

Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi Pengguna Aplikasi Pinjaman Online dalam Perspektif Hukum Telematika

Yahya Adib Prasetya¹, Muchammad Iksan²

^{1,2} Fakultas Hukum, Universitas Muhammadiyah Surakarta, Indonesia

Korespondensi: adibprasetya79@gmail.com, mi214@ums.ac.id

Informasi Artikel

Riwayat artikel:

Received Sept 7th, 2026

Revised Oct 4th, 2026

Accepted Oct 21th, 2026

Keyword:

Data pribadi; Hukum telematika;
Pelindungan data; Pinjaman online;
Tanggung jawab penyelenggara.

ABSTRAK

Pemanfaatan teknologi finansial telah memudahkan masyarakat mengakses layanan pinjaman melalui aplikasi digital. Di sisi lain, pemrosesan data pribadi dalam layanan tersebut menimbulkan risiko apabila dilakukan secara berlebihan, tanpa dasar yang sah, atau digunakan untuk menekan peminjam. Risiko dapat berupa pengumpulan data yang tidak relevan, penyebaran informasi kepada pihak lain, serta penggunaan kontak pribadi untuk melakukan penagihan yang mengganggu. Artikel ini bertujuan menganalisis bentuk perlindungan hukum terhadap data pribadi pengguna aplikasi pinjaman online serta tanggung jawab penyelenggara ketika terjadi penyalahgunaan. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual. Bahan hukum utama meliputi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, peraturan mengenai informasi dan transaksi elektronik, serta ketentuan sektoral terkait layanan pendanaan berbasis teknologi informasi. Analisis dilakukan secara kualitatif dengan menghubungkan prinsip pemrosesan data pribadi dengan kewajiban penyelenggara layanan digital. Pembahasan menunjukkan bahwa persetujuan pengguna saja tidak cukup untuk membenarkan setiap bentuk pengumpulan dan penggunaan data. Pemrosesan harus memiliki dasar yang sah, tujuan yang jelas, proporsional, transparan, dan disertai pengamanan yang memadai. Penegakan perlindungan membutuhkan mekanisme pengaduan yang mudah diakses, pengawasan terhadap penyelenggara, dan pemulihan bagi pengguna yang dirugikan. Artikel ini menawarkan kerangka penilaian yang menggabungkan legalitas pemrosesan, pembatasan tujuan, keamanan data, dan pertanggungjawaban penyelenggara.



© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong perubahan dalam penyediaan layanan keuangan. Salah satu bentuknya adalah pinjaman online yang memungkinkan calon peminjam mengajukan pembiayaan melalui aplikasi tanpa harus datang langsung ke kantor penyedia layanan. Proses digital dapat mempercepat pemeriksaan permohonan dan memperluas akses masyarakat terhadap layanan keuangan. Namun, kemudahan tersebut juga bergantung pada pengumpulan dan pemrosesan data pengguna, mulai dari identitas, informasi kontak, data pekerjaan, hingga informasi keuangan. Kajian terdahulu juga menyoroti bahwa kebutuhan perlindungan tidak berhenti pada keamanan data, tetapi mencakup kepastian mengenai pemanfaatan data dalam hubungan pinjaman digital (Nurmantari & Martana, 2019; Dewi & Sulistyawan, 2024).

Data pribadi memiliki nilai penting karena dapat digunakan untuk mengenali seseorang, menilai kelayakan layanan, dan menjalankan hubungan kontraktual. Ketika data diproses tanpa batas yang jelas, risiko terhadap pengguna meningkat. Dalam konteks pinjaman online, masalah dapat muncul ketika

aplikasi meminta akses yang tidak berkaitan dengan layanan, data digunakan untuk tujuan lain tanpa dasar yang sah, atau informasi peminjam disebarkan kepada orang lain sebagai cara penagihan. Praktik semacam itu berpotensi mengganggu privasi, menimbulkan rasa takut, dan merusak hubungan sosial pengguna.

Perlindungan data pribadi tidak cukup dipahami sebagai kewajiban menyediakan pemberitahuan privasi atau meminta pengguna menekan tombol persetujuan. Pengguna sering kali berada pada posisi yang kurang seimbang dibandingkan penyelenggara karena tidak memiliki informasi yang memadai mengenai jenis data yang dikumpulkan, pihak yang menerima data, masa penyimpanan, dan konsekuensi pemrosesannya. Karena itu, persetujuan harus ditempatkan dalam kerangka perlindungan yang lebih luas, termasuk dasar pemrosesan yang sah, transparansi, pembatasan tujuan, akurasi, keamanan, dan pemenuhan hak subjek data. Persoalan persetujuan dan penggunaan data pihak ketiga juga dibahas dalam penelitian mengenai data kontak darurat pada perjanjian pinjaman online (Rahim & Hassanah, 2026).

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan kerangka umum mengenai pemrosesan data pribadi dan kewajiban pihak yang mengendalikan atau memproses data. Di samping itu, penyelenggaraan layanan pinjaman berbasis teknologi informasi juga berada dalam lingkup pengaturan sektor jasa keuangan dan ketentuan mengenai sistem elektronik. Oleh sebab itu, analisis perlindungan pengguna harus membaca aturan perlindungan data bersama dengan ketentuan sektoral yang relevan, bukan hanya menitikberatkan pada hubungan pinjam-meminjam. Pada tingkat sektoral, POJK Nomor 40 Tahun 2024 menjadi rujukan penting bagi penyelenggaraan layanan pendanaan bersama berbasis teknologi informasi (Otoritas Jasa Keuangan, 2024).

Masalah lain adalah kesulitan pengguna dalam mengidentifikasi pihak yang bertanggung jawab ketika terjadi kebocoran atau penggunaan data yang tidak sesuai. Dalam suatu layanan, pemrosesan dapat melibatkan penyelenggara aplikasi, mitra penagihan, penyedia teknologi, atau pihak ketiga lainnya. Pembagian peran tersebut perlu dijelaskan agar pengguna mengetahui kepada siapa pengaduan diajukan dan bagaimana tanggung jawab ditentukan. Penyelenggara juga perlu menerapkan pengamanan teknis dan organisasi yang sesuai dengan risiko pemrosesan data.

Berdasarkan uraian tersebut, artikel ini mengkaji perlindungan hukum terhadap penyalahgunaan data pribadi pengguna aplikasi pinjaman online dalam perspektif hukum telematika. Fokus pembahasan diarahkan pada prinsip pemrosesan data, tanggung jawab penyelenggara, serta mekanisme perlindungan dan pemulihan bagi pengguna yang mengalami kerugian.

Penelitian ini menjawab pertanyaan berikut: 1. Bagaimana prinsip hukum yang mengatur pemrosesan data pribadi pengguna aplikasi pinjaman online di Indonesia? 2. Bagaimana tanggung jawab penyelenggara ketika terjadi penyalahgunaan data pribadi pengguna? 3. Bagaimana upaya perlindungan dan pemulihan hukum bagi pengguna yang dirugikan akibat penyalahgunaan data?

Penelitian ini bertujuan menganalisis prinsip hukum pemrosesan data pribadi pada layanan pinjaman online, mengkaji tanggung jawab penyelenggara atas penyalahgunaan data, serta menjelaskan pilihan perlindungan dan pemulihan hukum yang dapat ditempuh pengguna.

METODE PENELITIAN

Artikel ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Pendekatan perundang-undangan digunakan untuk menelaah norma mengenai perlindungan data pribadi, sistem elektronik, dan penyelenggaraan layanan pendanaan berbasis teknologi informasi. Pendekatan konseptual digunakan untuk memahami prinsip pemrosesan data yang sah, pembatasan tujuan, proporsionalitas, keamanan, akuntabilitas, dan pemulihan kerugian.

Bahan hukum primer mencakup peraturan perundang-undangan yang relevan. Bahan hukum sekunder berupa buku, artikel jurnal, dan karya ilmiah tentang perlindungan data pribadi, *fintech*, privasi digital, dan hukum telematika. Bahan hukum dikaji secara kualitatif melalui inventarisasi norma, penafsiran hubungan antaraturan, serta penerapan prinsip hukum terhadap risiko penyalahgunaan data pada layanan pinjaman online. Artikel ini merupakan kajian normatif dan tidak mengklaim temuan empiris mengenai frekuensi pelanggaran pada penyelenggara tertentu.

HASIL DAN PEMBAHASAN

Batas Legal Pengumpulan dan Pemrosesan Data Pengguna

Pemrosesan data pribadi merupakan kegiatan yang mencakup pengumpulan, pencatatan, penyimpanan, penggunaan, pengungkapan, pengiriman, penghapusan, atau tindakan lain terhadap data seseorang. Dalam layanan pinjaman online, sebagian pemrosesan memang diperlukan untuk verifikasi identitas, penilaian permohonan, pencegahan penipuan, dan pelaksanaan perjanjian. Akan tetapi, kebutuhan bisnis tidak secara otomatis membenarkan pengumpulan semua jenis data yang dapat diakses melalui perangkat pengguna. Analisis ini sejalan dengan kajian yang menempatkan perlindungan data peminjam sebagai persoalan hukum yang perlu dibaca bersama dengan aturan sektoral layanan pinjaman digital (Christiananta & Sawitri, 2025; Wafda et al., 2024).

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menempatkan pemrosesan data dalam kerangka dasar yang sah dan kewajiban pengendali data. Secara konseptual, penyelenggara perlu dapat menjelaskan alasan pemrosesan, tujuan spesifik, kategori data yang dibutuhkan, masa penyimpanan, serta pihak yang menerima data. Pengumpulan data seharusnya dibatasi pada informasi yang relevan dengan tujuan layanan dan tidak melampaui kebutuhan yang wajar. (Republik Indonesia, 2022).

Prinsip transparansi menuntut informasi yang mudah dipahami, bukan sekadar dokumen panjang yang sulit dibaca. Pengguna perlu mengetahui apa yang terjadi pada data mereka dan bagaimana haknya dapat dijalankan. Prinsip pembatasan tujuan juga berarti data yang dikumpulkan untuk verifikasi tidak semestinya digunakan untuk tujuan berbeda yang tidak sesuai dengan dasar pemrosesan semula. Jika tujuan atau dasar pemrosesan berubah, penyelenggara perlu menilai kembali legalitasnya sesuai dengan peraturan yang berlaku.

Persetujuan menjadi salah satu dasar pemrosesan yang mungkin digunakan, tetapi tidak dapat diperlakukan sebagai pembenaran tanpa batas. Persetujuan yang diperoleh melalui informasi yang tidak jelas atau pilihan yang tidak bermakna dapat melemahkan perlindungan pengguna. Di samping itu, penyelenggara harus memperhatikan dasar pemrosesan lain yang diakui oleh undang-undang dan memastikan dasar yang digunakan sesuai dengan keadaan konkret. Dengan demikian, analisis legalitas tidak berhenti pada pertanyaan apakah pengguna telah menyetujui syarat aplikasi.

Keamanan data juga merupakan bagian inti dari perlindungan. Penyelenggara perlu menerapkan pengendalian akses, pembatasan hak pegawai dan mitra, pengamanan penyimpanan dan pengiriman data, evaluasi vendor, serta prosedur penanganan insiden. Langkah tersebut harus sepadan dengan jenis data dan risiko yang mungkin muncul. Pengamanan yang hanya tertulis dalam kebijakan, tetapi tidak diterapkan dalam sistem operasional, tidak memadai untuk melindungi pengguna.

Berdasarkan prinsip-prinsip tersebut, akses terhadap daftar kontak, foto, atau informasi lain pada perangkat pengguna harus dinilai menurut relevansi, dasar pemrosesan, kebutuhan, dan ketentuan sektoral yang berlaku. Apabila suatu akses tidak diperlukan untuk tujuan layanan atau digunakan untuk mempermalukan dan menekan peminjam, praktik tersebut menimbulkan persoalan hukum yang tidak dapat dibenarkan hanya dengan alasan bahwa pengguna pernah menyetujui ketentuan aplikasi.

Akuntabilitas Penyelenggara dan Mitra Pemroses Data

Tanggung jawab penyelenggara perlu ditentukan berdasarkan perannya dalam pemrosesan data, tindakan yang dilakukan, kewajiban hukum yang berlaku, dan hubungan sebab akibat dengan kerugian yang dialami pengguna. Penyelenggara yang menentukan tujuan dan cara pemrosesan memiliki kewajiban untuk memastikan kegiatan tersebut sesuai dengan prinsip perlindungan data. Apabila pemrosesan dilakukan oleh pihak lain atas instruksi penyelenggara, hubungan kontraktual dan pembagian kewajiban perlu diatur secara jelas, tanpa menghilangkan kewajiban yang ditetapkan oleh hukum. Literatur juga menggarisbawahi pentingnya menilai kewajiban penyelenggara dan bentuk pemulihan bagi pihak yang datanya disalahgunakan (Kaeng et al., 2024; Dewi & Sulistyawan, 2024).

Salah satu risiko pada layanan pinjaman online adalah penggunaan data kontak untuk menyampaikan informasi utang kepada keluarga, teman, rekan kerja, atau pihak lain yang bukan pihak dalam perjanjian. Pengungkapan demikian perlu dinilai dari segi dasar hukum, tujuan, kebutuhan, kerahasiaan, dan aturan sektor jasa keuangan. Penagihan tidak semestinya dijadikan alasan umum untuk menyebarkan data pribadi secara luas atau melakukan tekanan yang tidak proporsional terhadap

pengguna. Masalah penggunaan data kontak darurat tanpa persetujuan pemiliknya telah menjadi objek kajian tersendiri dalam literatur terbaru (Rahim & Hassanah, 2026).

Ketika terjadi dugaan penyalahgunaan, penilaian tanggung jawab perlu memeriksa apakah penyelenggara telah menetapkan kebijakan yang memadai, membatasi akses data, mengawasi mitra, menangani keluhan, dan melakukan langkah pengamanan yang diwajibkan. Apabila pelanggaran dilakukan oleh mitra, pemeriksaan tidak cukup berhenti pada identitas mitra tersebut. Perlu pula dianalisis bagaimana data diberikan, apa instruksi yang berlaku, bagaimana pengawasan dilakukan, dan apakah pengendalian yang seharusnya diterapkan benar-benar berjalan.

Pertanggungjawaban administratif, perdata, atau pidana tidak boleh disamakan karena masing-masing memiliki dasar, unsur, dan prosedur yang berbeda. Sanksi administratif bergantung pada ketentuan yang dilanggar dan kewenangan lembaga terkait. Tuntutan perdata memerlukan dasar hukum dan pembuktian yang sesuai, sedangkan pertanggungjawaban pidana hanya dapat diterapkan jika unsur tindak pidana dalam peraturan yang berlaku terpenuhi. Perbedaan ini penting agar analisis hukum tidak menyimpulkan bahwa setiap insiden data secara otomatis merupakan tindak pidana.

Bukti digital menjadi bagian penting untuk menjelaskan apa yang terjadi. Dokumen kebijakan privasi, rekaman persetujuan, riwayat akses, pesan penagihan, surat elektronik, tangkapan layar, serta komunikasi dengan penyelenggara dapat membantu merekonstruksi peristiwa. Bukti perlu disimpan secara utuh, dengan tanggal, tautan, dan konteks yang memadai. Namun, tangkapan layar semata mungkin tidak selalu cukup untuk membuktikan keseluruhan peristiwa; keaslian dan keterkaitannya dengan pihak yang bertanggung jawab tetap perlu dinilai.

Akuntabilitas juga menuntut adanya mekanisme pengaduan yang dapat diakses. Pengguna perlu memperoleh jawaban yang jelas mengenai pengaduannya, langkah pembatasan dampak, dan tindakan korektif yang dilakukan. Penyelenggara yang memiliki tata kelola baik seharusnya dapat menelusuri alur data, mengidentifikasi pihak yang memperoleh akses, dan menjelaskan tindakan yang diambil ketika ditemukan penyimpangan.

Jalur Pengaduan, Pembuktian, dan Pemulihan bagi Pengguna

Perlindungan hukum terhadap pengguna dapat dimulai dari pencegahan. Sebelum menggunakan layanan, pengguna perlu memperoleh informasi yang mudah dipahami tentang data yang diminta, tujuan penggunaannya, penerima data, masa penyimpanan, serta cara mengajukan permintaan atau keluhan. Dari sisi penyelenggara, rancangan aplikasi sebaiknya menerapkan prinsip perlindungan data sejak tahap perancangan dan secara bawaan, sehingga pengumpulan data yang tidak dibutuhkan tidak menjadi praktik standar.

Ketika pengguna menduga terjadi penyalahgunaan, langkah awal yang dapat dilakukan adalah mengamankan bukti dan mengajukan pengaduan melalui kanal resmi penyelenggara. Pengguna dapat menyimpan syarat layanan yang berlaku, pemberitahuan privasi, bukti permintaan izin, pesan yang diterima, identitas akun atau nomor pengirim, dan kronologi kejadian. Pengaduan yang disusun dengan runtut memudahkan pemeriksaan dan membantu membedakan antara sengketa pembayaran dengan dugaan pelanggaran pemrosesan data.

Jika pengaduan internal tidak menyelesaikan persoalan, pengguna dapat mempertimbangkan jalur pengaduan kepada otoritas yang berwenang sesuai karakter pelanggaran dan status penyelenggara. Dalam konteks layanan keuangan, status perizinan dan pengawasan penyelenggara perlu diverifikasi melalui sumber resmi. Untuk dugaan pelanggaran data pribadi atau tindak pidana, jalur yang tepat harus dipilih berdasarkan sifat peristiwa dan aturan yang berlaku. Artikel ini tidak menyimpulkan bahwa satu kanal pengaduan berlaku untuk seluruh bentuk pelanggaran.

Pemulihan dapat mencakup penghentian penggunaan data yang tidak sah, koreksi atau penghapusan data sesuai ketentuan yang berlaku, perbaikan keamanan, penjelasan kepada pengguna, dan pemulihan kerugian melalui mekanisme hukum yang tersedia. Tidak semua bentuk pemulihan otomatis tersedia dalam setiap perkara; hak dan prosedurnya bergantung pada ketentuan yang berlaku serta fakta kasus. Oleh sebab itu, informasi yang akurat mengenai mekanisme pengaduan dan pemulihan perlu disediakan sejak awal.

Perlindungan yang efektif juga membutuhkan literasi digital. Pengguna sebaiknya memeriksa legalitas penyelenggara, membaca izin akses aplikasi, memahami informasi privasi, dan menghindari pemberian data yang tidak relevan. Meski demikian, literasi pengguna tidak boleh digunakan untuk

memindahkan seluruh beban perlindungan kepada konsumen. Penyelenggara tetap memiliki tanggung jawab untuk merancang sistem yang aman dan mematuhi kewajiban hukum.

Dengan demikian, pendekatan perlindungan yang memadai perlu menggabungkan pencegahan, pengawasan, penanganan pengaduan, pembuktian, dan pemulihan. Fokus tidak hanya pada perilaku pengguna atau pelaku penagihan, tetapi juga pada tata kelola data dan sistem yang memungkinkan penyalahgunaan terjadi.

Posisi Kajian dan Kerangka Analisis yang Ditawarkan

Pembahasan perlindungan data pribadi pada layanan digital kerap berpusat pada keberadaan persetujuan pengguna atau pada larangan akses data tertentu. Kedua aspek itu penting, tetapi belum cukup apabila tidak dihubungkan dengan alur pemrosesan, pembagian tanggung jawab, keamanan sistem, dan mekanisme pemulihan. Pada layanan pinjaman online, data dapat berpindah dari aplikasi kepada mitra atau penyedia layanan lain, sehingga penilaian yang hanya berfokus pada layar persetujuan berisiko melewatkan persoalan akuntabilitas.

Kerangka analisis yang ditawarkan artikel ini menggabungkan empat parameter: legalitas dasar pemrosesan, kesesuaian data dengan tujuan, keamanan dan pengawasan pihak yang memperoleh akses, serta tanggung jawab dan pemulihan. Parameter tersebut dapat digunakan untuk menilai kebijakan privasi maupun dugaan insiden tertentu secara lebih terstruktur. Kebaruan yang diajukan bersifat kerangka analisis normatif, bukan klaim bahwa penelitian ini telah membuktikan secara empiris tingkat pelanggaran pada industri pinjaman online.

Untuk pengembangan penelitian selanjutnya, kerangka tersebut dapat diterapkan pada putusan, keputusan regulator, atau kasus yang terdokumentasi. Penelitian empiris juga dapat dilakukan melalui wawancara dan analisis pengaduan yang telah dipublikasikan secara sah, dengan tetap menjaga kerahasiaan identitas pengguna. Dengan cara itu, kajian normatif dapat dilengkapi bukti mengenai efektivitas mekanisme perlindungan dalam praktik.

Uji Kerangka Analisis melalui Ilustrasi Hipotetis

Untuk memperlihatkan cara kerja kerangka analisis, bagian ini menggunakan ilustrasi hipotetis, bukan laporan atas kejadian nyata atau tuduhan terhadap penyelenggara tertentu. Misalnya, sebuah aplikasi meminta akses ke daftar kontak, lalu salah satu kontak pengguna menerima pesan penagihan yang memuat informasi utang. Penilaian hukum perlu dilakukan secara bertahap: memeriksa dasar dan tujuan akses, menilai apakah pengungkapan kepada pihak ketiga memang diperlukan dan dibenarkan, menelusuri siapa yang mengakses atau mengirim data, serta menguji kecukupan pengamanan dan mekanisme pengaduan. Fakta-fakta tersebut harus dibuktikan sebelum kesimpulan mengenai pelanggaran atau tanggung jawab dapat dibuat.

Tabel 1 Kerangka Penilaian Penyalahgunaan Data Pribadi pada Pinjaman Online

Tahap pemeriksaan	Pertanyaan kunci	Bahan yang dapat diperiksa
Legalitas pemrosesan	Apa dasar dan tujuan akses data?	Pemberitahuan privasi, persetujuan, ketentuan layanan
Pembatasan tujuan	Apakah data yang diminta relevan dan diperlukan?	Daftar izin aplikasi, fungsi layanan, alur pemrosesan
Pengungkapan dan keamanan	Siapa yang menerima atau mengakses data dan bagaimana pengamanan dilakukan?	Log akses, kontrak mitra, pesan penagihan, laporan insiden
Akuntabilitas dan pemulihan	Bagaimana pengaduan ditangani dan kerugian dipulihkan?	Nomor pengaduan, tanggapan penyelenggara, bukti kerugian

KESIMPULAN

Perlindungan data pribadi pengguna aplikasi pinjaman online perlu didasarkan pada pemrosesan yang sah, transparan, sesuai tujuan, proporsional, dan aman. Persetujuan pengguna tidak dengan sendirinya membenarkan setiap bentuk akses atau penggunaan data. Legalitas pemrosesan harus dinilai

dengan memperhatikan dasar hukum, kebutuhan data, tujuan, penerima, serta ketentuan sektoral yang berlaku. Tanggung jawab penyelenggara harus dianalisis berdasarkan peran dalam pemrosesan, kepatuhan terhadap kewajiban hukum, pengawasan terhadap mitra, dan hubungan dengan kerugian pengguna. Dugaan penyalahgunaan dapat menimbulkan konsekuensi administratif, perdata, atau pidana, tetapi setiap jalur mempunyai unsur dan prosedur tersendiri. Bukti digital dan dokumentasi alur data menjadi penting untuk menilai kejadian serta menentukan pihak yang bertanggung jawab.

Perlindungan yang efektif membutuhkan pencegahan sejak perancangan aplikasi, pengawasan, mekanisme pengaduan yang jelas, pengamanan bukti, dan akses pada pemulihan hukum. Kerangka legalitas, pembatasan tujuan, keamanan, dan akuntabilitas dapat membantu menilai kepatuhan penyelenggara serta mengidentifikasi kebutuhan perbaikan. Penyelenggara pinjaman online perlu menyampaikan pemberitahuan privasi yang jelas, meminta akses hanya untuk kebutuhan yang sah, mengawasi mitra pemroses data, dan menyediakan mekanisme pengaduan yang dapat ditelusuri. Evaluasi keamanan sebaiknya dilakukan secara berkala dan disesuaikan dengan risiko pemrosesan.

Regulator dan lembaga terkait perlu memperkuat koordinasi pengawasan dan memastikan informasi mengenai status penyelenggara serta kanal pengaduan mudah ditemukan masyarakat. Penanganan perkara perlu membedakan sengketa pembayaran, pelanggaran perlindungan data, dan dugaan tindak pidana agar pengguna diarahkan pada mekanisme yang tepat. Penelitian berikutnya disarankan menguji kerangka analisis ini melalui telaah putusan, dokumen resmi regulator, atau data pengaduan yang dapat diakses secara sah. Dengan dukungan sumber primer yang terverifikasi, hasil kajian dapat memberi rekomendasi yang lebih konkret bagi perlindungan pengguna layanan keuangan digital.

DAFTAR PUSTAKA

- Christiananta, M. V., & Sawitri, D. A. D. (2025). Perlindungan hukum bagi konsumen terhadap penyebaran data pribadi secara ilegal oleh penyelenggara pinjaman online. *Kertha Wicara: Journal Ilmu Hukum*, 14(8), 407–416.
- Dewi, S. P., & Sulistyawan, A. Y. (2024). Perlindungan hukum data pribadi nasabah dalam transaksi pinjaman online. *Notarius*, 17(3), 2265–2282.
- Kaeng, A. A., Sumiyati, B., Arpin, & Andini, N. Q. (2024). Perlindungan hukum terhadap penyebaran data pribadi dalam pinjaman online. *Unisan Law Review*, 9(2).
- Nurmantari, N. N. A. D., & Martana, N. A. (2019). Perlindungan hukum terhadap data pribadi peminjam dalam layanan aplikasi pinjaman online. *Kertha Wicara: Journal Ilmu Hukum*, 8(12), 1–14.
- Otoritas Jasa Keuangan. (2024). Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 40 Tahun 2024 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi.
- Rahim, A., & Hassanah, H. (2026). Perlindungan hukum data pribadi dalam perjanjian pinjaman online. *Res Nullius Law Journal*, 8(1), 16–30.
- Republik Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Republik Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Wafda, P. N., Rokhim, A., & Utami, N. S. (2024). Perlindungan hukum terhadap penyalahgunaan data pribadi dalam aplikasi pinjaman online. *DIVERSI: Jurnal Hukum*, 10(1), 35–63.