JIIC: JURNAL INTELEK INSAN CENDIKIA
https://jicnusantara.com/index.php/jiic
Vol : 03 No: 05, Mei 2026
E-ISSN : 3047-7824

Perlindungan Konsumen dalam Layanan Perbankan Digital di Era Financial Teknologi

Consumer Protection in Digital Banking Services in the Era of Financial Technology

Baidhowi[1], Edo Munawwar[2], Muhammad Fadli Dwi Anugrah[3*], Wanda Hamidah[4], Aldina Rachmadian[5], Revalina Dewi Roshinta
Ilmu Hukum Fakultas, Hukum,Universitas Negeri Semarang
Email: baidhowi@mail.unnes.ac.id[1], edomunawwar86@students.unnes.unnes.ac.id[2], mfadlidwianugrah06@students.unnes.ac.id[3], wandahamidah15@students.unnes.ac.id[4], aldinarm@students.unnes.ac.id[5], revalinaroshinta@students.unned.ac.id[6]*

Article Info

Article history:
Received : 03-05-2026
Revised : 05-05-2026
Accepted : 07-05-2026
Pulished : 09-05-2026

Abstract

The digital transformation in the banking sector has encouraged the emergence of various technology-based financial service innovations, such as mobile banking, internet banking, and integration with financial technology (fintech). These developments provide convenience, improve efficiency, and expand public access to conducting various financial transactions. However, behind these benefits, the digitalization of banking also introduces new risks, particularly those related to cybercrime and personal data breaches that may potentially harm customers. This study aims to examine the effectiveness of personal data protection regulations in ensuring the security of customer transactions in digital banking services, as well as to analyze the legal responsibility of banks for losses suffered by customers due to failures in digital security systems. The method used in this research is normative legal research with statutory and conceptual approaches. The primary legal materials include Law Number 8 of 1999 concerning Consumer Protection, Law Number 27 of 2022 concerning Personal Data Protection, as well as various regulations in the financial services sector. The results of the study indicate that, normatively, Indonesia already has a relatively adequate regulatory framework to protect customers. However, in its implementation, several challenges remain, such as rapid technological developments, increasing threats of cybercrime, potential overlapping authority among supervisory institutions, and the low level of public digital literacy. Therefore, it is necessary to strengthen supervision, improve banking system security standards, and enhance cooperation between the government, financial institutions, and the public in order to create a secure and trustworthy digital banking ecosystem.

Keywords: consumer protection, digital banking, personal data protection

Abstrak

Transformasi digital di sektor perbankan telah mendorong lahirnya berbagai inovasi layanan keuangan, seperti mobile banking, internet banking, serta integrasi dengan teknologi finansial (financial technology). Perkembangan tersebut memberikan kemudahan bagi masyarakat dalam mengakses layanan keuangan secara lebih cepat, efisien, dan tanpa batasan ruang dan waktu. Namun demikian, di balik berbagai kemudahan tersebut, digitalisasi perbankan juga menimbulkan konsekuensi berupa meningkatnya risiko kejahatan siber dan kebocoran data pribadi yang berpotensi merugikan nasabah sebagai pengguna layanan perbankan. Kondisi ini menimbulkan kebutuhan akan perlindungan hukum yang memadai untuk menjamin keamanan data dan transaksi nasabah dalam ekosistem perbankan digital. Penelitian ini bertujuan untuk menganalisis efektivitas regulasi perlindungan data pribadi dalam menjamin keamanan transaksi nasabah pada layanan perbankan digital serta mengkaji tanggung jawab hukum bank terhadap kerugian yang dialami

nasabah akibat kegagalan sistem keamanan digital. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Sumber data penelitian terdiri dari bahan hukum primer berupa peraturan perundang-undangan, seperti Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta regulasi di sektor jasa keuangan. Selain itu, penelitian ini juga menggunakan bahan hukum sekunder yang diperoleh dari buku, artikel jurnal ilmiah, dan hasil penelitian sebelumnya yang relevan. Data dianalisis secara kualitatif dengan menelaah ketentuan hukum yang berlaku serta implementasinya dalam praktik perlindungan nasabah pada layanan perbankan digital. Hasil penelitian menunjukkan bahwa secara normatif regulasi perlindungan data pribadi di Indonesia telah memberikan dasar hukum yang cukup kuat dalam melindungi kepentingan nasabah

Kata kunci: perlindungan konsumen, perbankan digital, perlindungan data pribadi.

PENDAHULUAN

Pesatnya transformasi digital dalam sektor perbankan membawa tantangan baru berupa risiko kejahatan siber yang semakin kompleks, sehingga memicu urgensi evaluasi terhadap instrumen hukum yang berlaku saat ini. Fokus utama dalam diskursus ini adalah bagaimana efektivitas regulasi perlindungan data pribadi dalam menjamin keamanan transaksi nasabah pada ekosistem perbankan digital. Mengingat kebocoran data sering kali menjadi pintu masuk bagi kerugian finansial yang masif. Kondisi tersebut memunculkan persoalan pelik mengenai kepastian hak konsumen, terutama terkait dengan sejauh mana tanggung jawab hukum bank terhadap kerugian nasabah yang disebabkan oleh kegagalan sistem keamanan digital. Ketidakjelasan batasan tanggung jawab ini berisiko menciptakan celah hukum yang merugikan nasabah sebagai pihak yang memiliki posisi tawar lebih rendah dalam kontrak elektronik perbankan.

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam cara masyarakat melakukan transaksi keuangan. Saat ini, transaksi keuangan digital menjadi pilihan utama bagi banyak konsumen karena menawarkan kemudahan, kecepatan, dan efisiensi dalam berbagai aktivitas finansial. Namun, di balik kemudahan tersebut, muncul berbagai risiko baru yang perlu diwaspadai, terutama yang berkaitan dengan keamanan data dan transaksi digital. Oleh karena itu, perlindungan konsumen dalam ruang digital menjadi tantangan tersendiri bagi regulator maupun pelaku industri keuangan. Kondisi ini menuntut adanya peninjauan kembali terhadap kerangka hukum yang berlaku agar tetap relevan dengan perkembangan teknologi finansial yang terus berkembang.

Perkembangan layanan keuangan digital di Indonesia menunjukkan pertumbuhan yang sangat pesat. Pada tahun 2023, total transaksi e-wallet tercatat mencapai Rp513 triliun atau meningkat sekitar 42% dibandingkan tahun sebelumnya. Saat ini terdapat lebih dari 50 penyedia layanan e-wallet yang telah memperoleh izin resmi, 103 platform peer-to-peer lending dengan total penyaluran pinjaman mencapai Rp71,4 triliun, serta 41 platform securities crowdfunding yang telah berhasil mendanai sekitar 800 UMKM dengan nilai pembiayaan mencapai Rp2,1 triliun. Regulasi yang mengatur sektor ini antara lain Peraturan Bank Indonesia Nomor 20/6/PBI/2018 terkait uang elektronik, POJK Nomor 77/POJK.01/2016 mengenai peer-to-peer lending, serta POJK Nomor 57/POJK.04/2020 yang mengatur securities crowdfunding.

Meskipun demikian, tantangan di bidang keamanan masih cukup besar, mengingat sekitar 41% kasus kejahatan siber berkaitan dengan layanan fintech dengan rata-rata kerugian sebesar Rp3,7 juta per kasus. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data

Pribadi menjadi langkah penting dalam memperkuat perlindungan terhadap data pengguna. Selain itu, diperlukan koordinasi yang lebih efektif antara Bank Indonesia, Otoritas Jasa Keuangan, dan Kementerian Komunikasi dan Informatika, serta peningkatan literasi digital masyarakat guna menciptakan ekosistem keuangan digital yang aman dan inklusif (Nugroho, 2020).(Langkat & Budi, 2025)

Konsumen sebagai pihak yang menggunakan produk atau jasa memiliki hak untuk memperoleh perlindungan hukum atas kepentingannya. Pada dasarnya, perlindungan hukum terhadap konsumen telah diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Namun, pengaturan yang lebih khusus mengenai perlindungan konsumen dalam sektor jasa keuangan diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Berdasarkan Pasal 1 angka 3 peraturan tersebut, yang dimaksud dengan konsumen adalah setiap pihak yang menempatkan dana dan/atau memanfaatkan layanan yang disediakan oleh lembaga jasa keuangan. Pihak tersebut antara lain meliputi nasabah pada sektor perbankan, pemodal di pasar modal, pemegang polis pada sektor perasuransian, serta peserta dana pensiun sebagaimana diatur dalam peraturan perundang-undangan di bidang jasa keuangan.

Isu perlindungan data pribadi konsumen semakin menjadi perhatian penting di era digital, terutama karena berbagai data sensitif seperti informasi pembayaran, alamat, dan preferensi belanja memiliki potensi tinggi untuk disalahgunakan dalam aktivitas transaksi elektronik, termasuk perbankan. Pengesahan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022 merupakan langkah strategis pemerintah dalam memperkuat jaminan hukum terhadap keamanan data pribadi masyarakat. Namun demikian, efektivitas implementasi regulasi tersebut masih menghadapi berbagai kendala, salah satunya terkait dengan belum optimalnya koordinasi antara UU PDP dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK), yang pada dasarnya memiliki tujuan saling melengkapi dalam memberikan perlindungan menyeluruh terhadap hak-hak konsumen. (Pdp, 2026)

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang berfokus pada analisis terhadap norma-norma hukum yang terdapat dalam peraturan perundang-undangan serta berbagai literatur hukum yang berkaitan dengan isu yang diteliti. Metode ini digunakan untuk mengkaji efektivitas regulasi perlindungan data pribadi dalam menjamin keamanan transaksi nasabah pada layanan perbankan digital, sekaligus menganalisis tanggung jawab hukum pihak bank terhadap kerugian yang dialami nasabah akibat terjadinya kegagalan sistem keamanan digital. Dalam penelitian ini digunakan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai ketentuan hukum yang mengatur mengenai perlindungan konsumen dan perlindungan data pribadi, antara lain Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta sejumlah regulasi di sektor jasa keuangan yang dikeluarkan oleh Otoritas Jasa Keuangan dan Bank Indonesia. Sementara itu, pendekatan konseptual digunakan untuk memahami berbagai konsep hukum yang berkaitan dengan perlindungan konsumen, tanggung jawab pelaku usaha, serta prinsip-prinsip perlindungan data dalam sistem perbankan digital.

HASIL DAN PEMBAHASAN

Efektivitas regulasi perlindungan data pribadi dalam menjamin keamanan transaksi nasabah pada ekosistem perbankan digital.

1. Konsep Perlindungan Konsumen dan Hak-Hak Nasabah Bank.

Pada dasarnya hukum memiliki tujuan untuk melindungi kepentingan manusia serta menjaga hak-hak yang melekat pada setiap orang. Oleh karena itu, hukum harus diterapkan secara konsisten dan tegas agar dapat berjalan dengan baik. Hukum seharusnya mampu menciptakan kehidupan masyarakat yang tertib, damai, dan teratur. Namun, ketika terjadi pelanggaran terhadap aturan hukum yang berlaku maka diperlukan adanya penegakan hukum untuk menindak pelanggaran tersebut. Agar penegakan hukum dapat berjalan dengan baik, diperlukan adanya kepastian hukum yang jelas sehingga dapat memberikan perlindungan yang adil bagi masyarakat terhadap berbagai permasalahan yang muncul. Dengan adanya kepastian hukum, masyarakat akan merasa lebih aman karena dapat menciptakan kondisi yang selaras, tertib, dan memberikan rasa keadilan dalam kehidupan Bersama.(April, 2025)

Konsep keadilan pertama kali dicetuskan oleh Aristoteles. Intinya, keadilan itu memberikan apa yang memang menjadi hak seseorang (fiat jutitia bereat mundus). Dia membagi keadilan jadi dua jenis: (Meji, P. (2019). Konsep keadilan menurut Aristoteles dalam buku Nicomachean ethics buku lima (Doctoral dissertation, Widya Mandala Catholic University Surabaya).

a. Keadilan Distributif

Ini tugasnya pemerintah atau pembuat undang-undang untuk membagi hak, hadiah, atau fasilitas ke masyarakat secara proporsional. Jadi, pembagiannya didasarkan pada kontribusi atau porsi masing-masing.

b. Keadilan Korektif

Kalau ini lebih ke ranah hukum untuk mencegah pelanggaran. Fokusnya adalah mengembalikan keadaan ke posisi semula. Misalnya, hakim memerintahkan ganti rugi atau pengembalian barang milik korban supaya semuanya kembali adil seperti sebelum kejadian.

Secara prinsip, setiap orang berhak mendapatkan keadilan dalam memenuhi kebutuhan hidupnya. Salah satu instrumen penting untuk menjaga hak tersebut adalah melalui sistem perlindungan konsumen. Dalam dunia bisnis, konsep ini sangat krusial untuk menjamin bahwa produk atau jasa yang dibeli masyarakat benar-benar berkualitas dan sesuai harapan. Pemerintah sendiri telah merumuskan UU No. 8 Tahun 1999 sebagai dasar hukum untuk menciptakan kepastian bagi konsumen. Namun, tanggung jawab ini tidak hanya dipikul oleh negara para pelaku usaha pun berkewajiban menjaga hak pembeli mereka. Jadi, perlindungan konsumen adalah bentuk sinergi antara regulasi pemerintah dan etika bisnis para pengusaha demi menciptakan pasar yang sehat

Langkah menciptakan kepastian hukum bagi konsumen sebenarnya punya tujuan yang lebih besar dari sekadar menghukum pelaku usaha yang nakal dengan ganti rugi. Fokusnya adalah memberikan proteksi nyata bagi masyarakat sekaligus mengedukasi pebisnis agar lebih sadar akan etika perlindungan konsumen. Secara hukum, cakupannya pun sangat luas; tidak

hanya lewat jalur perdata, tapi juga melibatkan aturan administrasi untuk pengawasan serta hukum pidana untuk sanksi yang lebih berat. Intinya, perlindungan konsumen adalah sinergi berbagai bidang hukum demi menciptakan ekosistem bisnis yang jujur, adil, dan sehat bagi siapa saja.

Dalam dunia perbankan, perlindungan hukum bagi nasabah umumnya terbagi menjadi dua mekanisme utama. Metode pertama adalah perlindungan tidak langsung, di mana fokusnya adalah memitigasi risiko kerugian yang muncul akibat kebijakan atau operasional bisnis bank itu sendiri. Sementara itu, metode kedua adalah perlindungan langsung, yang memberikan ruang bagi nasabah untuk melakukan pembelaan secara personal terhadap potensi risiko yang merugikan mereka. (Pamuji, R. A. (2018). (Pamuji, n.d.)hukum sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK). Dalam regulasi ini ditegaskan bahwa perlindungan diprioritaskan bagi konsumen akhir. Jika merujuk pada Pasal 1 ayat (2) UUPK, nasabah secara sah dikategorikan sebagai konsumen akhir. Oleh karena itu, segala bentuk interaksi dan hubungan hukum yang terjalin antara nasabah dengan pihak bank berada di bawah payung hukum UUPK, yang mengatur hak dan kewajiban antara konsumen dan pelaku usaha secara komprehensif.(Hukum et al., 2022)

Agar implementasi perlindungan konsumen berjalan efektif, seseorang harus memenuhi kriteria yang diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK). Berdasarkan aturan ini, perlindungan hukum ditujukan khusus bagi konsumen akhir yaitu mereka yang menggunakan barang atau jasa untuk keperluan pribadi atau rumah tangga bukan untuk diputar kembali sebagai modal usaha atau bisnis. Merujuk pada Pasal 1 ayat (2) UUPK, nasabah secara otomatis masuk ke dalam klasifikasi konsumen akhir tersebut. UUPK sendiri tidak hanya berfungsi sebagai landasan hak dan kewajiban tetapi juga sebagai instrumen yang mengatur hubungan hukum antara nasabah dan pihak bank. Tujuannya adalah untuk menciptakan pola interaksi yang lebih transparan, adil, dan seimbang antara pengguna jasa dan penyedia layanan keuangan.

Perlindungan nasabah adalah hak yang melekat di setiap transaksi, bukan sekadar beban bagi pelaku usaha. Di era digital ini, perbankan di Indonesia seharusnya sudah menetapkan standar keamanan yang solid untuk menjaga kepentingan nasabah dari ancaman *cyber attack*. Implementasi Pasal 7 huruf D dan G menjadi krusial di sini. Manajemen bank punya kewajiban hukum untuk memastikan bahwa layanan yang mereka berikan memenuhi standar mutu. Jadi, pihak bank dilarang keras memasarkan produk finansial tanpa adanya kepastian keamanan yang valid bagi penggunanya.

Dalam upaya standardisasi, integrasi elemen HSE (Health, Safety, Security, and Environment) menjadi hal yang sangat krusial. Hal ini mengingat sektor perbankan sangat bergantung pada aspek keamanan terutama dalam penggunaan produk digitalisasi. Namun kenyataannya, penerapan standar keamanan pada platform digital perbankan masih memiliki celah besar. Hal ini terbukti dari kasus serangan siber oleh kelompok *LockBit* yang berhasil membobol data nasabah dengan relatif mudah.Sebagai bentuk pertanggungjawaban, pihak bank wajib memberikan ganti rugi kepada nasabah yang terdampak. Proses penyelesaian sengketa ini sejalan dengan misi pemerintah dalam memberikan perlindungan konsumen, sebagaimana diatur dalam UU No. 21 Tahun 2011 tentang OJK. Oleh karena itu, masyarakat atau nasabah yang

merasa dirugikan dapat melayangkan pengaduan secara resmi kepada Otoritas Jasa Keuangan (OJK) demi menjamin hak-hak mereka

Kasus kebocoran data ini secara nyata telah mencederai prinsip etika, privasi, dan keamanan informasi digital. Akibat pencurian data tersebut, sektor perbankan di Indonesia harus menghadapi krisis terkait aspek kerahasiaan, integritas, hingga ketersediaan data nasabah. Tidak hanya di sektor finansial, insiden ini juga berdampak buruk pada operasional layanan kesehatan nasional, baik dari segi kerugian finansial maupun reputasi. Ujung-ujungnya rentetan masalah ini memicu krisis kepercayaan di tengah masyarakat terhadap keamanan siber di Indonesia.

2. Transformasi Layanan Perbankan Konvensional ke Era Digital

Transformasi layanan perbankan dari sistem yang sebelumnya konvensional menuju ke sistem digital merupakan salah satu bentuk adaptasi sistem sektor keuangan terhadap perkembangan teknologi informasi dan teknologi komunikasi yang saat ini semakin pesat. Perubahan ini tidak hanya bersifat teknis-operasional, tetapi juga menyentuh aspek fundamental dalam hubungan antara bank dan nasabah. Jika pada sebelumnya interaksi dilakukan secara langsung melalui kantor cabang, kini hubungan tersebut bergeser menjadi berbasis sistem elektronik yang mengandalkan jaringan internet dan perangkat digital.(Anjheli, 2024)

Digitalisasi perbankan melahirkan berbagai inovasi layanan, seperti mobile banking, internet banking, digital payment, hingga integrasi dengan ekosistem financial technology (fintech). Transformasi ini memberikan berbagai keuntungan, antara lain efisien operasional, kemudahan akses layanan tanpa batas ruang dan waktu, serta peningkatan inklusi keuangan.(Kholis, 2024) Namun demikian, di balik kemudahan tersebut terdapat konsekuensi berupa meningkatnya resiko terhadap keamanan data pribadi dan transaksi nasabah.(Abigael, 2024)

Dalam ekosistem perbankan digital, data pribadi merupakan elemen utama yang menopang seluruh aktivitas layanan. Data tersebut mencakup informasi identitas, nomor rekening, data biometrik, hingga history transaksi keuangan. Data ini memiliki nilai ekonomi yang tinggi serta menjadi target utama kejahatan siber. Oleh karena itu, perlindungan data pribadi tidak hanya menjadi isu teknis, tetapi juga menjadi isu hukum dan hak asasi manusia yang harus dijamin oleh negara. Sebagai bentuk perlindungan hukum, Indonesia telah mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang berfungsi sebagai payung hukum dalam mengatur pengelolaan data pribadi. regulasi ini menjadi instrumen penting dalam memastikan bahwa setiap proses pengumpulan, pengolahan, penyimpanan, dan distribusi data dilakukan secara sah, dan transparan. Dalam konteks perbankan digital, UU PDP menjadi dasar bagi bank dan penyelenggara sistem elektronik untuk menerapkan standar keamanan yang tinggi dalam melindungi data-data nasabah.(Palopo, 2025)

Efektifitas regulasi perlindungan data pribadi dalam menjamin keamanan transaksi nasabah dapat dianalisis melalui beberapa pendekatan, baik secara normatif maupun empiris. Dari perspektif normatif, regulasi perlindungan data pribadi di Indonesia telah mengadopsi prinsip-prinsip universal yang juga diterapkan dalam berbagai rezim hukum internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa. Prinsip-prinsip tersebut antara lain meliputi keabsahan pemrosesan data (lawfulness), pembatasan tujuan (purpose

limitation), minimalisasi data (data minimization), akurasi data, serta akuntabilitas pengendali data.(Dan & Pengaturan, 2024) Penerapan prinsip-prinsip ini dalam sektor perbankan mewajibkan bank untuk mengelola data nasabah secara hati-hati dan bertanggung jawab, serta tidak menyalahgunakan data untuk kepentingan di luar tujuan yang telah disepakati.

Tabel Tantangan Era Lama vs Era Digital.

Aspek	Erap Erbankan Konvensional	Era Digital Dan Fintech
Sistem Transaksi	Tatap muka di kantor bank	Online melalui aplikasi
Risiko utama	Kesalahan administrasi	Cyber crime dan hacking
Perlindungan konsumen	Berbasis kontrak fisik	Berbasis sistem digital
Data Nasabah	Disimpan secara manual	Disimpan secara elektronik
Pengawasan	Relatif sederhana	Membutuhkan sistem pengawasan Teknologi
Ancaman kejahatan	Penipuan konvesional	Phising, malware,pencurian data

Selain itu, tujuan regulasi juga memberikan pengakuan terhadap hak-hak subjek data, seperti hak untuk memperoleh informasi, hak untuk mengakses data, hak untuk memperbaiki data dalam kondisi tertentu. Pengakuan terhadap hak-hak ini merupakan langkah yang sangat penting dalam memperkuat posisi nasabah sebagai pemilik data, sekaligus menciptakan keseimbangan antara kepentingan individu dan kepentingan bisnis. Namun, efektifitas suatu regulasi tidak hanya ditentukan oleh kualitas norma yang terkandung di dalamnya, tetapi juga oleh bagaimana regulasi tersebut diimplementasikan. Dalam hal ini, pendekatan struktur hukum menjadi relevan. Struktur hukum mencakup lembaga-lembaga yang berperan dalam pengawasan, penegakan hukum serta koordinasi antar sektor. Dalam konteks perbankan digital, terdapat beberapa lembaga yang memiliki kewenangan, seperti Otoritas Jasa Keuangan (OJK) Bank Indonesia, serta kementrian yang melindungi komunikasi dan informatika.(Kholis, 2024)

Permasalahan yang sering muncul adalah adanya potensi tumpang tindih kewenangan antar lembaga, yang dapat menghambat efektivitas pengawasan. selain itu, keterbatasan sumber daya manusia dan teknologi dalam melakukan pengawasan terhadap sistem digital yang kompleks juga menjadi tantangan tersendiri. Tanpa pengawasan yang kuat dan terintegrasi, regulasi yang baik sekalipun tidak akan mampu memberikan perlindungan yang optimal. Dari perspektif budaya hukum, efektifitas regulasi sangat dipengaruhi oleh tingkat kesadaran dan kepatuhan masyarakat serta pelaku industri. Dalam konteks Indonesia, tingkat literasi digital masyarakat masih menjadi persoalan utama. Banyak kasus kebocoran data penipuan yang terjadi bukan semata-mata karena kelemahan sistem, tetapi juga karena kelalaian pengguna, seperti membagikan informasi sensitif kepada pihak lain. Hal ini menunjukan bahwa perlindungan data pribadi tidak hanya bergantung pada regulasi dan teknologi, tetapi juga pada perilaku individu.(Aroyo et al., 2025)

Di sisi lain, pelaku industri perbankan juga memiliki tingkat kesiapan yang berbeda-beda dalam menerapkan standar perlindungan data. Bank-Bank besar umumnya telah memiliki sistem keamanan yang bisa dibilang canggih, termasuk penggunaan enkripsi, autentikasi, multi-faktor, serta sistem pemantauan transaksi secara real-time. Namun, tidak semua bank memiliki kapasitas

yang sama, terutama lembaga keuangan kecil atau penyedia layanan fintech yang mungkin belum sepenuhnya menerapkan standar keamanan yang memadai.

Aspek teknologi juga menjadi faktor krusial dalam menentukan efektivitas perlindungan data. Perkembangan teknologi yang cepat menciptakan dinamika baru dalam ancaman keamanan siber. Metode serangan yang digunakan oleh pelaku kejahatan siber semakin canggih, seperti penggunaan malware, ransomware, phishing berbasis kecerdasan buatan, hingga eksploitasi kelemahan sistem (vulnerability exploitation). Dalam kondisi ini, regulasi harus mampu beradaptasi dengan perkembangan teknologi agar tidak tertinggal.(Christiana & Suahriyanto, 2025) Selain itu, munculnya konsep open banking dan integrasi API (Application Programming Interface) dalam layanan keuangan juga meningkatkan kompleksitas pengelolaan data. Data nasabah tidak hanya dikelola oleh bank, tetapi juga oleh pihak ketiga yang terhubung dalam ekosistem digital. Hal ini meningkatkan risiko kebocoran data serta menuntut adanya pengaturan yang lebih ketat mengenai tanggung jawab dan standar keamanan antar pihak.

Dari aspek penegakan hukum, keberadaan sanksi administratif dan pidana dalam UU PDP merupakan langkah penting dalam menciptakan efek jera. Namun, dalam prakteknya, penegakan hukum terhadap pelanggaran data pribadi masih menghadapi berbagai kendala. Salah satunya adalah kesulitan dalam pembuktian, terutama dalam kasus kejahatan siber yang melibatkan lintas negara. Selain itu, proses penanganan kasus yang cenderung lambat juga dapat mengurangi kepercayaan masyarakat terhadap sistem hukum. Permasalahan lain yang tidak kalah penting adalah terkait dengan transfer data lintas negara (cross-border data flow). Dalam era globalisasi digital, data nasabah sering kali disimpan atau diproses di server yang berada di luar negeri. Hal ini menimbulkan tantangan dalam hal yurisdiksi hukum dan perlindungan data, karena perbedaan standar regulasi antar negara. Oleh karena itu, diperlukan kerja sama internasional serta harmonisasi regulasi untuk memastikan bahwa data nasabah tetap terlindungi, meskipun berada di luar wilayah hukum Indonesia. Untuk meningkatkan efektivitas regulasi perlindungan data pribadi, diperlukan pendekatan yang komprehensif dan berkelanjutan. Pemerintah perlu memperkuat regulasi turunan serta membentuk lembaga pengawas yang independen dan memiliki kewenangan yang jelas.(Hukum et al., 2024)

Lembaga perbankan harus terus meningkatkan sistem keamanan serta menerapkan prinsip kehati-hatian dalam pengelolaan data. Selain itu, edukasi kepada masyarakat mengenai pentingnya perlindungan data pribadi harus menjadi prioritas, mengingat peran pengguna yang sangat penting dalam menjaga keamanan transaksi. Dengan demikian, dapat disimpulkan bahwa regulasi perlindungan data pribadi memiliki peran yang sangat strategis dalam menjamin keamanan transaksi nasabah dalam ekosistem perbankan digital. Meskipun secara normatif regulasi yang ada telah memadai, efektivitasnya masih dipengaruhi oleh berbagai faktor, seperti implementasi, pengawasan, perkembangan teknologi, serta tingkat kesadaran masyarakat. Oleh karena itu, diperlukan sinergi antara pemerintah, industri, dan masyarakat untuk menciptakan ekosistem perbankan digital yang aman, terpercaya, dan berkelanjutan.

Tanggung jawab hukum bank terhadap kerugian nasabah yang disebabkan oleh kegagalan sistem keamanan digital

1. Implementasi UU Perlindungan Data Pribadi (UU PDP) dalam Sektor Finansial

Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dalam sektor perbankan menandai pergeseran paradigma dari sekadar kerahasiaan bank menuju kedaulatan data nasabah yang komprehensif. Dalam ekosistem perbankan digital, bank tidak lagi hanya bertindak sebagai perantara keuangan, melainkan bertransformasi menjadi pengendali data pribadi yang memikul tanggung jawab hukum atas setiap siklus hidup data nasabah. Secara operasional, implementasi ini dimulai dengan restrukturisasi tata kelola internal melalui penunjukan Pejabat Pelindungan Data atau *Data Protection Officer* (DPO). Penunjukan DPO di sektor perbankan menjadi mandatori mengingat volume dan sensitivitas data finansial yang diproses sangat tinggi. DPO berfungsi sebagai pengawas independen yang memastikan bahwa setiap inovasi layanan digital—seperti *digital onboarding* atau *credit scoring* berbasis profil perilaku—tetap berada dalam koridor hukum privasi, sehingga memitigasi risiko gugatan konsumen akibat penyalahgunaan data. Fauzi, dkk. (2023).

Implementasi UU PDP menuntut integrasi prinsip *Privacy by Design* dan *Privacy by Default* ke dalam arsitektur teknologi informasi bank. Hal ini mengharuskan bank untuk memandang keamanan digital bukan sebagai beban biaya, melainkan sebagai standar kehati-hatian (*duty of care*) yang melekat pada produk perbankan digital. Dengan menerapkan enkripsi ujung-ke-ujung (*end-to-end encryption*), tokenisasi, dan sistem otentikasi berlapis sejak tahap perancangan aplikasi, bank membangun benteng pertahanan teknis yang selaras dengan mandat undang-undang. Kegagalan dalam mengintegrasikan standar keamanan ini sejak awal pengembangan sistem dapat dikualifikasikan sebagai bentuk kelalaian berat dalam penyelenggaraan sistem elektronik, yang memperlemah posisi tawar bank dalam sengketa ganti rugi karena bank dianggap gagal memenuhi kewajiban preventif dalam melindungi aset digital nasabah.

Selain aspek teknis, implementasi UU PDP secara kritis mengubah mekanisme hubungan kontraktual melalui pengelolaan persetujuan (*consent management*) yang lebih transparan. Bank wajib meninggalkan praktik penggunaan klausul baku yang bersifat menjebak (*contract of adhesion*) dan beralih pada mekanisme persetujuan yang eksplisit serta terperinci (*granular consent*). Nasabah harus diberikan pilihan yang tegas untuk menyetujui atau menolak penggunaan data mereka untuk tujuan di luar layanan perbankan inti, seperti pemasaran produk pihak ketiga atau pengolahan data oleh mitra eksternal. Tanpa adanya *explicit consent* yang sah, segala bentuk pemrosesan data oleh bank kehilangan legitimasi hukumnya, sehingga jika terjadi kebocoran data pada kanal yang tidak disetujui, bank memikul tanggung jawab mutlak atas seluruh kerugian yang timbul.

Dalam menghadapi risiko kegagalan sistem, bank juga diwajibkan untuk menjalankan *Data Protection Impact Assessment* (DPIA) secara berkala. Implementasi DPIA berfungsi sebagai instrumen akuntabilitas yuridis yang mendokumentasikan langkah-langkah mitigasi risiko yang telah diambil oleh bank sebelum mengoperasikan teknologi baru. Dokumen ini menjadi sangat krusial dalam pembuktian hukum, dimana bank dapat menunjukkan iktikad baiknya dalam melindungi data konsumen. Jika terjadi insiden siber, UU PDP menetapkan

standar waktu notifikasi yang ketat, yakni maksimal 72 jam kepada otoritas dan subjek data. Kecepatan dan transparansi dalam pemberian notifikasi ini merupakan perwujudan tanggung jawab sosial dan hukum bank untuk memberikan kesempatan bagi nasabah melakukan mitigasi mandiri guna meminimalisir dampak kerugian finansial.(Khair et al., 2025)

Namun, secara kritis, implementasi UU PDP di lapangan masih menghadapi tantangan pragmatis berupa benturan regulasi sektoral (*regulatory antinomy*). Terdapat dilema hukum antara hak subjek data untuk menghapus data pribadi (*right to erasure*) dengan kewajiban bank untuk menyimpan data transaksi selama minimal sepuluh tahun demi kepentingan Anti-Pencucian Uang (APU-PPT). Ketidakselarasan ini menuntut perbankan untuk mampu melakukan klasifikasi data secara presisi antara data identitas pribadi yang dapat dihapus dengan data riwayat transaksi yang wajib dipertahankan demi kepentingan penegakan hukum pidana ekonomi. Tantangan lainnya mencakup kesiapan infrastruktur pada bank yang memiliki keterbatasan finansial untuk memenuhi standar keamanan tinggi. Tanpa harmonisasi kebijakan, bank berisiko terjebak dalam ketidakpastian kepatuhan yang dapat mengaburkan standar perlindungan konsumen di mata pengadilan. (Mawaddah, 2024)

Sinkronisasi antara UU PDP dengan regulasi sektoral Otoritas Jasa Keuangan (OJK), khususnya POJK Nomor 11/POJK.03/2022, pada akhirnya menciptakan lapisan perlindungan yang lebih solid. Implementasi lintas regulasi ini mewajibkan bank untuk menjalankan audit teknologi informasi secara independen dan memastikan ketersediaan sistem deteksi dini (*fraud detection system*) yang mampu bekerja secara *real-time*. Keberhasilan implementasi UU PDP di sektor finansial bukan sekadar masalah teknis TI, melainkan strategi fundamental untuk melindungi hak asasi nasabah atas privasi di tengah arus digitalisasi ekonomi. Perbankan yang mampu menginternalisasi nilai-nilai perlindungan data pribadi ke dalam budaya organisasinya tidak hanya akan terhindar dari sanksi administratif, tetapi juga akan memenangkan kepercayaan publik sebagai lembaga keuangan yang aman dan akuntabel di era finansial modern. (Kholis, 2024)

2. Penegakan Hukum dan Skema Ganti Rugi bagi Nasabah Korban Cyber Crime

Penegakan hukum terhadap kejahatan siber (cyber crime) yang merugikan nasabah perbankan di Indonesia pada dasarnya telah memiliki landasan normatif yang cukup memadai, namun dalam implementasinya masih menghadapi berbagai tantangan yang bersifat multidimensional. Secara yuridis, keberadaan Undang-Undang Informasi dan Transaksi Elektronik menjadi instrumen utama dalam mengatur berbagai bentuk kejahatan berbasis teknologi informasi, termasuk penipuan daring, akses ilegal, dan manipulasi data elektronik. Di samping itu, regulasi di sektor jasa keuangan yang diawasi oleh Otoritas Jasa Keuangan turut memberikan kerangka perlindungan bagi nasabah sebagai konsumen layanan keuangan. Namun demikian, hasil penelitian menunjukkan bahwa keberadaan regulasi tersebut belum sepenuhnya mampu menjawab kompleksitas cyber crime yang terus berkembang, baik dari sisi modus operandi maupun teknologi yang digunakan oleh pelaku kejahatan. Hal ini disebabkan oleh sifat kejahatan siber yang dinamis, anonim, serta seringkali melibatkan jaringan lintas negara, sehingga menyulitkan proses penegakan hukum yang selama ini masih berbasis pada yurisdiksi teritorial.

Dalam praktiknya, aparat penegak hukum dihadapkan pada berbagai kendala, antara lain keterbatasan sumber daya manusia yang memiliki kompetensi di bidang digital forensik, kurangnya fasilitas teknologi pendukung, serta belum optimalnya koordinasi antar lembaga, baik di tingkat nasional maupun internasional. Proses pelacakan pelaku cyber crime membutuhkan kemampuan teknis yang tinggi, termasuk dalam hal pelacakan alamat IP, analisis jejak digital, serta pengamanan barang bukti elektronik agar tetap memiliki nilai pembuktian di pengadilan. Meskipun Undang-Undang Informasi dan Transaksi Elektronik telah mengakui alat bukti elektronik sebagai alat bukti yang sah, implementasinya masih menghadapi tantangan terkait dengan validitas, autentikasi, dan integritas data digital. Hal ini sejalan dengan pendapat para ahli yang menyatakan bahwa pembuktian dalam tindak pidana siber memiliki tingkat kompleksitas yang lebih tinggi dibandingkan dengan tindak pidana konvensional, sehingga memerlukan pendekatan khusus dan dukungan teknologi yang memadai. Riston, R., & Basoddin, B. (2025). (Siber et al., 2025)

Selain aspek penegakan hukum, persoalan yang tidak kalah penting adalah skema ganti rugi bagi nasabah korban cyber crime. Berdasarkan hasil analisis, mekanisme kompensasi yang diterapkan oleh lembaga perbankan di Indonesia masih bersifat kasuistik dan belum memiliki standar yang seragam. Pada umumnya, bank menggunakan pendekatan tanggung jawab berdasarkan kesalahan (fault liability), di mana nasabah harus dapat membuktikan bahwa kerugian yang dialaminya disebabkan oleh kelalaian atau kegagalan sistem dari pihak bank. Dalam praktiknya, hal ini menjadi beban yang cukup berat bagi nasabah, mengingat keterbatasan akses terhadap informasi dan teknologi yang dimiliki oleh bank. Akibatnya, tidak sedikit kasus di mana nasabah tidak memperoleh ganti rugi secara penuh, bahkan klaimnya ditolak dengan alasan adanya kelalaian dari pihak nasabah, seperti memberikan kode OTP, PIN, atau informasi rahasia lainnya kepada pihak yang tidak berwenang.

Dari perspektif teori perlindungan konsumen, kondisi ini menunjukkan adanya ketidakseimbangan posisi antara pelaku usaha dan konsumen. Menurut Shidarta (2006), perlindungan konsumen seharusnya menempatkan konsumen sebagai pihak yang perlu dilindungi dari potensi kerugian akibat penggunaan produk atau layanan. Dalam konteks ini, bank sebagai pelaku usaha memiliki kewajiban untuk menjamin keamanan sistem dan melindungi data serta dana nasabah. Oleh karena itu, penerapan prinsip tanggung jawab mutlak (strict liability) dalam kasus-kasus tertentu, khususnya yang berkaitan dengan kegagalan sistem keamanan, menjadi relevan untuk dipertimbangkan. Prinsip ini memungkinkan nasabah untuk memperoleh ganti rugi tanpa harus membuktikan adanya kesalahan dari pihak bank, sehingga dapat memberikan perlindungan yang lebih efektif dan adil. Kristiyanti, C. T. S. (2022). *Hukum*

Jika dibandingkan dengan praktik di negara lain, seperti di Uni Eropa, perlindungan terhadap nasabah korban cyber crime telah diatur secara lebih komprehensif melalui regulasi Payment Services Directive 2 (PSD2). Regulasi ini mengharuskan penyedia layanan pembayaran untuk mengembalikan dana nasabah yang hilang akibat transaksi tidak sah dalam waktu yang relatif singkat, kecuali jika dapat dibuktikan bahwa nasabah melakukan kelalaian berat atau tindakan fraud secara sengaja.(Langkat & Budi, 2025)Pendekatan ini menunjukkan adanya pergeseran paradigma dari fault liability menuju perlindungan konsumen yang lebih kuat, di mana beban pembuktian lebih banyak dibebankan kepada penyedia layanan. Dibandingkan

dengan Indonesia, pendekatan ini memberikan kepastian hukum yang lebih tinggi serta meningkatkan kepercayaan masyarakat terhadap sistem perbankan.

Peran Otoritas Jasa Keuangan dalam konteks ini menjadi sangat strategis, tidak hanya sebagai regulator tetapi juga sebagai fasilitator dalam penyelesaian sengketa antara nasabah dan lembaga jasa keuangan. Melalui mekanisme pengaduan konsumen, OJK berupaya menjembatani kepentingan kedua belah pihak, namun efektivitasnya masih perlu ditingkatkan. Salah satu kendala yang dihadapi adalah sifat hasil mediasi yang tidak selalu mengikat, sehingga tidak memberikan kepastian hukum yang kuat bagi nasabah. Oleh karena itu, diperlukan penguatan kewenangan OJK dalam menangani sengketa konsumen, termasuk kemungkinan untuk memberikan putusan yang bersifat final dan mengikat.

Selain itu, upaya preventif juga perlu mendapatkan perhatian yang lebih besar. Edukasi kepada masyarakat mengenai keamanan digital menjadi kunci dalam mengurangi risiko terjadinya cyber crime. Banyak kasus yang terjadi disebabkan oleh rendahnya tingkat literasi digital masyarakat, terutama dalam mengenali modus operandi kejahatan siber seperti phishing, social engineering, dan malware. Oleh karena itu, sinergi antara pemerintah, lembaga keuangan, dan masyarakat sangat diperlukan untuk menciptakan ekosistem digital yang aman dan terpercaya.

Keterkaitan dengan Undang Undang P2SK

Perlindungan konsumen dan keamanan data pribadi merupakan aspek penting dalam penyelenggaraan layanan perbankan digital. Operasional bank digital yang sepenuhnya memanfaatkan platform elektronik menyebabkan nasabah sangat bergantung pada keandalan sistem keamanan serta keterbukaan informasi yang diberikan oleh penyedia layanan. Efektivitas pengawasan terhadap layanan tersebut dapat dilihat dari rendahnya tingkat sengketa antara nasabah dan penyelenggara, kecepatan dalam penanganan pengaduan konsumen, serta tersedianya mekanisme mitigasi terhadap risiko kebocoran data dan serangan siber. Dalam hal ini, Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) memperkuat mandat Otoritas Jasa Keuangan untuk menjaga integritas pasar serta memberikan perlindungan kepada konsumen sebagai bagian dari upaya menjaga stabilitas sistem keuangan.

Apabila pengawasan tersebut dilaksanakan secara efektif, maka tingkat kepercayaan masyarakat terhadap layanan bank digital akan meningkat, yang pada akhirnya dapat mendorong pertumbuhan inklusi keuangan secara nasional. Selain itu, indikator lain yang menentukan efektivitas pengawasan adalah kapasitas kelembagaan serta koordinasi antarotoritas yang berwenang. Pengawasan terhadap bank digital tidak dapat dilakukan secara sektoral oleh satu lembaga saja, melainkan membutuhkan kerja sama dengan berbagai institusi terkait seperti Bank Indonesia dan Lembaga Penjamin Simpanan, serta otoritas lain yang memiliki peran dalam menjaga stabilitas sistem keuangan. Efektivitas pengawasan tersebut dapat diukur melalui tingkat kerja sama antar lembaga, integrasi sistem dan data pengawasan, serta kemampuan dalam merespons krisis atau gangguan pada sistem keuangan digital. Penguatan koordinasi antar lembaga ini juga sejalan dengan ketentuan dalam UU P2SK yang menekankan pentingnya sinergi kelembagaan dalam pengaturan dan pengawasan sektor jasa keuangan.(Digital et al., 2026)

KESIMPULAN

Berdasarkan pembahasan di atas, dapat disimpulkan bahwa perlindungan konsumen dan hak-hak nasabah bank merupakan bagian penting dari tujuan hukum dalam menciptakan keadilan, kepastian, dan ketertiban dalam masyarakat. Konsep keadilan yang dikemukakan Aristoteles, baik keadilan distributif maupun korektif, menjadi dasar dalam pemberian hak secara proporsional serta pemulihan kerugian akibat pelanggaran, termasuk dalam hubungan antara nasabah dan pihak bank.

Dalam sektor perbankan, nasabah dikategorikan sebagai konsumen akhir yang berhak mendapatkan perlindungan hukum sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Perlindungan ini mencakup upaya pencegahan risiko (perlindungan tidak langsung) maupun penyelesaian kerugian (perlindungan langsung), yang menjadi tanggung jawab pihak bank sebagai pelaku usaha.

Seiring dengan transformasi perbankan ke era digital, muncul berbagai kemudahan layanan seperti mobile banking dan fintech, namun juga diikuti dengan meningkatnya risiko kejahatan siber dan kebocoran data, seperti kasus serangan LockBit. Hal ini menunjukkan bahwa sistem keamanan perbankan masih memiliki kelemahan dan berdampak pada menurunnya kepercayaan masyarakat.

Meskipun Indonesia telah memiliki regulasi seperti Undang-Undang Perlindungan Data Pribadi, efektivitasnya masih menghadapi berbagai kendala, seperti lemahnya pengawasan, tumpang tindih kewenangan antar lembaga, perkembangan teknologi yang cepat, serta rendahnya literasi digital masyarakat. Oleh karena itu, diperlukan sinergi antara pemerintah, lembaga pengawas, sektor perbankan, dan masyarakat dalam meningkatkan keamanan sistem, penegakan hukum, serta kesadaran akan pentingnya perlindungan data pribadi, guna menciptakan ekosistem perbankan digital yang aman, adil, dan terpercaya. Dapat digunakan untuk menyebutkan sumber dana penelitian yang hasilnya dilaporkan pada jurnal ini dan memberikan penghargaan kepada beberapa institus

DAFTAR PUSTAKA.

Abigael, M. C. (2024). *No Title*. *1*(6), 335–347.

Anjheli, D. (2024). *Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023 , lebih dari 215 juta penduduk telah terhubung*. *4*(1).

April, V. N. (2025). *Implementasi Konsep Keadilan Terhadap Perlindungan Konsumen (Studi Kasus Serangan Cyber kepada Data Nasabah Bank Syariah Indonesia)*. *8*(1), 15–30.

Aroyo, D. O., Putri, K. A., Shakira, S. P., & Lia, U. (2025). *PERAN LITERASI DIGITAL DALAM MENANGGULANGI BERITA HOAKS : 01*(01), 60–72.

Christiana, V., & Suahriyanto, D. (2025). *Perlindungan Data Nasabah Perbankan dengan Perjanjian Pembukaan Rekening*. *3*(1), 1–16.

Dan, K., & Pengaturan, T. (2024). *PELINDUNGAN DATA PRIBADI DI BANK INDONESIA DAN LEMBAGA JASA KEUANGAN :*

Digital, B., Berlakunya, P., No, U. U., & Tentang, T. (2026). *EFEKTIVITAS PENGAWASAN OTORITAS JASA KEUANGAN TERHADAP BANK DIGITAL PASCA BERLAKUNYA UU NO 4 TAHUN 2023 TENTANG P2SK*. *16*(5).

Hukum, P., Data, T., Nasabah, P., Layanan, D., Banking, I., Hukum, F., Lampung, U., & Lampung, B. (2024). *Steven Saputra*.

Hukum, P., Konsumen, B., Transaksi, P., Aset, D., Ditinjau, K., Nurul, D., Kosasih, A., & Benia, E. (2022). *Padjadjaran Law Review*. *10*.

Khair, F., Wiraguna, S. A., Esa, U., Jakarta, U., Jeruk, K., & Barat, J. (2025). *Data Protection Impact Assessment (DPIA) sebagai Instrumen Kunci Menjamin Kepatuhan UU PDP 2022 di Indonesia*. *2*.

Kholis, I. M. (2024). *Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan : Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia*. *4*(2).

Langkat, P. A., & Budi, P. P. (2025). *IMPLIKASI HUKUM PERLINDUNGAN KONSUMEN DALAM TRANSAKSI KEUANGAN DIGITAL DAN PENINJAUAN PERATURAN PERBANKAN*. *03*(02), 106–117.

Mawaddah, D. (2024). *IMPLIKASI PERUBAHAN REGULASI ANTI PENCUCIAN UANG (AML) DAN PERLINDUNGAN DATA TERHADAP 1 . Bagaimana Perubahan Regulasi Pada Penerapan Kebijakan Anti Pencucian Uang Review (SLR). Kajian pustaka adalah suatu bentuk penelitian yang dilakukan melalui*. *2*(6), 76–86.

Palopo, N. (2025). *Perlindungan terhadap data pribadi di era digital berdasarkan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi*.

Pamuji, R. A. (n.d.). *Perlindungan Hukum Bagi Nasabah dan Tanggung Jawab Bank Dalam Kasus Card Skimming*. *8*, 25–43.

Pdp, U. U. (2026). *ANALISIS HUKUM PERLINDUNGAN DATA PRIBADI TERHADAP NASABAH BADAN PADA PERBANKAN DI INDONESIA DALAM TENTANG PERLINDUNGAN DATA PRIBADI*. *2*(1), 14–25.

Siber, P., Kasus, S., Muhram, L. O., Hukum, F., & Sulawesi, U. (2025). *Sultra Law Review*. *07*(1), 3744–3756.