Jurnal Cendekia Hukum Indonesia
Vol. 2 No. 1 April 2026

DOI: https://doi.org/10.71417/jchi.v2i1.190
https://hukum.journalpustakacendekia.com/index.php/JCHI

Perlindungan Data Pribadi Nasabah pada Layanan *Mobile Banking* di Indonesia

Indana Zulfa Hasanah
Universitas Negeri Semarang

Eka Ayu Safitri
Universitas Negeri Semarang

Linda Stianingrum
Universitas Negeri Semarang

Nayla Fikasari
Universitas Negeri Semarang

Baidhowi
Universitas Negeri Semarang

Alamat: Jalan Kolonel HR. Hadijanto, Sekaran, Gunungpati, Kota Semarang, Jawa Tengah 50229, Indonesia.
Korespondensi penulis: inzuha001@students.unnes.ac.id

Abstract. *The rapid growth of mobile banking services in Indonesia enhances financial inclusion but heightens cybersecurity risks, particularly data breaches exposing customer personal information. This study aims to analyze legal frameworks for customer data protection in mobile banking, bank responsibilities, and legal remedies for breaches. Employing normative juridical research with statute and conceptual approaches, the population includes relevant laws from 2021-2025, purposively sampled as UU PDP, UU ITE, and OJK regulations like POJK No. 11/POJK.03/2022. Instruments comprise primary and secondary legal materials analyzed qualitatively via deductive descriptive methods. Findings reveal comprehensive regulations mandating explicit consent, technical security, and banks' preventive-repressive duties, yet implementation gaps persist due to third-party partnerships. In conclusion, while frameworks exist, harmonization and enforcement are needed for robust protection, with customers accessing OJK complaints, LAPS SJK mediation, or civil suits.*

Keywords: *Data Protection, Legal Framework, Mobile Banking, Personal Data, Zakat Profession*

Abstrak. Perkembangan pesat layanan mobile banking di Indonesia meningkatkan inklusi keuangan namun memunculkan risiko keamanan siber, khususnya kebocoran data pribadi nasabah. Penelitian ini bertujuan menganalisis pengaturan hukum perlindungan data pribadi nasabah, tanggung jawab bank, dan upaya hukum atas kebocoran data. Menggunakan penelitian yuridis normatif dengan pendekatan perundang-undangan dan konseptual, populasi mencakup peraturan 2021-2025, disampel secara purposif seperti UU PDP, UU ITE, serta POJK No. 11/POJK.03/2022. Instrumen terdiri dari bahan hukum primer-sekunder dianalisis secara kualitatif deskriptif deduktif. Hasil menunjukkan regulasi komprehensif yang mewajibkan persetujuan eksplisit, keamanan teknis, dan kewajiban preventif-represif bank, tetapi terdapat

Received Maret 25, 2026; Revised Maret 28, 2026; Accepted Maret 28, 2026
*Corresponding author, e-mail address

kesenjangan implementasi akibat kemitraan pihak ketiga. Kesimpulannya, meski kerangka hukum ada, harmonisasi dan penegakan diperlukan untuk perlindungan optimal, dengan nasabah memanfaatkan pengaduan OJK, mediasi LAPS SJK, atau gugatan perdata.

Kata kunci: Data Protection, Legal Framework, Mobile Banking, Personal Data, Zakat Profession

LATAR BELAKANG

Perkembangan pesat layanan perbankan digital, khususnya mobile banking, telah membawa kemudahan transaksi finansial sekaligus risiko keamanan siber yang signifikan bagi nasabah di Indonesia. Teknologi informasi canggih yang diadopsi bank meningkatkan efisiensi dan inklusi keuangan, tetapi juga mengekspos data pribadi nasabah, mulai dari identitas hingga riwayat transaksi elektronik, terhadap ancaman penyalahgunaan atau kebocoran (Fitriani et al., 2024; Setyowati & Kurniawan, 2023). Kolaborasi antara pemerintah, regulator seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), bank, serta masyarakat menjadi kunci untuk membangun ekosistem mobile banking yang aman, di mana kepercayaan nasabah bergantung pada pengelolaan data yang ketat (Pratiwi et al., 2022; Fitriani et al., 2024).

Layanan keuangan digital yang rumit menuntut dukungan regulasi hukum yang kuat untuk melindungi hak konsumen dan menjaga keandalan sistem, terutama di tengah kemitraan bank dengan pihak ketiga seperti fintech dan penyedia cloud. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menempatkan bank sebagai pengendali data yang bertanggung jawab atas keamanan, keakuratan, dan kerahasiaan informasi nasabah, meskipun implementasinya masih parsial di lembaga perbankan (Sitanggang et al., 2025; Nugroho & Santoso, 2024). Bank Indonesia menekankan perlunya regulasi teknis pendukung UU PDP untuk sektor jasa keuangan, guna mengantisipasi ancaman yang semakin kompleks (Wardhono et al., 2024; Hidayat & Rahman, 2023).

Risiko kebocoran data semakin meningkat akibat kolaborasi dengan mitra eksternal, di mana perjanjian kerjasama harus mengatur prinsip perlindungan data secara ketat untuk mencegah penyalahgunaan. Peneliti menyoroti bahwa pengawasan regulator yang lebih kuat, harmonisasi peraturan lintas sektor, dan edukasi literasi data bagi masyarakat merupakan langkah strategis untuk menjaga kepercayaan publik pada perbankan digital (Aziz & Zaidan, 2025; Sari & Pratama, 2022). Tanpa penguatan ini, eksposur nasabah terhadap serangan siber akan terus membesar, sebagaimana terlihat pada kasus kebocoran data di platform fintech baru-baru ini (Kurniawan et al., 2024; Aziz & Zaidan, 2025).

Artikel ini bertujuan untuk menganalisis pengaturan hukum perlindungan data pribadi nasabah dalam layanan mobile banking di Indonesia serta bentuk tanggung jawab bank dan upaya hukum bagi nasabah atas kebocoran data. Urgensi penelitian ini muncul dari ketidakoptimalan implementasi UU PDP dan regulasi pendukungnya, yang masih belum selaras dengan dinamika ancaman siber terkini, sehingga diperlukan penguatan kebijakan untuk melindungi inklusi finansial nasional (Sitanggang et al., 2025; Wardhono et al., 2024). Kebaruan penelitian terletak pada pendekatan integratif yang menggabungkan analisis regulasi PDP dengan kasus kemitraan pihak ketiga, memberikan rekomendasi harmonisasi hukum yang belum banyak dieksplorasi dalam literatur terkini (Aziz & Zaidan, 2025; Fitriani et al., 2024).

METODE PENELITIAN

Jenis dan Metode Penelitian

Penelitian ini menggunakan jenis penelitian yuridis normatif yang menekankan studi terhadap norma-norma hukum tertulis sebagai sumber data utama untuk mengungkap pengaturan perlindungan data pribadi nasabah pada layanan mobile banking di Indonesia. Metode yuridis normatif dipilih karena memungkinkan analisis mendalam terhadap hierarki peraturan perundang-undangan seperti Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik (UU ITE) beserta perubahannya, serta Undang-Undang No. 10 Tahun 1998 tentang Perbankan, yang menjadi dasar hukum utama dalam konteks judul penelitian "Perlindungan Data Pribadi Nasabah pada Layanan Mobile Banking di Indonesia" (Sitanggang et al., 2025; Sugiyono, 2023). Pendekatan yang diterapkan mencakup pendekatan perundang-undangan (statute approach) untuk menguraikan regulasi sektoral seperti Peraturan Otoritas Jasa Keuangan (POJK) terkait keamanan data, serta pendekatan konseptual (conceptual approach) guna mengeksplorasi prinsip-prinsip hukum seperti kerahasiaan bank dan tanggung jawab pengendali data (Wardhono et al., 2024; Creswell & Creswell, 2023). Pendekatan ini selaras dengan latar belakang penelitian yang menyoroti risiko kebocoran data akibat kolaborasi dengan pihak ketiga, sehingga memastikan analisis yang komprehensif dan kontekstual terhadap fenomena perbankan digital (Fitriani et al., 2024; Emzir, 2022).

Instrumen dan Teknik Analisis Data

Instrumen penelitian terdiri dari bahan hukum primer seperti undang-undang dan peraturan OJK, bahan hukum sekunder berupa jurnal, buku, serta laporan resmi Bank Indonesia, dan bahan hukum tersier seperti kamus hukum serta literatur pendukung yang dikumpulkan melalui studi kepustakaan. Teknik pengumpulan data dilakukan secara sistematis dengan pencarian dokumen hukum terkini dari sumber terpercaya, di mana setiap bahan diidentifikasi berdasarkan relevansi dengan rumusan masalah mengenai pengaturan hukum dan tanggung jawab bank atas kebocoran data (Aziz & Zaidan, 2025; Sudaryono, 2023). Analisis data menggunakan metode kualitatif deskriptif dengan penarikan kesimpulan deduktif, yaitu menguraikan norma umum ke kasus khusus layanan mobile banking, termasuk interpretasi prinsip-prinsip UU PDP seperti persetujuan eksplisit dan sanksi pidana (Irmawati et al., 2024; Sugiyono, 2023). Teknik ini melibatkan triangulasi sumber untuk validasi, memastikan temuan kohesif dengan urgensi penelitian seperti harmonisasi regulasi dan kebaruan analisis kemitraan pihak ketiga (Creswell & Creswell, 2023; Emzir, 2022).

Populasi dan Sampel

Populasi penelitian mencakup seluruh peraturan perundang-undangan, putusan pengadilan, serta dokumen kebijakan sektoral yang mengatur perlindungan data pribadi di sektor perbankan Indonesia sejak tahun 2021 hingga 2025, termasuk regulasi OJK dan Bank Indonesia yang relevan dengan mobile banking. Sampel dipilih secara purposif dengan kriteria inklusif, yaitu dokumen primer seperti UU PDP, UU ITE, POJK No. 11/POJK.03/2022, dan POJK No. 06/POJK.07/2022, serta sekunder seperti studi kasus kebocoran data dari literatur terkini, untuk merepresentasikan isu utama dalam latar belakang seperti implementasi parsial UU PDP dan risiko mitra eksternal (Sitanggang et al., 2025; Wardhono et al., 2024). Pemilihan sampel ini bersifat non-probability sampling yang tepat sasaran, memfokuskan pada norma-norma yang paling berpengaruh terhadap tanggung jawab preventif dan represif bank (Sudaryono, 2023; Fitriani et al., 2024).

Prosedur Penelitian

Prosedur penelitian dimulai dengan identifikasi masalah berdasarkan latar belakang fenomena risiko siber dan regulasi parsial, dilanjutkan pengumpulan data melalui studi pustaka dari database hukum nasional. Selanjutnya, data diorganisasi secara tematik sesuai rumusan masalah, dianalisis dengan pendekatan deduktif untuk menyusun temuan mengenai pengaturan hukum dan upaya hukum nasabah, kemudian divalidasi melalui interpretasi konseptual (Aziz & Zaidan, 2025; Emzir, 2022). Tahap akhir meliputi penyusunan kesimpulan dan saran yang kohesif, seperti penguatan pengawasan OJK, sesuai dengan tujuan penelitian untuk harmonisasi regulasi (Creswell & Creswell, 2023; Sugiyono, 2023).

HASIL DAN PEMBAHASAN

Pengaturan Hukum Mengenai Perlindungan Data Pribadi Nasabah pada Layanan *Mobile Banking* di Indonesia

1. Konsep Dan Ruang Lingkup Data Pribadi dalam Layanan *Mobile Banking*

Perkembangan digitalisasi sektor perbankan telah mengubah pola interaksi antara bank dan nasabah. Layanan *mobile banking* memungkinkan transaksi keuangan dilakukan tanpa kehadiran fisik di kantor bank. Efisiensi tersebut bergantung pada sistem elektronik yang memproses berbagai informasi pribadi nasabah. Penggunaan sistem digital yang intensif menjadikan data pribadi sebagai elemen sentral sekaligus rentan terhadap risiko penyalahgunaan.

Pengaturan mengenai perlindungan nasabah bank dalam sistem hukum nasional Indonesia tersebar dalam berbagai peraturan perundang-undangan. Beberapa regulasi yang relevan antara lain Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahan-perubahannya. Ketiga peraturan tersebut memberikan dasar hukum bagi perlindungan hak-hak nasabah, terutama yang berkaitan dengan keamanan transaksi dan penggunaan sistem elektronik di sektor perbankan (V. Sitanggang et al., 2025).

Data pribadi merujuk pada setiap informasi mengenai seseorang yang dapat mengidentifikasi atau membuat seseorang dapat diidentifikasi, baik secara langsung maupun melalui kombinasi data tertentu. Pengertian ini ditegaskan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengakui data pribadi sebagai bagian dari hak atas privasi warga negara. Regulasi tersebut membedakan data pribadi menjadi data yang bersifat umum dan data yang bersifat spesifik (sensitif), yang tingkat perlindungannya lebih tinggi.

Undang-Undang mengenai perlindungan data pribadi tidak hanya mengatur prinsip pengelolaan data, tetapi juga menetapkan sejumlah larangan beserta sanksi pidana bagi pelanggarannya. Ketentuan tersebut bertujuan memberikan perlindungan yang kuat terhadap hak privasi setiap individu dari tindakan penyalahgunaan data. Pertama, setiap orang dilarang memperoleh atau mengakses data pribadi milik orang lain secara melawan hukum dengan maksud untuk memperoleh keuntungan pribadi yang dapat menimbulkan kerugian bagi pihak lain. Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi pidana berupa penjara paling lama lima tahun dan/atau denda paling banyak lima miliar rupiah. Kedua, setiap orang juga dilarang mengungkapkan atau menyebarluaskan informasi yang berkaitan dengan data pribadi milik pihak lain tanpa hak atau tanpa persetujuan pemilik data. Perbuatan tersebut dapat dikenai ancaman pidana penjara paling lama empat tahun dan/atau pidana denda paling banyak empat miliar rupiah. Ketiga, penggunaan data pribadi milik orang lain secara tidak sah atau bertentangan dengan hukum juga termasuk perbuatan yang dilarang. Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi pidana berupa penjara paling lama lima tahun dan/atau denda paling banyak lima miliar rupiah (Irmawati et al., 2024).

Secara umum, data pribadi didefinisikan sebagai setiap informasi yang menyangkut identitas seseorang, baik yang dapat diidentifikasi secara langsung maupun tidak langsung melalui data kombinasi tertentu. Dalam pelayanan *mobile banking*, data pribadi mencakup identitas dasar nasabah (nama, alamat, NIK), data finansial (nomor rekening, histori transaksi, saldo), serta data autentikasi seperti PIN, sandi, dan data biometrik yang digunakan untuk otentikasi akses aplikasi bank (misalnya sidik jari atau pengenalan wajah) (Fitriani et al., 2024). Data-data ini menjadi bagian dari sistem informasi bank agar transaksi dapat dilakukan dengan aman dan akurat.

Kegiatan operasional *mobile banking* melibatkan proses pengumpulan, pencatatan, penyimpanan, pemanfaatan, hingga penghapusan data. Setiap tahapan tersebut berkaitan langsung dengan hak subjek data. Karakteristik layanan *mobile banking* yang berbasis aplikasi dan jaringan internet menyebabkan ruang lingkup data pribadi tidak hanya terbatas pada identitas konvensional, tetapi juga meluas pada data digital dan teknis (Rohendi & Kharisma, 2025).

Ruang lingkup data pribadi dalam mobile banking dapat dikelompokkan sebagai berikut:

A. **Informasi Identitas Dasar:** Meliputi data yang secara langsung mengidentifikasikan nasabah seperti nama lengkap, alamat, nomor telepon dan nomor identifikasi resmi (misalnya NIK). Data ini diperlukan untuk proses registrasi dan verifikasi nasabah.
B. **Data Finansial dan Transaksi:** Mencakup nomor rekening, histori transaksi, jumlah saldo, jenis rekening, serta informasi lain terkait aktivitas finansial nasabah yang diproses melalui aplikasi mobile banking. Keberadaan data ini penting untuk mencatat aktivitas sekaligus mencegah transaksi yang tidak sah.
C. **Data Autentikasi dan Keamanan Digital:** Meliputi PIN, kata sandi, OTP (one-time password), serta data biometrik yang digunakan untuk mengamankan akses layanan. Kategori ini dianggap sangat sensitif karena apabila jatuh ke tangan pihak yang tidak berwenang, risiko penyalahgunaan atau pembobolan rekening meningkat signifikan.
D. **Data Elektronik dan Jejak Digital:** Termasuk metadata perangkat seperti alamat IP, model perangkat, serta pola login. Informasi ini digunakan bank untuk memonitor perilaku transaksi dan mendeteksi aktivitas mencurigakan sebagai bagian dari strategi keamanan siber.

Pengelompokan tersebut menunjukkan bahwa cakupan data pribadi pada layanan *mobile banking* bersifat luas dan kompleks. Interaksi digital menghasilkan lapisan informasi yang saling berkaitan. Risiko kebocoran tidak hanya berdampak pada privasi, tetapi juga pada stabilitas sistem keuangan dan kepercayaan publik terhadap industri perbankan.

2. Dasar Hukum Perlindungan Data Pribadi di Indonesia

Perkembangan layanan *mobile banking* telah membuat masyarakat lebih mudah mengakses jasa keuangan kapan saja dan di mana saja. Namun, kehadiran teknologi baru ini juga menambah kompleksitas risiko keamanan data pelanggan (Fitriani et al., 2024). Data pribadi yang dimiliki bank (nama, alamat, rekening, biometrik, dsb.) menjadi aset berharga sekaligus rentan kebocoran atau penyalahgunaan. Untuk mewujudkan ekosistem mobile banking yang aman, diperlukan kejelasan aturan hukum yang memadukan perlindungan data pribadi dan perlindungan konsumen keuangan.

Pada tahun 2022 sampai 2023, sejumlah payung hukum baru mulai berlaku. UU No. 27 Tahun 2022 menanamkan kerangka perlindungan data komprehensif di semua sektor, termasuk perbankan. Selain itu, UU ITE masih relevan sebagai undang-undang tertua tentang transaksi elektronik. Di samping itu, Otoritas Jasa Keuangan (OJK) telah mengeluarkan beberapa peraturan yang mengatur perlindungan nasabah bank digital dan fintech. Kajian ini bertujuan memetakan aturan-aturan tersebut (terutama UU PDP, UU ITE, dan peraturan OJK) serta mengevaluasi penerapannya dalam konteks layanan mobile banking. Analisis mempertimbangkan kewajiban bank (sebagai pengendali data), persetujuan nasabah, mekanisme transfer lintas batas, keamanan teknis, dan prosedur pelaporan insiden. Hasil penelitian juga akan mengidentifikasi kesenjangan hukum dan tantangan implementasi, serta memberikan rekomendasi kebijakan dan praktik kepatuhan bagi pelaku perbankan untuk meningkatkan perlindungan data nasabah.

A. UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

UU PDP adalah regulasi nasional pertama yang khusus mengatur perlindungan data pribadi secara komprehensif. Ruang lingkupnya sangat luas: berlaku untuk *setiap orang* (perorangan/badan publik/organisasi internasional) yang melakukan pemrosesan data pribadi di wilayah hukum RI atau berdampak pada WNI di luar negeri (Aziz & Zaidan, 2025). Dengan diketoknya UU ini, data keuangan dan transaksi nasabah bank kini masuk kategori *data pribadi spesifik* yang dilindungi ketat (diatur dalam Pasal 4, misalnya data kesehatan, biometrik, dan data keuangan pribadi).

Pertama, ada prinsip-prinsip dalam pasal 16 undang-undang ini. Prinsip-prinsip tata kelola data mengarah pada standar internasional, mirip GDPR, antara lain: pengumpulan data dilakukan secara *terbatas, sah, dan transparan*, pemrosesan harus sesuai tujuan yang

dinyatakan, data diproses secara akurat dan mutakhir, keamanan dijamin dari akses atau pengungkapan ilegal, serta ada pemberitahuan tentang tujuan dan setiap *kegagalan* perlindungan (mis. insiden kebocoran). Setelah data tidak diperlukan lagi (masa retensi berakhir atau atas permintaan), data harus dihapus. Prinsip-prinsip lain meliputi akuntabilitas pengendali data dan hak-hak individu.

Kedua, UU PDP mengakui berbagai hak bagi nasabah sebagai subjek data. Contohnya, nasabah berhak memperoleh informasi tentang penggunaan datanya (Pasal 5), berhak memperbaiki atau memperbarui data yang keliru (Pasal 6), meminta akses salinan data (Pasal 7), menghapus data (Pasal 8), menarik persetujuan (Pasal 9), dan menolak pemrosesan otomatis tertentu (Pasal 10). Hak untuk mendapat ganti rugi atau kompensasi juga disebut dalam Pasal 12. Dengan demikian, bank sebagai pengendali wajib memberikan mekanisme bagi nasabah untuk mengeksekusi hak-hak tersebut sesuai regulasi.

Ketiga, UU PDP memerintahkan pengendali data (dalam hal ini bank) memastikan setiap pemrosesan data pribadi memiliki dasar hukum yang sah (misalnya persetujuan eksplisit Nasabah, atau pemenuhan kontrak). Pengendali juga wajib menjaga keamanan sistem dan data, melindungi kerahasiaan informasi, dan memastikan integritas data pelanggan. Secara khusus, bank harus memperoleh persetujuan eksplisit nasabah sebelum mengumpulkan atau memproses data mereka. Persetujuan tersebut harus penuh informasi (terinformasi), spesifik untuk tujuan yang dinyatakan, dan dapat ditarik kapan saja oleh nasabah. Di samping itu, ketika bekerjasama dengan pihak ketiga (misalnya fintech atau penyedia teknologi), bank wajib melakukan due diligence dan mengikat mereka dalam perjanjian tertulis yang mengatur perlindungan data. Dalam perjanjian ini, bank harus menetapkan hak dan kewajiban masing-masing, mekanisme audit keamanan, dan prosedur respons insiden (misalnya kompensasi jika terjadi kebocoran).

Keempat, sanksi pada pasal 67 sampai pasal 69. UU ini mengenakan sanksi tegas untuk pelanggaran. Secara pidana, setiap orang yang dengan sengaja dan melawan hukum memperoleh, mengungkapkan, atau menggunakan data pribadi milik orang lain dapat dipidana penjara hingga 4–5 tahun dan/atau denda hingga Rp4–5 miliar. Misalnya, Pasal 67 menyatakan penjara paling lama 5 tahun untuk pengumpulan ilegal data pribadi, Pasal 68 mengenakan 6 tahun penjara bagi pembuat data palsu untuk keuntungan sendiri. Terdapat juga sanksi administratif (peringatan tertulis, penghentian sementara, kewajiban menghapus data, denda) jika terjadi pelanggaran kewajiban pengendali. Dengan demikan, rezim hukuman PDP memberikan efek jera dan penegasan tanggung jawab hukum bagi pihak perbankan yang lalai.

B. UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Perubahannya

Meskipun dibuat lebih awal, UU ITE tetap merupakan payung hukum penting terkait data elektronik. UU ITE (diubah oleh UU No.19/2016) mendefinisikan data pribadi sebagai bagian dari hak privasi (p*rivacy rights*). Pasal 26 UU ITE menyatakan bahwa setiap penggunaan informasi melalui media elektronik yang menyangkut data pribadi seseorang harus mendapatkan persetujuan orang yang bersangkutan. Artinya, pemrosesan data nasabah melalui aplikasi mobile banking tidak boleh dilakukan tanpa izin eksplisit nasabah. Pelanggaran pasal ini memungkinkan nasabah menuntut ganti rugi (Pasal 26(2)). Selain itu, UU ITE juga memuat pasal-pasal tentang kejahatan siber (*access* tanpa hak, penyadapan, penipuan digital) yang dapat diterapkan jika terjadi manipulasi data nasabah.

C. Peraturan OJK terkait Perlindungan Nasabah dan Data Pribadi

Selain regulasi umum di atas, OJK mengeluarkan sejumlah peraturan sektoral yang menguatkan perlindungan data nasabah dalam konteks perbankan dan *fintech*. Beberapa di antaranya:

a. POJK No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital (sebelumnya *Fintech*): Peraturan ini mewajibkan bank dan lembaga jasa keuangan lain yang bermitra dengan penyedia teknologi finansial untuk membuat perjanjian tertulis terkait perlindungan data pribadi. Misalnya, Pasal 12(2) mengharuskan perjanjian kerjasama memuat hak dan kewajiban mengelola data, mekanisme audit TI pihak ketiga, serta penanganan insiden keamanan data. Dengan demikian, setiap transfer data nasabah kepada fintech (seperti *e-wallet, peer-to-peer lending*) harus diawasi melalui kontrak yang memastikan standar PDP terpenuhi.
b. POJK No. 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum: Peraturan terbaru ini menggantikan aturan lama terkait manajemen risiko TI di bank. Salah satu ketentuan pentingnya adalah bahwa data bank dan nasabah merupakan aset yang wajib dijamin keamanannya. Pasal 16 menegaskan bahwa bank wajib mengamankan informasi secara efektif, menjaga kerahasiaan, integritas, dan ketersediaan data nasabah. Lampiran terkait menyebutkan bahwa meski *front-end global* diperbolehkan (mis. aplikasi internasional), back-end yang memproses data individu dan transaksi nasabah harus ditempatkan di Indonesia. Ini mengatur transfer lintas batas: bank mobile banking tidak boleh menyimpan data inti nasabah di luar negeri kecuali memenuhi persyaratan regulasi (mis. izin otoritas). Peraturan ini juga mengimplikasikan kewajiban audit independen, *backup*, dan *Disaster Recovery Plan* bagi sistem *mobile banking*.
c. POJK No. 06/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan: Meskipun berfokus pada keseluruhan jasa keuangan, POJK ini secara eksplisit menyebut perlindungan data pribadi konsumen. Pasal 11 melarang penyelenggara jasa keuangan memberikan data/informasi pribadi konsumen kepada pihak lain tanpa izin. Penelitian Amandha dan Yuspin (2024) menunjukkan bahwa dalam konteks kebocoran data nasabah Bank Syariah Indonesia, POJK ini digunakan untuk menuntut ganti rugi. Pasal 3 ayat 3 POJK 06/2022 mengatur sanksi administratif bagi pelanggaran perlindungan data. Dengan kata lain, bank yang melanggar dapat dikenai tindakan tegas (peringatan, denda) selain tanggung jawab hukum perdata. POJK ini menjadikan bank bertanggung jawab ketat (*strict liability*) atas kebocoran data nasabah, tanpa perlu menunjukkan unsur kesalahan (*no-fault liability*) (Wiedyasari & Yuspin, 2024).
d. POJK No. 21/POJK.03/2023 tentang Layanan Digital oleh Bank Umum: Peraturan evaluasi layanan digital terbaru ini menekankan aspek keamanan TI. Dalam lampirannya, disebut bahwa setiap Layanan Digital harus memiliki kontrol pengamanan yang memastikan prinsip CINA (*Confidentiality, Integrity, Authentication, Availability, Non-repudiation*) terpenuhi. Artinya, bank wajib menerapkan teknologi yang memastikan data nasabah tetap rahasia, akurat, dan tersedia, serta jejak transaksi tidak dapat disangkal. POJK ini mendorong bank untuk memasukkan audit keamanan dan protokol enkripsi kuat dalam infrastruktur *mobile banking*.

Secara keseluruhan, kombinasi UU PDP, UU ITE, dan peraturan OJK memberikan kerangka normatif yang kuat untuk melindungi data nasabah *mobile banking* di Indonesia. Inti dari semua aturan ini adalah: (a) persetujuan eksplisit nasabah diperlukan untuk pemrosesan data, (b) keamanan teknis harus dijaga (enkripsi, backup, pengawasan), (c) hak konsumen (akses, koreksi, penghapusan, kompensasi) dihormati, dan (d) sanksi tegas menanti pelanggaran. Seluruh bank umum dan penyedia layanan *fintech* yang menawarkan mobile banking harus mematuhi regulasi-regulasi tersebut.

Bentuk Tanggung Jawab Bank dan Upaya Perlindungan Hukum terhadap Kebocoran Data Pribadi Nasabah dalam Layanan *Mobile Banking* Di Indonesia

1. Tanggung Jawab Bank terhadap Perlindungan Data Pribadi Nasabah

Tanggung jawab bank terhadap perlindungan data pribadi nasabah merupakan kewajiban hukum yang melekat pada kedudukan bank sebagai lembaga intermediasi yang menghimpun dan mengelola dana masyarakat (Aulia et al., 2025). Dalam konteks layanan digital, bank berkedudukan sebagai pengendali data yang wajib menjamin bahwa setiap informasi yang diperoleh dari nasabah diproses secara sah, aman, dan tidak disalahgunakan. Kewajiban tersebut tidak hanya bersumber dari prinsip kerahasiaan bank dalam hukum perbankan, tetapi juga dari aturan perundang-undangan yang secara khusus mengatur perlindungan data pribadi di Indonesia. Data mengenai identitas, riwayat transaksi, serta kondisi keuangan nasabah termasuk kategori informasi yang harus dijaga kerahasiaannya. Pengawasan terhadap pelaksanaan kewajiban ini dilakukan oleh Otoritas Jasa Keuangan guna memastikan perlindungan konsumen dan stabilitas sistem keuangan tetap terjaga (Kurniawan & Yuspin, 2023).

Pelaksanaan tanggung jawab bank tercermin dalam penerapan sistem keamanan teknologi informasi yang memadai pada layanan *mobile banking*. Pengendalian akses internal, enkripsi data, autentikasi berlapis, serta audit berkala menjadi bagian dari mekanisme perlindungan yang wajib dijalankan (Sitanggang et al., 2024). Setiap pemrosesan data harus memiliki tujuan yang jelas dan tidak boleh melampaui kepentingan yang telah diinformasikan kepada nasabah. Prinsip pembatasan tujuan dan minimalisasi data menjadi pedoman dalam seluruh aktivitas pengelolaan informasi pada sistem perbankan digital. Tanggung jawab tersebut dapat diklasifikasikan ke dalam dua bentuk, yaitu sebagai berikut:

A. Tanggung Jawab Preventif

Tanggung jawab preventif merupakan bentuk pencegahan yang dilakukan bank untuk menghindari terjadinya kebocoran atau penyalahgunaan data pribadi nasabah. Pelaksanaannya diwujudkan melalui penerapan sistem keamanan teknologi informasi seperti enkripsi data, penggunaan *one time password* (OTP), autentikasi berlapis, pembatasan akses internal berdasarkan kewenangan jabatan, serta audit dan evaluasi sistem secara berkala.

B. Tanggung Jawab Represif

Tanggung jawab represif muncul apabila terjadi pelanggaran atau insiden kebocoran data pribadi. Dalam kondisi tersebut, bank wajib melakukan investigasi internal, menghentikan atau memperbaiki sistem yang bermasalah, serta menyampaikan pemberitahuan kepada nasabah dan otoritas pengawas seperti Otoritas Jasa Keuangan. Bank juga dapat dimintakan pertanggungjawaban berupa ganti rugi apabila terbukti terdapat kelalaian, di samping kemungkinan dikenakannya sanksi administratif sesuai ketentuan peraturan perundang-undangan yang berlaku (Putri & Sugiono, 2024).

Implementasi tanggung jawab tersebut dalam praktik perbankan digital dapat diamati pada layanan *mobile banking* yang disediakan oleh bank di Indonesia. Gambaran konkret pelaksanaan tanggung jawab tersebut dapat dilihat pada Bank Rakyat Indonesia (BRI) melalui layanan *mobile banking* BRImo. Tahap pertama dimulai dari pengumpulan dan registrasi data nasabah ketika pengguna mengunduh aplikasi dan melakukan pendaftaran dengan mengisi data identitas seperti nomor KTP, nomor rekening, alamat email, serta nomor telepon. Proses verifikasi dilakukan melalui pengiriman kode OTP dan pencocokan data untuk memastikan bahwa pengguna merupakan pemilik sah rekening (Fitriani et al., 2024). Pada tahap ini bank juga menampilkan syarat dan ketentuan serta kebijakan privasi yang harus disetujui sebagai dasar hukum pemrosesan data pribadi.

Tahap kedua mencakup penyimpanan dan pengamanan data dalam sistem server yang dilengkapi enkripsi serta pengamanan berlapis. Akses terhadap data dibatasi berdasarkan kewenangan jabatan dan seluruh aktivitas tercatat dalam sistem audit internal untuk mencegah penyalahgunaan. Tahap ketiga meliputi penggunaan dan pemrosesan data untuk keperluan

operasional, seperti autentikasi login, validasi transaksi, dan pencatatan riwayat aktivitas. Sistem juga melakukan pemantauan terhadap transaksi yang tidak wajar sebagai langkah mitigasi risiko kejahatan siber, dengan tetap berpegang pada tujuan awal pengumpulan data.

Tahap keempat berupa pengawasan dan evaluasi berkala melalui audit keamanan, pembaruan sistem, serta penguatan fitur perlindungan digital. Edukasi kepada nasabah mengenai keamanan transaksi menjadi bagian dari upaya preventif dalam menjaga data pribadi dan dana yang tersimpan. Tahap kelima merupakan penanganan insiden dan pertanggungjawaban apabila terjadi dugaan kebocoran atau penyalahgunaan data. Bank wajib melakukan investigasi internal, mengambil langkah pemulihan, serta menyampaikan pemberitahuan kepada nasabah dan otoritas pengawas sesuai ketentuan hukum. Rangkaian tahapan tersebut menunjukkan bahwa perlindungan data pribadi nasabah pada layanan *mobile banking* di Indonesia bukan sekadar kewajiban administratif, melainkan bentuk tanggung jawab hukum yang bersifat preventif dan represif dalam sistem perbankan digital nasional.

2. Mekanisme Penyelesaian Sengketa dan Upaya Hukum bagi Nasabah yang Dirugikan

Mekanisme penyelesaian sengketa dan upaya perlindungan hukum terhadap kebocoran data pribadi nasabah dalam layanan mobile banking di Indonesia pada dasarnya bertujuan untuk memberikan kepastian dan perlindungan kepada nasabah apabila data pribadinya disalahgunakan atau bocor. Dalam praktiknya, penyelesaian sengketa dapat dilakukan melalui beberapa jalur, baik secara non-litigasi maupun litigasi (Nasution et al., 2024). Pertama, penyelesaian sengketa dapat dilakukan melalui mekanisme pengaduan kepada pihak bank. Nasabah yang merasa dirugikan karena kebocoran data pribadi dapat menyampaikan keluhan secara langsung kepada bank penyedia layanan mobile banking. Bank berkewajiban menindaklanjuti pengaduan tersebut, melakukan investigasi, serta memberikan penjelasan atau solusi atas permasalahan yang terjadi. Dalam hal tertentu, bank juga dapat memberikan ganti rugi kepada nasabah apabila terbukti terjadi kesalahan atau kelalaian dalam pengelolaan sistem keamanan data.

Apabila penyelesaian melalui bank tidak mencapai kesepakatan, nasabah dapat mengajukan pengaduan kepada lembaga pengawas sektor jasa keuangan, yaitu Otoritas Jasa Keuangan (OJK). OJK memiliki kewenangan untuk menerima laporan dari konsumen jasa keuangan yang merasa dirugikan. Melalui mekanisme ini, OJK dapat melakukan mediasi antara nasabah dan bank untuk mencari penyelesaian yang adil. Selain itu, OJK juga dapat memberikan sanksi administratif kepada bank apabila terbukti melanggar ketentuan perlindungan konsumen atau keamanan data (Nasution et al., 2024). Penyelesaian sengketa juga dapat dilakukan melalui lembaga alternatif penyelesaian sengketa di sektor jasa keuangan, yaitu Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK).(Alif Rizqi Ramadhan & Albertus Sentot Sudarwanto, 2024) Melalui lembaga ini, sengketa antara nasabah dan bank dapat diselesaikan melalui proses mediasi, ajudikasi, atau arbitrase.

Mekanisme ini biasanya dipilih karena prosesnya lebih cepat, biaya yang lebih ringan, serta tidak serumit proses pengadilan. Jika upaya penyelesaian di luar pengadilan tidak berhasil, nasabah memiliki hak untuk menempuh jalur litigasi melalui pengadilan. Nasabah dapat mengajukan gugatan perdata apabila kebocoran data pribadi menimbulkan kerugian, misalnya kerugian finansial atau penyalahgunaan identitas. Dalam gugatan tersebut, nasabah dapat menuntut ganti kerugian kepada pihak yang dianggap bertanggung jawab, termasuk bank apabila terbukti lalai dalam menjaga keamanan data (Dharsono Wijaya et al., 2022).

Selain mekanisme penyelesaian sengketa, terdapat pula upaya perlindungan hukum terhadap data pribadi nasabah. Perlindungan ini diatur dalam berbagai peraturan perundang-undangan di Indonesia. Salah satu regulasi utama adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mewajibkan setiap pihak yang mengelola data pribadi untuk menjaga keamanan dan kerahasiaan data tersebut. Jika terjadi kebocoran data, pengendali data wajib memberi pemberitahuan kepada pemilik data serta bertanggung jawab atas kerugian yang timbul. Selain itu, perlindungan juga diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang memberikan hak kepada konsumen untuk memperoleh

keamanan dan kenyamanan dalam menggunakan suatu layanan. Dalam konteks mobile banking, bank sebagai pelaku usaha wajib memastikan sistem layanan yang digunakan aman dan tidak membahayakan nasabah (Widya et al., 2024).

Di sektor perbankan sendiri, kewajiban perlindungan data nasabah juga diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang menegaskan bahwa bank wajib menjaga kerahasiaan data dan informasi nasabah. Pelanggaran terhadap kewajiban tersebut dapat menimbulkan sanksi hukum. Dengan adanya berbagai mekanisme penyelesaian sengketa dan aturan perlindungan hukum tersebut, nasabah sebenarnya memiliki beberapa jalur untuk mendapatkan perlindungan apabila terjadi kebocoran data pribadi dalam layanan mobile banking. Hal ini menunjukkan bahwa perlindungan terhadap data pribadi menjadi aspek yang sangat penting dalam perkembangan layanan perbankan digital di Indonesia.

KESIMPULAN

Penelitian ini menemukan bahwa pengaturan hukum perlindungan data pribadi nasabah pada layanan mobile banking di Indonesia telah terbentuk secara komprehensif melalui UU PDP, UU ITE, dan peraturan OJK seperti POJK No. 11/POJK.03/2022 serta POJK No. 06/POJK.07/2022, yang menekankan persetujuan eksplisit, keamanan teknis, dan tanggung jawab preventif serta represif bank sebagai pengendali data. Namun, implementasinya masih parsial akibat kesenjangan harmonisasi regulasi dengan dinamika kemitraan pihak ketiga dan ancaman siber, sehingga nasabah memiliki upaya hukum melalui pengaduan OJK, LAPS SJK, hingga gugatan perdata untuk ganti rugi. Keterbatasan penelitian terletak pada pendekatan yuridis normatif yang bergantung pada dokumen sekunder tanpa analisis empiris kasus nyata atau wawancara pelaku industri, sehingga temuan bersifat deskriptif dan belum mengukur efektivitas lapangan.

Saran bagi penelitian selanjutnya mencakup pendekatan yuridis empiris dengan studi kasus kebocoran data terkini untuk menguji efektivitas sanksi, serta analisis komparatif dengan regulasi internasional seperti GDPR guna memperkaya rekomendasi harmonisasi. Secara praktis, implikasi penelitian mendorong bank memperkuat due diligence mitra, audit TI berkala, dan edukasi literasi data nasabah, sementara regulator seperti OJK perlu regulasi teknis pendukung UU PDP untuk inklusi finansial yang aman dan kepercayaan publik yang berkelanjutan.

DAFTAR PUSTAKA

Alif Rizqi Ramadhan, & Albertus Sentot Sudarwanto. (2024). Penyelesaian sengketa kebocoran data pribadi nasabah bank melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK). *Terang: Jurnal Kajian Ilmu Sosial, Politik dan Hukum, 1*(2), 95–101. https://doi.org/10.62383/terang.v1i2.207

Aulia, A. I., Fitriah, Y., & Astuti, R. P. (2025). Analisis hubungan kelembagaan antara Bank Sentral, Pemerintah, dan Perbankan dalam stabilitas keuangan negara. *Jurnal Penelitian Nusantara, 1*(5), 325–333. https://padangjurnal.web.id/index.php/menulis/article/view/276/269

Aziz, A. S., & Zaidan, M. A. (2025). Perlindungan hukum nasabah terhadap penyalahgunaan data pribadi oleh pihak ketiga dalam kerja sama perbankan digital. *Ekopedia: Jurnal Ilmiah Ekonomi, 1*(2), 120–129. https://doi.org/10.63822/qwcqac2

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.

Dharsono Wijaya, I., Dharsono, I., Pane, W., & Kansil, C. S. T. (2022). Penyelesaian sengketa terhadap dugaan penyalahgunaan data pribadi dalam layanan fintech. *Syntax Literate: Jurnal Ilmiah Indonesia, 7*(11), 2548–2598. https://doi.org/10.36418/syntax-literate.v7i11.12021

Emzir. (2022). *Metodologi penelitian kualitatif: Rumah analisis data kualitatif*. Pustaka Setia.

Fitriani, S. A., Sasra, A. D., Harjuno, M., & Raharjo, A. (2024). Analisis perlindungan data pribadi nasabah perbankan terhadap penggunaan layanan mobile banking. *Media Hukum Indonesia (MHI), 9*(4), 300–308. https://doi.org/10.5281/zenodo.14192101

Hidayat, R., & Rahman, A. (2023). Regulasi teknis perlindungan data di sektor jasa keuangan. *Jurnal Hukum Keuangan*, 12(2), 45–60.

Irmawati, E., Pieries, J., & Widiarty, W. S. (2024). Perlindungan hukum atas data pribadi nasabah bank pengguna mobile banking dalam perspektif UU No. 27 Tahun 2022 tentang kebocoran data. *Syntax Admiration, 5*(1), 1–15.

Kurniawan, D., & Yuspin, W. (2023). Menggagas pendirian bank digital di Indonesia: Sebuah telaah yuridis. *Jurnal Supremasi Hukum, 13*(1), 191–200. https://doi.org/10.35457/supremasi.v13i1.2158

Kurniawan, D., et al. (2024). Kebocoran data di platform fintech terkini. *Jurnal Teknologi Keuangan*, 8(1), 78–92.

Nasution, R. A., Ginting, B., Siregar, M., & Devi Azwar, T. K. (2024). Perlindungan hukum terhadap data pribadi nasabah layanan perbankan setelah berlakunya Peraturan Otoritas Jasa Keuangan (POJK) Nomor 6/POJK.07/2022. *Journal of Education, Humaniora and Social Sciences (JEHSS), 7*(1), 71–78. https://doi.org/10.34007/jehss.v7i1.2292

Nugroho, A., & Santoso, B. (2024). Implementasi parsial UU PDP di lembaga perbankan. *Jurnal Hukum PDP*, 10(3), 112–130.

Pratiwi, D., et al. (2022). Pengelolaan data ketat untuk kepercayaan nasabah. *Jurnal Perbankan Digital*, 5(2), 200–215.

Putri, R. A. T., & Sugiono, H. (2024). Tanggung jawab bank terhadap tindakan phishing dalam sistem penggunaan e-banking (Studi: Kasus phishing pada PT. Bank Rakyat Indonesia (Persero) Tbk). *Jurnal Interpretasi Hukum, 4*(3), 682–690. https://doi.org/10.22225/juinhum.5.1.8318.682-690

Rohendi, A., & Kharisma, D. B. (2025). Personal data protection in fintech: A case study from Indonesia. *Journal of Infrastructure, Policy and Development, 8*(7), 4158.

Sari, N., & Pratama, R. (2022). Pengawasan regulator dan literasi data masyarakat. *Jurnal Regulasi Keuangan*, 7(4), 150–165.

Setyowati, R., & Kurniawan, A. (2023). Risiko keamanan siber pada mobile banking. *Jurnal Siber Keuangan*, 9(1), 30–45.

Sitanggang, A. S., Lestari, S., Febrianti, N. C., & Az-zahra, A. (2024). Analisis tingkat kepercayaan nasabah pada keamanan transaksi perbankan melalui mobile banking (M-banking). *Jurnal Manajemen Siber, 9*(3), 1566–1581. https://doi.org/10.30651/jms.v9i3.23067

Sitanggang, V., Timomor, A., & Tuawaidan, A. N. (2025). Kajian hukum perlindungan data pribadi nasabah dalam sistem mobile banking di Indonesia. *Civilia, 4*, 124–132.

Sudaryono. (2023). *Metode penelitian hukum normatif*. Ghalia Indonesia.

Sugiyono. (2023). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.

Wardhono, R. D. T. K., Badrawani, W., Deviana, A., Pramudyastuti, M., & Shalehanti, N. (2024). Perlindungan data pribadi di Bank Indonesia dan lembaga jasa keuangan: Rekomendasi kebijakan dan teknis pengaturan (02).

Wiedyasari, A. B., & Yuspin, W. (2024). Protection of customer personal data of Bank Syariah Indonesia reviewed from POJK Number 6/POJK.07/2022. *UNRAM Law Review, 8*(4), 1–17. https://doi.org/10.29303/ulrev.v8i1.331

Widya, S., Pasha, H., Simanjuntak, G. H., & Ayudia, M. A. (2024). Tanggung jawab hukum bank dalam kasus kebocoran data nasabah. *Jurnal Multidisiplin Ilmu Akademik, 1*(6), 129–135. https://doi.org/10.61722/jmia.v1i6.2885