

Perlindungan Hukum Data Pribadi Nasabah pada Pelaksanaan Bank Digital di Indonesia Berdasarkan Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Martin Luther Manullang

Universitas HKBP Nommensen, Indonesia

 aryatejakusuma14@gmail.com

Abstrak

Perkembangan teknologi informasi telah mendorong transformasi sektor perbankan menuju sistem berbasis digital yang mengandalkan pemrosesan data pribadi nasabah secara intensif. Kondisi ini menimbulkan risiko tinggi terhadap kebocoran dan penyalahgunaan data pribadi, sehingga memerlukan perlindungan hukum yang komprehensif. Penelitian ini bertujuan untuk menganalisis pengaturan perlindungan data pribadi nasabah dalam penyelenggaraan bank digital di Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta mengkaji tanggung jawab hukum bank digital atas kebocoran data pribadi nasabah. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual, menggunakan data sekunder yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa Undang-Undang Perlindungan Data Pribadi menempatkan bank digital sebagai Pengendali Data Pribadi yang wajib menerapkan prinsip-prinsip pemrosesan data, seperti legalitas, transparansi, pembatasan tujuan, minimalisasi data, keamanan, dan akuntabilitas, serta kewajiban memperoleh persetujuan dan melakukan Penilaian Dampak Perlindungan Data (DPIA). Perlindungan hukum terhadap data pribadi nasabah terdiri atas perlindungan preventif dan represif yang saling melengkapi. Selanjutnya, tanggung jawab hukum bank digital atas kebocoran data bersifat kumulatif, meliputi tanggung jawab administratif, perdata, dan pidana. Tanggung jawab administratif dikenakan atas pelanggaran kewajiban hukum, tanggung jawab perdata berfungsi sebagai mekanisme pemulihan kerugian nasabah, sedangkan tanggung jawab pidana diterapkan apabila terdapat unsur kesengajaan sebagai ultimum remedium, termasuk pertanggungjawaban pidana korporasi. Sinkronisasi antara Undang-Undang Perlindungan Data Pribadi sebagai lex generalis dan regulasi Otoritas Jasa Keuangan sebagai lex specialis menjadi faktor penting dalam menjamin kepastian hukum dan efektivitas perlindungan data pribadi nasabah dalam penyelenggaraan bank digital.

Kata Kunci: *Perlindungan data pribadi, Bank digital, Tanggung jawab hukum, Kebocoran data, UU PDP.*

ARTICLE INFO

Received
February 02,
2026
Revised
March 02, 2026
Accepted
April 30, 2026

Diterbitkan oleh

ISSN

Website

Ini adalah artikel akses terbuka di bawah lisensi CC BY SA

Fakultas Syariah Sekolah Tinggi Agama Islam (STAI) Al-Furqan Makassar

2622-5212

<https://ojs.staialfurqan.ac.id/jtm/>

<https://creativecommons.org/licenses/by-sa/4.0/>



PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi signifikan dalam berbagai sektor, termasuk sektor jasa keuangan. Transformasi tersebut ditandai dengan hadirnya bank digital sebagai model layanan perbankan berbasis sistem elektronik yang memungkinkan seluruh aktivitas perbankan dilakukan secara daring tanpa kehadiran fisik nasabah. Dalam praktiknya, bank digital mengandalkan pengelolaan data pribadi nasabah secara intensif, meliputi data identitas, data keuangan, data biometrik, hingga data transaksi, yang menjadi elemen fundamental dalam penyelenggaraan layanan.

Data pribadi nasabah tidak hanya berfungsi sebagai instrumen operasional, tetapi juga memiliki nilai ekonomi yang tinggi sehingga menjadikannya aset strategis bagi bank digital. Namun demikian, tingginya nilai tersebut juga meningkatkan kerentanan terhadap ancaman kejahatan siber, seperti kebocoran data, phishing, dan akses tidak sah terhadap sistem elektronik.

Peningkatan insiden serangan siber di sektor keuangan serta berbagai kasus kebocoran data di Indonesia menunjukkan bahwa perlindungan data pribadi masih menjadi permasalahan serius, terutama dalam kaitannya dengan perlindungan hak privasi sebagai bagian dari hak asasi manusia.

Dalam konteks ini, bank digital sebagai pengendali data pribadi memiliki kewajiban hukum untuk menjamin keamanan, kerahasiaan, dan pemrosesan data pribadi nasabah secara sah, adil, dan transparan. Kewajiban tersebut tidak hanya bertujuan melindungi kepentingan nasabah, tetapi juga menjaga kepercayaan publik dan stabilitas sistem perbankan nasional. Sebagai respons terhadap meningkatnya ancaman tersebut, Pemerintah Indonesia telah menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang memberikan landasan hukum komprehensif terkait hak subjek data, kewajiban pengendali data, serta sanksi atas pelanggaran.

Namun demikian, meskipun secara normatif telah terdapat pengaturan yang jelas, dalam praktiknya masih ditemukan kesenjangan antara ketentuan hukum dan implementasinya. Hal ini terlihat dari masih terjadinya kebocoran data di sektor perbankan, yang menunjukkan adanya kelemahan dalam sistem keamanan, pengawasan, serta penegakan hukum. Kondisi tersebut menimbulkan persoalan hukum terkait efektivitas perlindungan data pribadi serta tanggung jawab bank digital sebagai pengendali data.

Berdasarkan uraian tersebut, permasalahan dalam penelitian ini difokuskan pada: (1) bagaimana pengaturan perlindungan data pribadi nasabah dalam penyelenggaraan bank digital di Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; dan (2) bagaimana tanggung jawab hukum bank digital sebagai pengendali data pribadi terhadap terjadinya kebocoran data pribadi nasabah. Sejalan dengan itu, penelitian ini bertujuan untuk menganalisis pengaturan perlindungan data pribadi dalam bank digital serta mengkaji tanggung jawab hukum bank digital atas kebocoran data pribadi nasabah. Penelitian ini diharapkan dapat memberikan kontribusi teoritis dan praktis dalam memperkuat perlindungan hukum terhadap data pribadi serta menjamin kepastian hukum dalam penyelenggaraan perbankan digital di Indonesia.

Kerangka Teoritis

Dalam penelitian hukum normatif, teori berfungsi sebagai kerangka konseptual untuk menafsirkan dan menganalisis norma hukum yang berlaku. Teori tidak dipahami sebagai variabel empiris, melainkan sebagai alat analisis untuk menjelaskan hukum (*das sein*) sekaligus menilai hukum (*das sollen*). Dengan demikian, kerangka teori digunakan untuk mempertajam objek kajian, mengklasifikasikan norma hukum, serta mengidentifikasi kelemahan dalam implementasi hukum. Penelitian ini menggunakan dua teori utama, yaitu Teori Perlindungan Hukum dan Teori Sistem Hukum.

1. **Teori Perlindungan Hukum** Teori perlindungan hukum merupakan teori fundamental yang bertujuan menjamin terpenuhinya hak-hak subjek hukum serta memberikan perlindungan terhadap potensi pelanggaran. Dalam negara hukum (*rechtstaat*), perlindungan hukum menjadi kewajiban negara sebagai bentuk penghormatan terhadap hak asasi manusia. Perlindungan hukum tidak hanya bersifat normatif, tetapi juga harus mampu memberikan perlindungan secara nyata terhadap kepentingan masyarakat. Perlindungan hukum dibedakan menjadi dua bentuk, yaitu preventif dan represif. **Perlindungan hukum preventif** bertujuan mencegah terjadinya pelanggaran melalui pengaturan norma, standar, dan kewajiban hukum. Dalam konteks perlindungan data pribadi, bentuk ini diwujudkan melalui regulasi, pengawasan, serta penerapan prinsip kehati-hatian, keamanan sistem, dan kepatuhan oleh pengendali data. Sementara itu, **perlindungan hukum represif** berfungsi menyelesaikan sengketa dan memulihkan hak setelah terjadinya pelanggaran. Mekanisme ini meliputi pemberian sanksi administratif, perdata, maupun pidana terhadap pihak yang lalai atau melanggar kewajiban perlindungan data pribadi. Perlindungan represif juga berperan sebagai instrumen akuntabilitas dan efek jera guna mencegah pelanggaran berulang. Dengan demikian, teori perlindungan hukum digunakan untuk menganalisis upaya pencegahan dan penegakan hukum dalam perlindungan data pribadi nasabah bank digital, baik sebelum maupun setelah terjadinya kebocoran data.
2. **Teori Sistem Hukum** Teori sistem hukum digunakan untuk menganalisis bekerjanya hukum secara menyeluruh, tidak hanya dari aspek norma tertulis, tetapi juga dari pelaksanaan dan kepatuhannya dalam praktik. Teori ini memandang hukum sebagai suatu sistem yang terdiri dari unsur-unsur yang saling berkaitan dalam mencapai keadilan, kepastian hukum, dan kemanfaatan. Menurut Friedman, sistem hukum terdiri atas tiga komponen utama, yaitu

struktur hukum, substansi hukum, dan budaya hukum. Ketiga komponen tersebut harus berjalan secara sinergis agar hukum dapat berfungsi secara efektif. Ketidakseimbangan di antara ketiganya dapat menimbulkan kesenjangan antara hukum tertulis (*law in books*) dan praktik (*law in action*), sebagaimana terlihat dalam perlindungan data pribadi di sektor perbankan digital yang masih menghadapi kasus kebocoran data.

- a. **Struktur hukum (legal structure)** Struktur hukum mencakup lembaga dan aparat yang berwenang dalam pembentukan, pelaksanaan, pengawasan, dan penegakan hukum. Efektivitas hukum sangat bergantung pada kapasitas, integritas, dan koordinasi antar lembaga.
- b. **Substansi hukum (legal substance)** Substansi hukum berkaitan dengan norma, asas, dan peraturan perundang-undangan yang mengatur perlindungan data pribadi. Kualitasnya ditentukan oleh kejelasan, konsistensi, dan kelengkapan pengaturan serta sanksi.
- c. **Budaya hukum (legal culture)** Budaya hukum merupakan sikap dan kesadaran masyarakat serta aparat terhadap hukum. Tingkat kepatuhan dan komitmen terhadap norma sangat memengaruhi efektivitas penerapannya.

Kerangka konsep merupakan pedoman operasional yang menjabarkan kerangka teoritis ke dalam definisi yang lebih konkret. Dalam penelitian hukum normatif, kerangka konsep berfungsi untuk membatasi makna istilah yang digunakan serta memudahkan proses analisis agar tetap terarah sesuai dengan tujuan penelitian. Berdasarkan fokus penelitian, konsep yang digunakan adalah perlindungan hukum data pribadi dalam sistem hukum Indonesia.

1. **Perlindungan Hukum Data Pribadi dalam Sistem Hukum Indonesia**

Perlindungan hukum data pribadi adalah segala upaya hukum untuk menjamin pengakuan, penghormatan, dan perlindungan hak subjek data dalam setiap proses pengolahan data. Perlindungan ini merupakan bagian dari hak atas privasi yang dijamin secara konstitusional. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mendefinisikan data pribadi sebagai setiap data tentang individu yang dapat diidentifikasi, baik secara langsung maupun tidak langsung. Undang-undang tersebut juga mengatur prinsip-prinsip pemrosesan data pribadi, seperti legalitas, pembatasan tujuan, minimalisasi data, akurasi, keamanan, dan akuntabilitas, yang wajib dipatuhi oleh pengendali data, termasuk bank digital.

- a. **Perlindungan hukum preventif** merupakan upaya pencegahan terhadap pelanggaran melalui pengaturan norma, standar keamanan, serta kewajiban pengendali data dalam pengelolaan data pribadi. Dalam konteks bank digital, perlindungan ini mencakup transparansi, persetujuan nasabah, serta penerapan sistem keamanan untuk mencegah kebocoran data sejak awal.
- b. **Perlindungan hukum represif** merupakan upaya penyelesaian setelah terjadinya pelanggaran, yang meliputi penegakan hukum, pemberian sanksi, dan pemulihan hak subjek data. UU Perlindungan Data Pribadi mengatur sanksi administratif, gugatan perdata untuk ganti rugi, serta sanksi pidana bagi pelanggaran tertentu.

2. **Prinsip-Prinsip Perlindungan Data Pribadi dalam UU No. 27 Tahun 2022**

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menetapkan prinsip-prinsip dasar yang wajib dipatuhi dalam setiap pemrosesan data pribadi. Prinsip-prinsip ini menjadi landasan normatif bagi pengendali data, termasuk bank digital, agar pemrosesan data dilakukan secara sah, terbatas, dan bertanggung jawab.

- a. **Prinsip Legalitas dan Persetujuan (Consent)** Pemrosesan data pribadi harus memiliki dasar hukum yang sah, salah satunya melalui persetujuan subjek data. Persetujuan harus diberikan secara sadar, spesifik, dan dapat dibuktikan, serta didasarkan pada informasi yang jelas. Subjek data juga berhak menarik kembali persetujuan tersebut.
- b. **Prinsip Pembatasan Tujuan (Purpose Limitation)** Data pribadi hanya dapat diproses untuk tujuan tertentu, sah, dan telah diberitahukan kepada subjek data. Penggunaan data di luar tujuan awal tidak diperbolehkan tanpa dasar hukum atau persetujuan baru.
- c. **Prinsip Minimalisasi Data (Data Minimization)** Pengumpulan data harus dibatasi pada data yang relevan dan sesuai dengan kebutuhan. Pengendali data

tidak diperkenankan mengumpulkan data secara berlebihan yang tidak berkaitan dengan tujuan pemrosesan.

- d. **Prinsip Akurasi dan Keterkinian Data** Pengendali data wajib memastikan data yang diproses akurat, lengkap, dan mutakhir. Selain itu, harus tersedia mekanisme bagi subjek data untuk memperbaiki atau memperbarui datanya.
 - e. **Prinsip Keamanan Data (Security Principle)** Data pribadi harus dilindungi dari akses tidak sah, kebocoran, atau penyalahgunaan melalui langkah teknis dan organisatoris yang memadai, seperti sistem keamanan dan pembatasan akses.
 - f. **Prinsip Akuntabilitas (Accountability)** Pengendali data bertanggung jawab atas seluruh pemrosesan data dan harus mampu membuktikan kepatuhan terhadap ketentuan hukum, antara lain melalui kebijakan internal, audit, dan pengawasan.
3. **Kedudukan Bank Digital sebagai Pengendali Data Pribadi** Bank digital merupakan lembaga perbankan yang menyelenggarakan layanan berbasis sistem elektronik, di mana seluruh aktivitas, seperti pembukaan rekening, verifikasi identitas, dan transaksi keuangan, dilakukan secara daring. Kondisi ini menyebabkan tingginya ketergantungan terhadap pengelolaan data pribadi nasabah. Dalam konteks ini, bank digital berkedudukan sebagai pengendali data pribadi yang memiliki tanggung jawab utama untuk menjamin keamanan, kerahasiaan, dan integritas data nasabah. Data pribadi nasabah mencakup data identitas, keuangan, transaksi, hingga biometrik, yang memiliki nilai strategis dalam penyelenggaraan layanan perbankan. Kebocoran data pribadi merupakan pelanggaran keamanan yang mengakibatkan data diakses atau disalahgunakan oleh pihak tidak berwenang. Peristiwa ini dapat menimbulkan kerugian finansial, pencurian identitas, serta menurunkan kepercayaan masyarakat terhadap perbankan. Oleh karena itu, sebagai pengendali data, bank digital memiliki tanggung jawab hukum atas perlindungan data pribadi nasabah, terutama dalam mencegah dan menanggulangi kebocoran data.
4. **Tanggung Jawab Hukum Bank** merupakan kewajiban yang timbul akibat pelanggaran terhadap perlindungan data pribadi nasabah. Tanggung jawab ini mencakup aspek administratif, perdata, dan pidana sebagai bentuk akuntabilitas bank digital sebagai pengendali data pribadi.
- a. **Tanggung Jawab Administratif** dikenakan apabila bank melanggar ketentuan dalam Undang-Undang Perlindungan Data Pribadi. Sanksi dapat berupa peringatan tertulis, penghentian sementara pemrosesan data, penghapusan data, atau denda administratif. Selain itu, bank digital juga dapat dikenakan sanksi oleh Otoritas Jasa Keuangan apabila pelanggaran berkaitan dengan tata kelola dan prinsip kehati-hatian.
 - b. **Tanggung Jawab Perdata** Bank dapat dimintai pertanggungjawaban perdata apabila pelanggaran data pribadi menimbulkan kerugian bagi nasabah. Dasarnya dapat berupa perbuatan melawan hukum maupun wanprestasi dalam hubungan kontraktual. Nasabah berhak menuntut ganti rugi atas kerugian materiil maupun immateriil akibat kebocoran atau penyalahgunaan data.
 - c. **Tanggung Jawab Pidana** timbul apabila terdapat perbuatan melawan hukum, seperti pengungkapan atau penggunaan data pribadi tanpa hak. Sanksi dapat berupa pidana penjara dan/atau denda. Dalam konteks korporasi, pertanggungjawaban pidana dapat dikenakan tidak hanya kepada pelaku individu, tetapi juga kepada bank sebagai badan hukum.

METODE

Metode penelitian merupakan cara yang digunakan untuk mencapai tujuan serta memecahkan permasalahan hukum yang dikaji. Penelitian ini menggunakan jenis penelitian hukum yuridis normatif, yaitu penelitian yang berfokus pada pengkajian hukum sebagai norma melalui analisis terhadap peraturan perundang-undangan dan doktrin hukum. Penelitian ini bertujuan untuk menghasilkan argumentasi hukum, konsep, dan preskripsi dalam menjawab isu perlindungan data pribadi nasabah dalam penyelenggaraan bank digital. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan yang berkaitan dengan perlindungan data pribadi dan sektor perbankan digital,

khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Sementara itu, pendekatan konseptual digunakan untuk mengkaji konsep-konsep hukum seperti perlindungan hukum, tanggung jawab hukum, pengendali data pribadi, serta prinsip-prinsip perlindungan data pribadi. Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh melalui studi kepustakaan. Data sekunder terdiri atas bahan hukum primer berupa peraturan perundang-undangan yang relevan, bahan hukum sekunder berupa buku, jurnal ilmiah, dan pendapat para ahli, serta bahan hukum tersier seperti kamus hukum dan ensiklopedia untuk memperjelas istilah dan konsep hukum. **Teknik pengumpulan data** dilakukan melalui studi kepustakaan dengan cara menelaah, mengkaji, dan mengklasifikasikan bahan hukum berdasarkan relevansi dan kredibilitasnya. Seluruh bahan hukum yang telah dikumpulkan kemudian dianalisis secara sistematis guna memperoleh pemahaman yang komprehensif terhadap permasalahan yang diteliti. **Analisis data** dilakukan secara kualitatif dengan metode yuridis, yaitu dengan menafsirkan peraturan perundang-undangan dan doktrin hukum yang relevan. Hasil analisis disajikan secara deskriptif-analitis dengan menggambarkan kondisi hukum yang berlaku, mengidentifikasi permasalahan, serta memberikan argumentasi hukum yang sistematis. Penarikan kesimpulan dilakukan secara deduktif, yaitu dari ketentuan umum menuju penerapannya pada permasalahan khusus.

HASIL DAN PEMBAHASAN

EKSISTENSI PENGADILAN TINDAK PIDANA KORUPSI DALAM MELAKUKAN PEMBERANTASAN KORUPSI

A. Perlindungan Hukum Data Pribadi Nasabah dalam Pelaksanaan Bank Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022

Transformasi layanan perbankan menuju sistem berbasis teknologi informasi telah melahirkan model *digital banking* yang mengandalkan sistem elektronik dalam seluruh proses operasionalnya, mulai dari pembukaan rekening, verifikasi identitas melalui *electronic Know Your Customer* (e-KYC), hingga pemrosesan transaksi dan penyimpanan data. Kondisi ini menempatkan data pribadi sebagai aset utama sekaligus objek perlindungan hukum yang strategis. Dalam perspektif hukum, keberadaan hukum berfungsi untuk memberikan perlindungan terhadap kepentingan manusia. Sejalan dengan itu, Satjipto Rahardjo menyatakan bahwa perlindungan hukum merupakan upaya melindungi kepentingan seseorang melalui pemberian kewenangan untuk bertindak dalam rangka mempertahankan kepentingannya tersebut.

Dalam konteks perbankan digital, data pribadi nasabah merupakan bagian dari kepentingan hukum yang harus dilindungi oleh negara serta oleh setiap subjek hukum yang memprosesnya. Perlindungan ini menjadi semakin penting mengingat tingginya intensitas pemrosesan data dalam sistem elektronik yang berpotensi menimbulkan risiko pelanggaran, seperti kebocoran data dan penyalahgunaan data. Oleh karena itu, pengaturan mengenai perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 menjadi landasan normatif yang penting dalam menjamin perlindungan hak-hak nasabah dalam penyelenggaraan bank digital.

1. **Kedudukan Data Pribadi Nasabah sebagai Hak yang Dilindungi** Data pribadi dalam sistem hukum modern tidak lagi dipandang sebagai informasi administratif semata, melainkan sebagai bagian dari hak fundamental yang melekat pada setiap individu. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan bahwa perlindungan data pribadi merupakan bagian dari perlindungan hak asasi manusia. Oleh karena itu, setiap aktivitas pemrosesan data oleh bank digital harus ditempatkan dalam kerangka perlindungan hak konstitusional warga negara. Hak atas data pribadi berakar pada hak atas privasi (*right to privacy*) yang dijamin dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Hak ini mencakup perlindungan terhadap diri pribadi, kehormatan, martabat, serta harta benda. Dalam konteks perbankan digital, data pribadi nasabah meliputi beberapa kategori, antara lain:
 - a. Data identitas (nama, NIK, alamat, tanggal lahir);
 - b. Data biometrik dalam proses *electronic Know Your Customer* (e-KYC);
 - c. Data transaksi dan histori keuangan
 - d. Data perilaku digital dan preferensi finansial

- e. Data pribadi spesifik sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi.

Karakteristik layanan bank digital yang berbasis sistem elektronik menyebabkan intensitas pemrosesan data menjadi tinggi, sehingga meningkatkan risiko terjadinya pelanggaran, seperti kebocoran data (*data breach*), penyalahgunaan data, dan akses tanpa hak oleh pihak ketiga. Dalam konteks ini, perlindungan hukum terhadap data pribadi menjadi krusial sebagai upaya menjaga kepentingan hukum nasabah sebagai subjek data. Nasabah sebagai subjek data memiliki hak untuk mengendalikan data pribadinya (*informational self-determination*), yang meliputi: Hak untuk memperoleh informasi; Hak untuk mengakses data pribadi; Hak untuk memperbaiki data; Hak untuk menghapus data tertentu.

2. Prinsip-Prinsip Perlindungan Data Pribadi dalam Pelaksanaan Bank Digital

Prinsip perlindungan data pribadi merupakan dasar normatif dalam mengatur pemrosesan data oleh pengendali data, termasuk bank digital. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menegaskan bahwa pemrosesan data harus dilakukan secara sah, terbatas, dan bertanggung jawab guna menjamin perlindungan hak atas privasi. Dalam konteks bank digital, prinsip-prinsip ini menjadi krusial mengingat tingginya risiko kebocoran dan penyalahgunaan data dalam sistem elektronik.

- a. **Prinsip Legalitas dan Persetujuan (Lawfulness and Consent)** Pemrosesan data harus didasarkan pada persetujuan yang sah atau dasar hukum lain yang diakui. Persetujuan harus diberikan secara bebas, spesifik, dan terinformasi. Dalam praktik digital banking, persetujuan umumnya berbentuk persetujuan elektronik, sehingga transparansi informasi menjadi syarat utama untuk menjamin keabsahannya. Prinsip ini berfungsi sebagai perlindungan preventif agar setiap pemrosesan data memiliki dasar hukum yang jelas.
- b. **Prinsip Pembatasan Tujuan (Purpose Limitation)** Data pribadi hanya boleh diproses untuk tujuan tertentu yang sah dan telah diberitahukan kepada subjek data. Penggunaan data di luar tujuan awal tanpa persetujuan tambahan berpotensi melanggar hak privasi dan asas itikad baik dalam hubungan hukum.
- c. **Prinsip Minimalisasi Data (Data Minimization)** Pengendali data hanya boleh mengumpulkan data yang relevan dan diperlukan sesuai tujuan pemrosesan. Pengumpulan data yang berlebihan meningkatkan risiko kebocoran dan dapat bertentangan dengan prinsip kehati-hatian dalam perbankan.
- d. **Prinsip Akurasi dan Pembaruan Data (Accuracy)** Data harus akurat, lengkap, dan diperbarui. Pengendali data wajib menyediakan mekanisme koreksi untuk mencegah kerugian akibat penggunaan data yang keliru, sekaligus menjamin kepastian hukum dalam layanan perbankan.
- e. **Prinsip Keamanan dan Kerahasiaan Data (Security and Confidentiality)** Pengendali data wajib melindungi data dari akses tidak sah dan kebocoran melalui langkah teknis dan organisatoris yang memadai. Dalam perbankan, prinsip ini sejalan dengan kewajiban kerahasiaan bank dan menjadi dasar pertanggungjawaban apabila terjadi pelanggaran.
- f. **Prinsip Akuntabilitas (Accountability)** Pengendali data bertanggung jawab atas seluruh pemrosesan data dan wajib membuktikan kepatuhannya. Prinsip ini diwujudkan melalui tata kelola perlindungan data, audit, serta kewajiban notifikasi apabila terjadi pelanggaran data.

Selain itu, perlindungan hukum terhadap data pribadi tidak hanya bersifat represif, tetapi juga preventif. Hal ini menegaskan bahwa negara tidak hanya menyediakan mekanisme penyelesaian sengketa setelah terjadi pelanggaran, tetapi juga membangun sistem pencegahan melalui pengaturan yang ketat terhadap pengendali dan pemroses data pribadi. Pengakuan terhadap perlindungan data pribadi sebagai hak fundamental juga tercermin dalam perkembangan hukum internasional, seperti *General Data Protection Regulation (GDPR)* Uni Eropa. Hal ini menunjukkan adanya keselarasan prinsip antara hukum nasional dan standar global dalam perlindungan data pribadi. Dengan demikian, kedudukan data pribadi nasabah dalam sistem hukum Indonesia dapat dirumuskan sebagai berikut: Hak konstitusional yang

berakar pada perlindungan hak atas privasi; Hak keperdataan yang memberikan dasar bagi pengajuan klaim atas kerugian, Objek perlindungan hukum dalam kerangka negara hukum (*rechtsstaat*).

3. **Sinkronisasi UU PDP dengan Regulasi Sektor (OJK)** Perlindungan data pribadi nasabah dalam bank digital tidak hanya diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), tetapi juga dalam regulasi sektoral yang ditetapkan oleh Otoritas Jasa Keuangan (OJK). Oleh karena itu, sinkronisasi antara kedua rezim hukum tersebut diperlukan guna menjamin harmonisasi norma, kepastian hukum, dan efektivitas perlindungan data pribadi.
 - a. **Kedudukan UU PDP sebagai *Lex Generalis* dan Regulasi OJK sebagai *Lex Specialis*** UU PDP berkedudukan sebagai *lex generalis* karena mengatur perlindungan data pribadi secara menyeluruh lintas sektor, mencakup prinsip pemrosesan data, hak subjek data, serta mekanisme pertanggungjawaban. Sementara itu, regulasi OJK merupakan *lex specialis* yang mengatur secara teknis penyelenggaraan layanan perbankan, termasuk penggunaan teknologi informasi dan manajemen risiko. Hubungan keduanya bersifat komplementer, di mana UU PDP menjadi dasar normatif perlindungan hak, sedangkan regulasi OJK memperjelas aspek operasional di sektor perbankan. Dalam hal terjadi disharmonisasi, ketentuan UU PDP tetap menjadi rujukan utama karena memiliki kedudukan lebih tinggi dalam hierarki peraturan perundang-undangan. Dengan demikian, regulasi OJK berfungsi sebagai pelengkap yang memperkuat implementasi perlindungan data pribadi dalam praktik perbankan digital.
 - b. **Harmonisasi Prinsip Perlindungan Data dengan Manajemen Risiko Teknologi Informasi OJK** UU PDP menetapkan prinsip-prinsip dasar perlindungan data, seperti legalitas, pembatasan tujuan, minimalisasi data, akurasi, keamanan, dan akuntabilitas. Prinsip-prinsip tersebut mengharuskan pengendali data, termasuk bank digital, untuk menerapkan perlindungan teknis dan organisatoris, serta melakukan penilaian risiko terhadap pemrosesan data. Di sisi lain, regulasi OJK mewajibkan penerapan manajemen risiko teknologi informasi, termasuk pengamanan sistem, pengendalian akses, dan mitigasi risiko siber. Secara substansial, terdapat keselarasan antara prinsip keamanan dalam UU PDP dengan standar teknis yang ditetapkan OJK. Namun demikian, terdapat perbedaan orientasi, di mana regulasi OJK lebih menekankan stabilitas sistem keuangan, sedangkan UU PDP berfokus pada perlindungan hak individu. Oleh karena itu, harmonisasi keduanya menuntut agar pengamanan sistem tidak hanya berorientasi pada kepatuhan administratif, tetapi juga pada perlindungan hak privasi nasabah.

Integrasi kedua rezim hukum tersebut menciptakan sistem perlindungan berlapis (*multi-layered protection*), di mana UU PDP memberikan standar normatif, dan regulasi OJK memperkuat implementasi teknisnya. Dengan demikian, sinkronisasi keduanya menjadi prasyarat penting dalam mewujudkan perlindungan data pribadi yang efektif dalam penyelenggaraan bank digital.

Tabel 4.1
Perbandingan UU PDP dan Regulasi OJK

Aspek	UU PDP	Regulasi OJK	Analisis
Kedudukan	Lex Generalis	Lex Specialis	Bersifat komplementer
Fokus Perlindungan	Hak Subjek Data	Stabilitas & Manajemen Risiko	Orientasi berbeda
Hak Nasabah	Diatur eksplisit	Terbatas	UU PDP memperkuat posisi nasabah
Keamanan Sistem	Prinsip normatif	Standar teknis operasional	Saling melengkapi
Pengawasan	Otoritas PDP	OJK	Potensi overlapping

4. **Bentuk Perlindungan Preventif dan Represif terhadap Data Pribadi Nasabah dalam Penyelenggaraan Bank Digital** berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dibedakan menjadi perlindungan hukum preventif dan represif.
- a. **Perlindungan Hukum Preventif** Perlindungan hukum preventif merupakan upaya pencegahan terhadap pelanggaran data pribadi melalui pengaturan norma, kewajiban, dan mekanisme pengawasan sejak tahap awal pemrosesan data. Dalam konteks bank digital, perlindungan ini menjadi krusial mengingat tingginya intensitas pemrosesan data berbasis sistem elektronik. **Pengaturan Prinsip Pemrosesan Data Pribadi** UU PDP menetapkan prinsip-prinsip dasar seperti legalitas, pembatasan tujuan, minimalisasi data, akurasi, keamanan, dan akuntabilitas. Prinsip-prinsip ini berfungsi membatasi kewenangan pengendali data agar tidak terjadi penyalahgunaan atau pemrosesan data yang tidak sah sejak awal. **Kewajiban Memperoleh Persetujuan (Consent) yang Sah** Pemrosesan data harus didasarkan pada persetujuan yang bebas, spesifik, dan terinformasi. Dalam praktik bank digital, persetujuan diberikan secara elektronik, sehingga transparansi informasi menjadi syarat utama. Nasabah juga memiliki hak untuk menarik kembali persetujuan tersebut. **Kewajiban Menjamin Keamanan dan Kerahasiaan Data** Bank digital wajib menerapkan langkah teknis dan organisatoris, seperti enkripsi dan pengendalian akses, untuk mencegah kebocoran data. Kewajiban ini mencerminkan pendekatan berbasis risiko dan prinsip kehati-hatian dalam pengelolaan data. **Kewajiban Melakukan Penilaian Dampak Perlindungan Data (DPIA)** Dalam pemrosesan berisiko tinggi, pengendali data wajib melakukan DPIA guna mengidentifikasi dan memitigasi risiko sejak tahap perencanaan. Mekanisme ini mencerminkan pendekatan preventif berbasis risiko (*risk-based approach*). **Kewajiban Transparansi dan Pemberian Informasi** Pengendali data wajib memberikan informasi yang jelas mengenai tujuan pemrosesan, dasar hukum, jangka waktu penyimpanan, serta hak subjek data. Transparansi ini memastikan adanya kontrol dari nasabah terhadap data pribadinya dan mendukung terbentuknya *informed consent*.
- b. **Perlindungan Hukum Represif**
Perlindungan hukum represif merupakan bentuk perlindungan yang diberikan setelah terjadinya pelanggaran terhadap data pribadi. Berbeda dengan perlindungan preventif yang berorientasi pada pencegahan, perlindungan represif bertujuan menegakkan hukum, memulihkan hak subjek data, serta memberikan sanksi kepada pelaku pelanggaran. Dalam konteks bank digital, perlindungan ini menjadi penting mengingat tingginya risiko kebocoran data, peretasan sistem, dan penyalahgunaan informasi pribadi nasabah. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menyediakan instrumen berupa sanksi administratif, tanggung jawab perdata, dan sanksi pidana.
Sanksi Administratif Sanksi administratif merupakan instrumen utama yang bersifat korektif dan preventif untuk memastikan kepatuhan pengendali data. Bentuknya meliputi teguran tertulis, penghentian sementara pemrosesan data, penghapusan atau pemusnahan data, serta denda administratif. Sanksi ini dapat dikenakan apabila bank digital melanggar kewajiban, seperti tidak menjaga keamanan data, tidak memperoleh persetujuan yang sah, atau tidak melakukan notifikasi kebocoran data. Selain itu, pengawasan juga dilakukan oleh Otoritas Jasa Keuangan (OJK), sehingga tercipta sistem pengawasan berlapis. Secara konseptual, sanksi administratif berfungsi menegakkan kepatuhan sekaligus mencegah pelanggaran lanjutan.
Tanggung Jawab Perdata Tanggung jawab perdata memberikan hak kepada nasabah untuk menuntut ganti rugi atas kerugian yang timbul akibat pelanggaran data pribadi. Dasar hukumnya dapat merujuk pada perbuatan melawan hukum dalam Pasal 1365 KUHPerdata, dengan unsur perbuatan melawan hukum, kesalahan, kerugian, dan hubungan kausal. Dalam praktik bank digital, kerugian dapat berupa kerugian finansial, pencurian identitas, maupun kerugian immateriil. Mekanisme ini memiliki fungsi pemulihan (restoratif), sehingga memperkuat

posisi nasabah sebagai subjek data. Selain itu, tanggung jawab ini juga berkaitan dengan kewajiban bank menerapkan prinsip kehati-hatian dan manajemen risiko secara optimal.

Sanksi Pidana UU PDP juga mengatur sanksi pidana terhadap perolehan, pengungkapan, atau penggunaan data pribadi secara melawan hukum. Pelanggaran tersebut dapat dikenakan pidana penjara dan/atau denda, terutama jika dilakukan dengan sengaja untuk keuntungan tertentu. Sanksi pidana berfungsi sebagai ultimum remedium, yaitu upaya terakhir dalam penegakan hukum. Dalam konteks bank digital, pertanggungjawaban pidana dapat dikenakan tidak hanya kepada individu, tetapi juga kepada korporasi apabila pelanggaran terjadi secara sistemik. Dengan demikian, sanksi pidana memberikan efek jera sekaligus memperkuat perlindungan terhadap hak privasi nasabah.

B. Analisis Tanggung Jawab Hukum Bank Digital atas Kebocoran Data Pribadi Nasabah

Kebocoran data pribadi dalam penyelenggaraan bank digital merupakan pelanggaran terhadap hak subjek data sekaligus pelanggaran kewajiban hukum Pengendali Data Pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam hal ini, bank digital berkedudukan sebagai Pengendali Data Pribadi karena menentukan tujuan dan mengendalikan pemrosesan data nasabah. Oleh karena itu, setiap kegagalan dalam perlindungan data menimbulkan konsekuensi tanggung jawab hukum.

1. **Tanggung Jawab Administratif** timbul akibat pelanggaran kewajiban hukum publik oleh bank digital sebagai Pengendali Data Pribadi. UU PDP memberikan kewenangan kepada otoritas pengawas untuk menjatuhkan sanksi administratif berupa teguran tertulis, penghentian sementara pemrosesan data, penghapusan atau pemusnahan data, serta denda administratif. Tanggung jawab ini muncul apabila kebocoran data terjadi akibat kelalaian, seperti kegagalan menerapkan sistem keamanan yang memadai, tidak melakukan penilaian dampak perlindungan data (DPIA), atau tidak melakukan pemberitahuan kepada subjek data dan otoritas terkait. Sanksi administratif berfungsi korektif untuk memperbaiki pelanggaran, sekaligus preventif guna mencegah terulangnya pelanggaran serupa. Selain tunduk pada UU PDP sebagai *lex generalis*, bank digital juga berada di bawah pengawasan Otoritas Jasa Keuangan (OJK) sebagai regulator sektoral. Dengan demikian, kebocoran data dapat menimbulkan sanksi administratif ganda (dual regulatory exposure). Secara konseptual, tanggung jawab administratif ini mencerminkan prinsip **akuntabilitas** dan **kehati-hatian**, di mana bank digital dituntut memiliki standar perlindungan data yang tinggi. Kegagalan memenuhi standar tersebut tidak hanya merupakan kesalahan teknis, tetapi juga pelanggaran terhadap prinsip tata kelola yang baik (*good corporate governance*).
2. **Tanggung Jawab Hukum dalam Hukum Perdata** merupakan bentuk pertanggungjawaban atas pelanggaran hak subjek data yang menimbulkan kerugian, serta berfungsi sebagai mekanisme pemulihan (*restorative mechanism*). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan hak kepada nasabah untuk mengajukan gugatan dan memperoleh ganti rugi, sehingga perlindungan data pribadi juga memiliki dimensi hukum privat. Dalam konteks kebocoran data, tanggung jawab perdata dapat didasarkan pada perbuatan melawan hukum (PMH) sebagaimana Pasal 1365 KUHPerdata, dengan unsur adanya perbuatan melawan hukum, kesalahan, kerugian, dan hubungan kausal. Kelalaian bank dalam menjaga keamanan sistem, pengawasan internal, atau kerahasiaan data dapat memenuhi unsur tersebut apabila menimbulkan kerugian, baik finansial maupun non-finansial. Selain itu, tanggung jawab bank digital juga mencakup tanggung jawab korporasi. Bank sebagai badan hukum bertanggung jawab atas tindakan pegawai dalam lingkup pekerjaannya (*vicarious liability*). Dengan demikian, tanggung jawab perdata tidak hanya timbul akibat kesengajaan, tetapi juga akibat kelalaian dalam pengelolaan data.
3. **Pertanggungjawaban Pidana Korporasi (Corporate Liability)** Tanggung jawab pidana dalam UU PDP timbul apabila pelanggaran data pribadi dilakukan secara sengaja dan melawan hukum. Perbuatan seperti memperoleh, mengungkapkan, menggunakan, atau memalsukan data pribadi tanpa hak dapat dikenakan pidana penjara dan/atau denda. Dalam praktik bank digital, pertanggungjawaban pidana dapat muncul, antara lain, dalam

hal:penyalahgunaan data oleh pegawai internal, kerja sama ilegal dengan pihak ketiga, pembiaran celah keamanan yang diketahui, penggunaan data secara sengaja untuk kepentingan tertentu. Penerapan pidana mensyaratkan adanya unsur kesalahan (*mens rea*). Tidak semua kebocoran data berimplikasi pidana; jika terjadi karena kelalaian, maka mekanisme administratif atau perdata lebih tepat. Hal ini sejalan dengan asas *ultimum remedium*, yaitu hukum pidana sebagai upaya terakhir. UU PDP juga mengakui pertanggungjawaban pidana korporasi, sehingga bank digital sebagai badan hukum dapat dimintakan pertanggungjawaban apabila pelanggaran terjadi dalam lingkup kegiatan usahanya atau akibat lemahnya pengawasan internal. Dengan demikian, sanksi pidana berfungsi sebagai instrumen represif untuk memberikan efek jera, namun penerapannya harus tetap proporsional agar tidak menimbulkan over-kriminalisasi dalam sektor jasa keuangan.

Tabel 4.2

Perbandingan Tanggung Jawab Hukum Bank Digital atas Kebocoran Data Pribadi Nasabah Berdasarkan UU No. 27 Tahun 2022

No	Jenis Tanggung Jawab	Dasar Hukum	Sifat Pelanggaran	Bentuk Sanksi/Konsekuensi	Tujuan Penegakan
1	Administratif	Pasal 57-58 UU PDP	Pelanggaran kewajiban administratif (keamanan, transparansi, DPIA, notifikasi kebocoran)	Teguran tertulis, penghentian sementara pemrosesan data, penghapusan data, denda administratif	Korektif dan preventif (mendorong kepatuhan)
2	Perdata	Pasal 12 UU PDP jo. Pasal 1365 KUHPerdata	Kerugian akibat kelalaian atau kesalahan dalam pemrosesan data	Ganti rugi materiil dan/atau immateriil	Restoratif (pemulihan hak nasabah)
3	Pidana	Pasal 65-70 UU PDP	Perolehan, pengungkapan, penggunaan data secara melawan hukum dan/atau disengaja	Pidana penjara dan/atau denda, termasuk pidana terhadap korporasi	Represif dan efek jera (<i>ultimum remedium</i>)

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menempatkan bank digital sebagai Pengendali Data Pribadi yang memiliki kewajiban hukum untuk menerapkan prinsip-prinsip pemrosesan data, memperoleh persetujuan yang sah, menjamin transparansi, menjaga keamanan dan kerahasiaan data, serta melakukan Penilaian Dampak Perlindungan Data (DPIA). Pengaturan ini menunjukkan pergeseran paradigma menuju perlindungan data berbasis hak individu (*rights-based approach*). Perlindungan hukum terhadap data pribadi nasabah dalam penyelenggaraan bank digital terdiri atas perlindungan preventif dan represif yang saling melengkapi, di mana perlindungan preventif diwujudkan melalui pengaturan prinsip pemrosesan data, kewajiban transparansi, consent, sistem keamanan, dan DPIA, sedangkan perlindungan represif diwujudkan melalui sanksi administratif, tanggung jawab perdata, dan sanksi pidana.

Selanjutnya, tanggung jawab hukum bank digital atas kebocoran data pribadi bersifat kumulatif, meliputi tanggung jawab administratif, perdata, dan pidana. Kebocoran data yang terjadi akibat kelalaian menimbulkan konsekuensi sanksi administratif dan tanggung jawab perdata, sedangkan pelanggaran yang dilakukan dengan unsur kesengajaan dapat berimplikasi pidana, termasuk pertanggungjawaban pidana korporasi. Dalam hal ini, sinkronisasi antara UU PDP sebagai *lex generalis* dan regulasi sektoral Otoritas Jasa Keuangan sebagai *lex specialis* menjadi faktor

penting dalam menjamin kepastian hukum serta perlindungan yang optimal bagi nasabah bank digital.

REFERENSI

Buku

- Abimanyu, Anggito. *Hukum Perlindungan Data Pribadi di Indonesia: Antara Regulasi dan Praktik*. Jakarta: Sinar Grafika, 2023.
- Achmad Ali. *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan*. Jakarta: Kencana, 2017.
- Achmad Ali dan Wiwie Heryani. *Menjelajahi Kajian Empiris terhadap Hukum*. Jakarta: Prenadamedia Group, 2022.
- Albanjari, Fatkhur Rohman dkk. *Lembaga Keuangan Syariah*. Bandung: Media Sains Indonesia, 2020.
- Arief, Barda Nawawi. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*. Jakarta: Kencana, 2023.
- Budhijanto, Danrivanto. *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi*. Bandung: Refika Aditama, 2019.
- Djafar, Wahyudi. *Hukum Perlindungan Data Pribadi*. Jakarta: Elsam, 2022.
- Fuady, Munir. *Teori-Teori Besar (Grand Theory) dalam Hukum*. Jakarta: Prenadamedia Group, 2017.
- Hadjon, Philipus M. *Perlindungan Hukum bagi Rakyat di Indonesia*. Surabaya: Bina Ilmu, 2019.
- Hadjon, Philipus M. *Perlindungan Hukum bagi Rakyat Indonesia*. Jakarta: Rajawali Pers, 2020.
- HR, Ridwan. *Hukum Administrasi Negara*. Jakarta: Rajawali Pers, 2020.
- Ibrahim, Johnny. *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia Publishing, 2021.
- Indrati, Maria Farida. *Ilmu Perundang-undangan: Proses dan Teknik Pembentukannya*. Yogyakarta: Kanisius, 2017.
- Kristanto, Kiki dkk. *Transformasi Hukum dalam Era Revolusi Teknologi Blockchain*. Medan: PT Media Penerbit Indonesia, 2024.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2020.
- Makarim, Edmon. *Hukum Telematika dan Perlindungan Data Pribadi di Indonesia*. Depok: Rajawali Pers, 2023.
- Mertokusumo, Sudikno. *Mengenal Hukum: Suatu Pengantar*. Yogyakarta: Cahaya Atma Pustaka, 2019.
- Rahardjo, Satjipto. *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2014.
- Rahardjo, Satjipto. *Hukum dan Perubahan Sosial*. Yogyakarta: Genta Publishing, 2020.
- Riswandi, Budi Agus. *Hukum Perlindungan Data Pribadi di Indonesia*. Yogyakarta: UII Press, 2020.
- Rosadi, Sinta Dewi. *Perlindungan Data Pribadi di Indonesia: Konsep dan Implementasinya*. Bandung: Refika Aditama, 2023.
- Shidarta. *Hukum Perlindungan Konsumen Indonesia*. Jakarta: Grasindo, 2018.
- Sitompul, Josua. *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2021.
- Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: UI Press, 2019.
- Soekanto, Soerjono dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: RajaGrafindo Persada, 2019.
- Suhariyanto, Budi. *Perlindungan Data Pribadi dan Tantangan Era Digital di Indonesia*. Jakarta: (jika buku, sesuaikan penerbit), 2023.

Jurnal / Artikel Ilmiah

- Alfitri, Nur Alfiana, Rahmawati, dan Firmansyah. "Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024). Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022 | Journal Social Society
- Aritonang, Lenny Maria, Zyetwill, dan Rara Handayani. "Analisis Hukum terhadap Kebocoran Data Pribadi dan Penyalahgunaan Identitas dalam Perbankan." *Ranah Research Journal* 7, no. 5 (2025). Vol. 7 No. 5 (2025): Ranah Research : Journal Of Multidisciplinary Research and Development | Ranah Research : Journal of Multidisciplinary Research and Development

- Argiansyah, Hikmal Yusuf, dan M. Rizki Yudha Prawira. "Analisis Hukum Hak Atas Privasi dan Perlindungan Data Pribadi." *Jurnal Hukum Pelita* 5, no. 1 (2024). (PDF) Analisis Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia
- Aziz, Muhammad Faisal, Hamzah, dan Sepriyadi Adhan S. "Perlindungan Hukum terhadap Nasabah atas Penyalahgunaan Data Pribadi." *Al-Zayn: Jurnal Ilmu Sosial dan Hukum* 3, no. 6 (2025).
- Hosnah, Asmak Ul dkk. "Analisis Perlindungan Data Pribadi dalam Implementasi Undang-Undang Nomor 27 Tahun 2022 di Era Artificial Intelligence." *QAWIUN* 1, no. 2 (2026).
- Muchamad Nurdin Alwi, dkk. "Tantangan dan Peluang Perbankan Digital." *Jurnal Cahaya Mandalika* (2024). (PDF) Tantangan dan Peluang Perbankan Digital: Studi Kasus Inovasi Keuangan dan Transformasi Perbankan
- Nasution, Alvin Hamzah. "The Urgency of Customer Personal Data Protection in Digital Banking." *Rechtsvinding* 3, no. 1 (2025).
- Rahmadani, Ardita Esti, Yoga Pangestu, dan Nur Halizhah. "Perlindungan Data Pribadi di Era Digital." *Media Hukum Indonesia* 2, no. 4 (2024). Perlindungan Data Pribadi di Era Digital: Tantangan dan Solusi Dalam Sistem Perbankan | Rahmadani | Media Hukum Indonesia (MHI)
- Rinjani, Muhamad Adri dan Ricky Firmansyah. "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum* 8, no. 1 (2025).
- Rizieq, Muhammad. "Transformasi Layanan Perbankan." *BanKu: Jurnal Perbankan dan Keuangan* 5, no. 2 (2024).
[bing.com/ck/a?!&&p=0f65dfe59d881c1bc2c5d9598ef17b7b1e16264956c069cca41d60bde8408550JmltdHM9MTc3MDE2MzIwMA&ptn=3&ver=2&hsh=4&fclid=252f4c7e-9bed-687b-170c-5ab49a646932&psq=Rizieq%2c+Muhammad.+%2c+Transformasi+Layanan+Perbankan.+BanKu%3a+Jurnal+Perbankan+dan+Keuangan+5%2c+no.+2+\(2024\).&u=a1aHR0cHM6Ly9qdXJuYWwudW5zaWwuYWMuaWQvaW5kZXgucGhwL2Jhbmt1L2FydGljbGUvZG93bmxxvYWQvMTMyMTcvcGRm&ntb=1](https://www.bing.com/ck/a?!&&p=0f65dfe59d881c1bc2c5d9598ef17b7b1e16264956c069cca41d60bde8408550JmltdHM9MTc3MDE2MzIwMA&ptn=3&ver=2&hsh=4&fclid=252f4c7e-9bed-687b-170c-5ab49a646932&psq=Rizieq%2c+Muhammad.+%2c+Transformasi+Layanan+Perbankan.+BanKu%3a+Jurnal+Perbankan+dan+Keuangan+5%2c+no.+2+(2024).&u=a1aHR0cHM6Ly9qdXJuYWwudW5zaWwuYWMuaWQvaW5kZXgucGhwL2Jhbmt1L2FydGljbGUvZG93bmxxvYWQvMTMyMTcvcGRm&ntb=1)
- Suhariyanto, Budi. "Urgensi Perlindungan Data Pribadi dalam Era Ekonomi Digital di Indonesia." *Jurnal RechtsVinding* 9, no. 2 (2020).

Peraturan Perundang-undangan

- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.
- Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek).
- Peraturan Otoritas Jasa Keuangan Nomor 7/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.
- Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.

Sumber Internet / Laporan Resmi

- Otoritas Jasa Keuangan. *Perkembangan Layanan Perbankan Digital di Indonesia*. 2019.
- Otoritas Jasa Keuangan. *Cetak Biru Transformasi Digital Perbankan Indonesia*. Jakarta: OJK, 2021.
- Tempo.co. "Polemik Data Pribadi: 5 Kasus Kebocoran Data di Indonesia Selama 2023–2024." Juli 2025.