dalam praktik. Penelitian ini diharapkan mampu menjelaskan kedudukan hukum bank sebagai pengendali data serta mengkaji efektivitas sanksi administratif dalam memberikan perlindungan terhadap data nasabah.

**Hasil Dan Pembahasan**

**A. Tanggung Jawab Bank Dalam Perlindungan Data Rekening Nasabah**

Tanggung jawab bank dalam melindungi data rekening nasabah diatur secara eksplisit dalam berbagai regulasi nasional. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menetapkan bahwa bank wajib merahasiakan keterangan nasabahnya yang disimpan baik secara manual maupun digital. Kewajiban menjaga kerahasiaan ini merupakan bagian dari prinsip kehati-hatian dan perlindungan konsumen dalam industri perbankan (Sibagariang & Parhusip, 2024). Perlindungan terhadap data pribadi nasabah menjadi semakin penting seiring dengan berkembangnya digitalisasi perbankan. Saat ini, hampir seluruh transaksi dan layanan perbankan dapat diakses melalui platform digital, sehingga data nasabah tidak hanya terdiri dari data identitas, tetapi juga data biometrik, data transaksi, dan data perilaku pengguna aplikasi perbankan (Syarifah et al., 2024).

Dalam konteks Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, bank dikategorikan sebagai pengendali data. Sebagai pengendali data, bank memiliki kewajiban administratif dan teknis yang ketat. Pasal 20 UU PDP mengatur bahwa pengendali data wajib mendapatkan persetujuan eksplisit dari subjek data sebelum memproses data pribadi. Sementara itu, Pasal 21 mewajibkan pengendali data untuk memberikan informasi secara lengkap kepada subjek data mengenai tujuan pengumpulan data, jangka waktu penyimpanan, jenis data yang dikumpulkan, serta hak-hak subjek data (Syarifah et al., 2024). Kewajiban teknis ini mencakup penerapan sistem keamanan siber, enkripsi data, dan pembatasan akses internal yang

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 90-97

ketat. Namun, dalam praktiknya, masih banyak bank yang belum sepenuhnya mematuhi ketentuan ini. Kelalaian dalam menjalankan kewajiban tersebut membuka celah terjadinya kebocoran data dan menjadi dasar pemberian sanksi administratif (Wyanda Kinanti Syauqi Ramadhani, 2025).

**B. Bentuk Kegagalan Bank dalam Melindungi Data Nasabah**

Kegagalan bank dalam melindungi data nasabah dapat terjadi baik karena serangan eksternal maupun kelalaian internal. Dua kasus menonjol yang mencerminkan kondisi ini adalah insiden yang dialami oleh Bank Syariah Indonesia (BSI) dan Bank Jago pada tahun 2023.

Kasus pertama menimpa BSI yang menjadi korban serangan siber oleh kelompok peretas internasional LockBit 3.0. Serangan ini berhasil membobol sistem digital BSI dan mencuri lebih dari 15 juta data pribadi nasabah, termasuk nama, alamat, nomor rekening, serta histori transaksi (Raudhin Zulfikar et al., 2024). Hasil penyelidikan mengungkap bahwa BSI tidak memiliki sistem pertahanan berlapis (*multi-layered defense*) yang memadai dan gagal melakukan pembaruan sistem keamanan secara berkala. Kelalaian ini jelas merupakan pelanggaran terhadap prinsip-prinsip dalam Undang-Undang Perlindungan Data Pribadi, khususnya mengenai kewajiban pengendali data untuk memberikan perlindungan optimal terhadap data pribadi (Elda Septi Darmayanti, 2025).

Sementara itu, kasus kedua terjadi di Bank Jago, di mana kebocoran data justru disebabkan oleh pihak internal. Seorang pegawai diketahui menyalahgunakan aksesnya untuk membuka dan menjual data nasabah kepada pihak ketiga tanpa izin. Kasus ini menunjukkan lemahnya pengawasan internal serta tidak diterapkannya prinsip *least privilege*, yaitu pembatasan akses sesuai dengan kebutuhan kerja pegawai. Kondisi ini mencerminkan kegagalan manajerial dalam mengendalikan risiko internal serta pelanggaran terhadap prinsip perlindungan data pribadi sebagaimana diatur dalam UU PDP (Wicaksana et al., 2024).

Dari kedua kasus tersebut dapat disimpulkan bahwa bentuk kegagalan bank dalam melindungi data nasabah tidak hanya disebabkan oleh serangan dari luar, tetapi juga oleh lemahnya tata kelola internal dan ketidakpatuhan terhadap protokol keamanan. Baik pelanggaran oleh pihak eksternal seperti peretas, maupun oleh pegawai internal yang menyalahgunakan kewenangan, menunjukkan bahwa perlindungan data nasabah belum dijalankan secara maksimal oleh institusi perbankan, dan menandakan pelanggaran terhadap ketentuan hukum yang berlaku.

**C. Ketentuan Sanksi Administratif dalam UU PDP**

UU PDP secara tegas mengatur sanksi administratif sebagai instrumen penegakan hukum terhadap pengendali data yang lalai dalam menjalankan kewajibannya. Pasal 57 UU PDP mengatur jenis sanksi administratif yang dapat dikenakan, yaitu:

1. Teguran tertulis,
2. Penghentian sementara kegiatan pengolahan data,
3. Penghapusan atau pemusnahan data pribadi,
4. Denda administratif hingga 2% dari pendapatan tahunan,
5. Pencabutan izin operasional.

Sanksi administratif ini diterapkan apabila ditemukan pelanggaran terhadap prinsip pemrosesan data pribadi, seperti tidak adanya persetujuan eksplisit, pengumpulan data tanpa tujuan yang sah, atau tidak adanya sistem pengamanan data (Agustina & Wiraguna, 2025). Dalam kasus BSI dan Bank Jago, pelanggaran-pelanggaran ini sangat jelas terjadi, sehingga seharusnya menjadi dasar pemberian sanksi administratif. Namun, implementasi sanksi ini menghadapi banyak kendala. Otoritas yang diberikan kepada lembaga pengawas seperti Kementerian Komunikasi dan Informatika belum sepenuhnya optimal. Selain itu, belum adanya lembaga

ISSN: 3032-7482
(2025), 2 (2): 90-97

independen yang secara khusus menangani sengketa data pribadi juga membuat pemberian sanksi administratif menjadi tidak maksimal (Rifa & Hidayati, 2024).

**D. Tantangan dan Evaluasi Implementasi Sanksi Administratif**

Sebelum hadirnya UU PDP, perlindungan data pribadi di Indonesia bersifat sektoral dan terfragmentasi. Hal ini menyebabkan ketidakkonsistenan dalam pelaksanaan perlindungan data dan lemahnya koordinasi antar lembaga. Regulasi seperti UU ITE dan Peraturan OJK hanya mengatur sebagian kecil dari prinsip-prinsip perlindungan data, tanpa memiliki kekuatan eksekusi yang kuat terhadap pelanggaran administratif (Rifa & Hidayati, 2024). Rendahnya literasi digital di kalangan pelaku industri perbankan dan masyarakat juga menjadi hambatan utama. Banyak nasabah yang tidak memahami hak-hak mereka atas data pribadi, sementara bank sering kali menganggap perlindungan data sebagai beban operasional daripada investasi jangka panjang (Khetrina Maria Angnesia, 2025). Ketiadaan lembaga pengawas yang independen dan berwenang untuk menyelesaikan sengketa secara administratif membuat mekanisme penyelesaian pelanggaran menjadi lemah. Sebagian besar penyelesaian masih bergantung pada mekanisme pengadilan, yang memakan waktu dan biaya tinggi, serta tidak responsif terhadap dinamika teknologi yang berkembang cepat (Rifa & Hidayati, 2024).

Dari seluruh uraian di atas, jelas bahwa tanggung jawab bank dalam melindungi data nasabah tidak hanya bersifat normatif, tetapi juga menyangkut aspek teknis dan kelembagaan. Ketika kewajiban ini tidak dijalankan, maka negara melalui perangkat hukumnya berhak memberikan sanksi administratif demi menegakkan keadilan dan melindungi kepentingan konsumen. Sebagai penutup bagian ini, diperlukan sinergi antara regulator, pelaku industri perbankan, dan masyarakat dalam menciptakan sistem perlindungan data yang efektif. Perluasan kewenangan lembaga pengawas, penguatan pengawasan internal bank, serta peningkatan literasi digital publik merupakan langkah-langkah yang mendesak untuk segera diimplementasikan.

**E. Refleksi Teoritis dan Dampak Jangka Panjang**

Jika ditinjau dari perspektif teori hukum perlindungan konsumen dan hak atas privasi sebagai bagian dari hak asasi manusia, kegagalan bank dalam melindungi data pribadi nasabah merupakan bentuk pelanggaran terhadap dua prinsip utama: *the right to be left alone* dan *the right to control personal information*. Pelanggaran ini juga dapat berimplikasi pada hilangnya kontrol individu atas data mereka sendiri, yang dalam konteks perbankan dapat menyebabkan kerugian ekonomi, pemerasan digital, hingga pencurian identitas (Berto Purnomo Sidik, 2025).

Kerugian yang timbul akibat kebocoran data tidak hanya dialami nasabah sebagai pihak individu. Reputasi bank sebagai institusi juga mengalami degradasi, yang pada gilirannya mempengaruhi stabilitas dan kepercayaan terhadap sistem perbankan nasional. Dalam kondisi lebih ekstrem, penarikan dana besar-besaran dapat terjadi karena kepanikan publik terhadap sistem keamanan data bank yang dianggap tidak memadai. Dalam jangka panjang, kondisi ini akan memengaruhi kredibilitas lembaga keuangan dan menurunkan indeks kepercayaan publik terhadap sektor perbankan (Yuspin et al., 2023).

Dari sisi regulasi, keberadaan UU PDP menjadi landasan penting, namun belum cukup. Dibutuhkan harmonisasi antara UU PDP dengan regulasi sektoral seperti UU Perbankan, POJK Perlindungan Konsumen, dan UU ITE agar tidak terjadi konflik norma maupun tumpang tindih kewenangan antar lembaga penegak. Sinkronisasi ini akan menciptakan sistem hukum yang lebih kohesif dan mampu menjawab tantangan perkembangan teknologi finansial secara dinamis (Rifa & Hidayati, 2024).

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 90-97

**F. Rekomendasi Penerapan dan Reformasi Kebijakan**

Berdasarkan hasil analisis dan evaluasi yang telah diuraikan, berikut beberapa rekomendasi praktis yang dapat diajukan untuk memperkuat sistem perlindungan data nasabah di sektor perbankan:

1. **Penguatan Kelembagaan**: Dibentuknya lembaga otoritatif independen yang secara khusus menangani perlindungan data pribadi dan diberi kewenangan untuk melakukan penyelesaian sengketa secara administratif, menjatuhkan sanksi, serta mengawasi praktik pengendalian data oleh bank dan lembaga keuangan.
2. **Audit Kepatuhan Berkala**: Diberlakukannya audit keamanan siber dan kepatuhan terhadap UU PDP secara berkala di semua institusi perbankan yang dilakukan oleh pihak independen yang terakreditasi.
3. **Standarisasi Teknologi Perlindungan Data**: Pemerintah dan OJK perlu merumuskan standar minimal infrastruktur keamanan data yang wajib dipenuhi oleh seluruh bank di Indonesia, termasuk sistem enkripsi, sistem login dua faktor, dan disaster recovery system.
4. **Edukasi Literasi Digital**: Penyelenggaraan program nasional literasi digital untuk nasabah dan pegawai bank secara periodik. Hal ini penting agar masyarakat sadar akan haknya sebagai subjek data dan dapat bertindak apabila terjadi pelanggaran.
5. **Integrasi Sistem Pelaporan dan Tindak Lanjut**: Sistem pelaporan insiden kebocoran data harus disederhanakan dan terintegrasi dengan pusat komando siber nasional. Ini akan mempercepat respons terhadap pelanggaran dan meningkatkan kecepatan pemulihan.
6. **Peningkatan Sanksi**: Perlu adanya peninjauan ulang terhadap besaran denda administratif dalam UU PDP agar menimbulkan efek jera, khususnya bagi bank besar yang memiliki kapitalisasi tinggi.
7. **Perlindungan Khusus Data Sensitif**: Data biometrik dan data keuangan harus dikategorikan sebagai data sensitif dengan lapisan perlindungan tambahan. Pemrosesan jenis data ini wajib melewati proses verifikasi ganda dan persetujuan eksplisit dengan pemahaman penuh dari nasabah.

**Kesimpulan**

Dalam era digital yang terus berkembang, bank memegang peran yang sangat penting dalam menjaga kepercayaan masyarakat terhadap sistem keuangan. Salah satu bentuk tanggung jawab tersebut adalah kewajiban untuk melindungi data pribadi nasabah, termasuk informasi rekening dan data biometrik yang kini banyak digunakan dalam layanan perbankan digital (Syarifah et al., 2024). Kewajiban hukum ini telah diatur dengan tegas dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang mewajibkan setiap bank untuk merahasiakan dan menjaga keamanan data nasabah yang mereka kelola (Sibagariang & Parhusip, 2024).

Seiring berjalannya waktu, kompleksitas data yang dikelola bank dan ancaman terhadap keamanannya meningkat drastis, terutama karena penggunaan teknologi digital dan kemunculan layanan perbankan berbasis aplikasi. Untuk menjawab tantangan ini, hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi titik krusial dalam memperkuat fondasi hukum perlindungan data di Indonesia. UU ini menetapkan tanggung jawab pengendali data, dalam hal ini bank, untuk memperoleh persetujuan eksplisit dari subjek data serta menyediakan informasi lengkap mengenai penggunaan data tersebut (Syarifah et al., 2024).

Dalam praktiknya, pelaksanaan sanksi administratif terhadap pelanggaran perlindungan data pribadi oleh bank belum menunjukkan efektivitas yang optimal. Meskipun regulasi telah

ISSN: 3032-7482
(2025), 2 (2): 90-97

dirumuskan secara komprehensif dan mencakup berbagai jenis sanksi administratif mulai dari teguran tertulis hingga pencabutan izin usaha Agustina & Wiraguna (2025), implementasinya masih menghadapi kendala serius. Hambatan terbesar terletak pada lemahnya infrastruktur pengawasan, kurangnya koordinasi antar lembaga, serta rendahnya kapasitas teknis aparat penegak hukum dalam menangani kejahatan siber (Rifa & Hidayati, 2024).

Kasus serangan siber terhadap Bank Syariah Indonesia (BSI) dan pembobolan rekening oleh pegawai Bank Jago menjadi bukti nyata dari kegagalan bank dalam menjalankan kewajiban perlindungan data. Dalam kasus BSI, lebih dari 15 juta data pribadi nasabah bocor akibat lemahnya sistem keamanan internal, sementara pada kasus Bank Jago terjadi penyalahgunaan wewenang oleh pihak internal yang berdampak langsung pada kerugian nasabah (Raudhin Zulfikar et al., 2024; Wicaksana et al., 2024).

Permasalahan lain yang turut memperlemah perlindungan data adalah belum adanya lembaga pengawas independen yang memiliki otoritas penuh untuk menyelesaikan sengketa administratif terkait pelanggaran data pribadi. Selain itu, tingkat literasi digital yang masih rendah di kalangan masyarakat membuat banyak nasabah tidak menyadari hak-haknya atas data pribadi mereka sendiri (Yuspin et al., 2023).

Untuk itu, perlindungan data dalam industri perbankan tidak bisa hanya mengandalkan regulasi yang telah ada, melainkan harus dibarengi dengan penegakan hukum yang konsisten dan kolaborasi antar lembaga pengawas yang kuat. Reformasi kelembagaan, penguatan audit internal, serta edukasi publik menjadi langkah strategis yang perlu diambil secara simultan guna memastikan bahwa hak privasi nasabah benar-benar terlindungi dan dijamin oleh hukum (Agustina & Wiraguna, 2025).

Sebagai penutup, dapat ditegaskan bahwa perlindungan data pribadi di sektor perbankan merupakan bentuk konkret dari penghormatan terhadap hak asasi manusia, khususnya hak atas privasi. Bank sebagai pengendali data memiliki tanggung jawab tidak hanya secara hukum, tetapi juga secara etis dan sosial. Kegagalan dalam menjalankan tanggung jawab ini tidak hanya berdampak pada individu, tetapi juga pada kepercayaan publik terhadap sistem keuangan nasional secara keseluruhan. Oleh karena itu, penegakan hukum yang konsisten, transparan, dan adil merupakan kebutuhan mendesak dalam menjamin keamanan data rekening nasabah di Indonesia (Wildan et al., 2024).

**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.

Elda Septi Darmayanti, S. A. (2025). Tanggung jawab hukum pinjaman online terhadap penyebaran data nasabah secara ilegal. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 233-251.

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.

Sidi Ahyar, w. (2025). EKSPLORASI METODE PENELITIAN DENGAN PENDEKATAN NORMATIF DAN EMPIRIS DALAM PENELITIAN HUKUM DI INDONESIA. *LEX JURNALICA*, 66-72.

ISSN: 3032-7482
(2025), 2 (2): 90-97

Wyanda Kinanti Syauqi Ramadhani, S. A. (2025). Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan. *Perspektif Administrasi Publik dan hukum*, 158-175.

Agustina, W., & Wiraguna, S. A. (2025). Upaya perlindungan hukum hak privasi terhadap data pribadi dari kejahatan peretasan. *Media Hukum Indonesia*, 2(6), 117–127. https://doi.org/10.5281/zenodo.15486554

Fauzi, R., & Hidayati, M. N. (2024). Kebijakan penal dalam perlindungan data pribadi nasabah fintech lending di Indonesia. *Binamulia Hukum*, 13(2), 461–481. https://doi.org/10.37893/jbh.v13i2.964

Sibagariang, D. N., & Parhusip, N. A. (2024). Peran dan efektivitas undang-undang perbankan dalam memberikan perlindungan hukum bagi korban pembobolan rekening di Indonesia. *Jurnal Multidisiplin Ilmu Akademik*, 1(6), 77–82. https://doi.org/10.61722/jmia.v1i6.2854

Syarifah, A., Ananda, A., Azzahra, Z., Rakhmawati, C. S., & Nurjihad. (2023). Implikasi Pasal 20 dan 21 Undang Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi terhadap Bank dalam Pemrosesan Data Biometrik Nasabah. *Prosiding Nasional Hukum Aktual*, 481–482

Wildan, M., Ramadhan, D. R. C., & Wijayanti, Z. R. (2024). Analisis tanggung jawab bank terhadap kebocoran data nasabah: Ditinjau dalam perspektif hukum perbankan. *Media Hukum Indonesia*, 2(4), 392–397. https://doi.org/10.5281/zenodo.14201758

Wicaksana, D. H., Ramadhan, N. R., Ramadhan, A. R., Winata, H., & Ardian, M. F. (2024). Analisis tinjauan yuridis terhadap pembobolan rekening bank digital yang dilakukan pegawai bank: Studi kasus Bank Jago 2023. *Media Hukum Indonesia*, 2(4), 515–522. https://doi.org/10.5281/zenodo.14220517

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal data protection law in digital banking governance in Indonesia. *Studia Iuridica Lublinensia*, 32(1), 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130

Zulfikar, F. R., & Harley, A. B. M. (2023). Analisis hukum dalam kasus serangan siber pada Bank Syariah Indonesia (BSI). *Media Hukum Indonesia*, 2(4), 501–504. https://doi.org/10.5281/zenodo.14216236