

**MENELISIK CELAH HUKUM DALAM KASUS PENIPUAN APLIKASI DANA:
ANTARA TANGGUNG JAWAB KONSUMEN, PENYEDIA LAYANAN,
DAN APARAT PENEGAK HUKUM**

**Alin Juni Aminar¹, Atthaya Shaka Aisha P.², Samantha Amerys Marsada D.³,
Yunia Dian Pratiwi⁴**

¹⁻⁴Ilmu Hukum, Fakultas Hukum, UPN Veteran Jakarta,
Jl. R.S Fatmawati No. 1, Cilandak, Jakarta Selatan.

¹2310611269@mahasiswa.upnvj.ac.id, ²2310611124@mahasiswa.upnvj.ac.id,
³2310611459@mahasiswa.upnvj.ac.id, ⁴2310611158@mahasiswa.upnvj.ac.id

Abstrak

Penelitian ini membahas celah hukum dalam perlindungan konsumen terhadap kasus penipuan digital melalui aplikasi dompet elektronik DANA. Meskipun pemerintah telah menerbitkan berbagai regulasi seperti UU Perlindungan Konsumen, UU ITE, dan UU Perlindungan Data Pribadi, kenyataannya perlindungan yang diberikan masih belum optimal. Konsumen masih menghadapi risiko besar akibat lemahnya literasi digital, sistem keamanan yang belum maksimal, serta mekanisme pengaduan yang tidak efektif. Di sisi lain, penyedia layanan seperti DANA seringkali membatasi tanggung jawab mereka. Penelitian ini menggunakan pendekatan hukum normatif untuk menganalisis tanggung jawab konsumen, penyedia layanan, dan aparat penegak hukum. Hasil penelitian menunjukkan perlunya kolaborasi lintas sektor, reformasi regulasi, dan peningkatan edukasi publik untuk membangun ekosistem digital yang aman, adil, dan akuntabel.

Kata kunci: DANA; perlindungan konsumen; penipuan digital; hukum fintech

Abstract

This research explores the legal gaps in consumer protection concerning digital fraud cases through the DANA e-wallet application. Although the Indonesian government has issued various regulations, such as the Consumer Protection Act, the Electronic Information and Transactions Law, and the Personal Data Protection Law, their implementation remains suboptimal. Consumers face significant risks due to low digital literacy, insufficient system security, and ineffective complaint mechanisms. Meanwhile, service providers like DANA often limit their responsibilities. This study employs a normative legal approach to analyze the responsibilities of consumers, service providers, and law enforcement agencies. The findings emphasize the need for cross-sector collaboration, regulatory reform, and public education to build a secure, fair, and accountable digital ecosystem.

Keywords: DANA, consumer protection; digital fraud; fintech law

Article History

Received: June 2025
Reviewed: June 2025
Published: June 2025
Plagiarism Checker No. 234
Prefix DOI : Prefix DOI :
10.8734/CAUSA.v1i2.365
Copyright : Author
Publish by : CAUSA



This work is licensed under
a [Creative Commons
Attribution-NonCommercial
4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

LATAR BELAKANG

Di Indonesia perkembangan teknologi finansial telah mengalami pertumbuhan yang pesat. Pertumbuhan ini diiringi dengan meningkatnya penggunaan layanan dompet digital. Kemudahan transaksi dalam penggunaan dompet digital memang tidak dapat dipungkiri lagi. Akan tetapi, dibalik kemudahan itu juga membawa risiko kejahatan siber, termasuk juga kasus penipuan. Berbagai banyak modus penipuan yang mana telah menimbulkan kerugian bagi para pengguna kemudian mengalami kesulitan dalam mendapatkan perlindungan hukum.

Dalam era digital yang semakin maju, aplikasi keuangan atau *e-wallet* seperti DANA telah menjadi bagian integral dari kehidupan sehari-hari pengguna di Indonesia. Namun, penggunaan aplikasi ini tidak lepas dari risiko penipuan. Maraknya penipuan terkait DANA memunculkan isu tentang kelemahan hukum serta pembagian tanggung jawab antara konsumen, DANA sebagai penyedia layanan, dan pihak berwajib.

Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa Indonesia menghadapi 74 juta serangan siber hingga Mei 2024, angka yang sangat mengkhawatirkan. Salah satu ilustrasi risiko keamanan dalam transaksi digital adalah kasus pembobolan dana nasabah yang dialami oleh beberapa *platform* dompet digital, termasuk DANA. Kompleksitas masalah keamanan transaksi digital semakin bertambah dengan maraknya penipuan melalui *customer care* palsu, *phishing* dengan link palsu terkait DANA, dan pembuatan kartu fisik palsu.

Pemerintah Indonesia terus memperkuat regulasi dan pengawasan sektor keuangan digital seiring meningkatnya kejahatan siber. Otoritas Jasa Keuangan (OJK) berperan memastikan penyedia layanan seperti DANA mematuhi standar perlindungan konsumen. OJK telah menerbitkan berbagai aturan untuk mendukung keamanan sistem digital. Salah satunya adalah POJK No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital. Aturan ini mencakup perlindungan konsumen serta pengelolaan risiko teknologi.

Selain OJK, Bank Indonesia (BI) juga berperan dalam mengatur dan mengawasi sistem pembayaran, termasuk dompet digital. BI mewajibkan penyedia layanan untuk memenuhi persyaratan tertentu, seperti penggunaan autentikasi ganda, sertifikasi keamanan sistem, serta pelaporan berkala atas insiden keamanan. Tidak hanya itu, pemerintah juga mengesahkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang memperkuat aspek perlindungan hak-hak individu atas data pribadi mereka dalam ekosistem digital.

Pembagian tanggung jawab antara konsumen, penyedia layanan, dan aparat penegak hukum menjadi aspek krusial dalam menangani kasus penipuan digital. Dalam sistem hukum Indonesia, konsumen memiliki hak atas perlindungan, keamanan, dan informasi yang benar atas produk atau jasa yang digunakan, sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Penyedia layanan seperti DANA, di sisi lain, memiliki tanggung jawab yang lebih besar dari segi perlindungan teknis maupun hukum terhadap pengguna. Mereka wajib menyediakan sistem yang aman, transparan, serta mudah diakses untuk pelaporan dan penanganan keluhan.

Kewajiban ini tidak hanya bersumber dari etika bisnis, tetapi juga dari regulasi yang berlaku, seperti ketentuan dari OJK dan BI, serta UU Perlindungan Data Pribadi yang menekankan pentingnya pengelolaan data pengguna secara hati-hati dan bertanggung jawab. Kegagalan penyedia layanan dalam memberikan sistem keamanan yang memadai bisa membuka ruang gugatan hukum dari pengguna yang dirugikan.

Meskipun regulasi-regulasi tersebut telah disusun, tantangan implementasi di lapangan masih menjadi persoalan tersendiri. Banyak pengguna belum memahami hak-haknya sebagai konsumen digital, dan penyedia layanan pun tidak jarang abai terhadap kewajiban edukasi serta transparansi informasi. Oleh karena itu, kehadiran regulasi belum sepenuhnya menjawab kompleksitas persoalan penipuan digital, sehingga diperlukan evaluasi menyeluruh terhadap efektivitas pelaksanaannya.

Konsumen sebagai pengguna layanan memiliki hak untuk mendapatkan perlindungan atas data pribadi dan keamanan transaksi mereka. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menegaskan hak-hak konsumen, termasuk hak atas kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan/atau jasa¹. Namun, dalam praktiknya, banyak konsumen yang kurang memahami risiko penipuan digital, sehingga rentan menjadi korban kejahatan siber².

Di sisi lain, penyedia layanan seperti DANA memiliki kewajiban untuk menjamin keamanan sistem dan melindungi data pengguna³. Meski DANA telah dilengkapi dengan fitur keamanan seperti autentikasi dua faktor dan enkripsi data, celah keamanan tetap memungkinkan pelaku kejahatan siber untuk menembus sistem⁴. Hal ini menunjukkan bahwa upaya perlindungan yang ada belum sepenuhnya efektif dalam pencegahan penipuan.

Aparat penegak hukum memegang peran krusial menindak pelaku kejahatan siber dan memberikan rasa aman bagi masyarakat⁵. Meskipun demikian, ada sejumlah tantangan yang dihadapi, yaitu keterbatasan sumber daya, kurangnya pemahaman teknis mengenai kejahatan siber, dan rumitnya pelacakan jejak digital pelaku⁶. Solusi efektif untuk mengatasi masalah ini adalah melalui kolaborasi antara penyedia layanan, aparat penegak hukum, serta instansi-instansi terkait lainnya⁷.

Perkembangan teknologi finansial dan dompet digital di Indonesia membawa kemudahan dalam bertransaksi, namun juga meningkatkan risiko kejahatan siber, termasuk penipuan. Meski pemerintah, melalui lembaga seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), telah menerbitkan regulasi untuk memperkuat pengawasan dan perlindungan konsumen, tantangan dalam implementasi regulasi tetap ada.

Penyedia layanan, seperti DANA, memiliki tanggung jawab besar dalam menjaga keamanan dan melindungi data pengguna, namun celah keamanan yang ada masih memungkinkan terjadinya penipuan. Selain itu, aparat penegak hukum menghadapi kesulitan dalam menangani kasus penipuan digital, baik karena keterbatasan sumber daya maupun kurangnya pemahaman teknis.

Oleh karena itu, perlu adanya kolaborasi antara penyedia layanan, aparat penegak hukum, dan instansi terkait lainnya, serta upaya yang lebih intensif untuk mengedukasi konsumen agar lebih waspada terhadap potensi penipuan digital. Perbaikan dalam sistem regulasi, pengawasan, dan penegakan hukum akan sangat penting dalam menciptakan ekosistem digital yang aman dan dapat dipercaya.

¹ Septia, G., Ningsih, R. A., Lindawati, Faadhilah, S. D. N., & Anugrah, D. (2024). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana Atas Kejahatan Link Phising dan Hacking Pada Layanan Digital. *LETTERLIJK: Jurnal Hukum Perdata*, 1(1), 4.

² Paridah, N., Yunitasari, K., Putri, R. A. A., Sahrir, I. F. (2024). Perlindungan Hukum Terhadap Nasabah Bank Dalam Penggunaan Aplikasi Dana Di Indonesia, 47.

³ Ummi, A. Y., Pinasti, S. A., Ramadhani, S. P. (2024). Hukum Perlindungan Konsumen dalam Produk Perbankan Digital (Studi Kasus Dana). 118.

⁴ Septia, G., et al., *Op.Cit*, 8.

⁵ *Ibid*.

⁶ Paridah, N., et al., *Op.Cit*, 45.

⁷ *Ibid*, 48.

RUMUSAN MASALAH

Berdasarkan uraian latar belakang tersebut, untuk meneliti mengenai celah hukum dalam kasus penipuan aplikasi dana antara tanggung jawab, penyedia layanan, dan aparat penegak hukum, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana perlindungan hukum konsumen yang didapatkan oleh pengguna aplikasi *E-Wallet* DANA atas kasus pencurian data dan penipuan yang mengatasnamakan pihak DANA?
2. Bagaimana pengaturan perlindungan hukum terhadap korban tindak pidana penipuan melalui aplikasi digital di masa mendatang?

RUANG LINGKUP

Ruang lingkup dalam penelitian ini hanya terbatas pada pembahasan dari aspek hukum pidana dan hukum bisnis dalam konteks perlindungan hukum terhadap konsumen pengguna aplikasi *E-Wallet* DANA yang menjadi korban pencurian data dan tindak pidana penipuan digital. Dari hukum pidana, penelitian ini difokuskan pada bagaimana konstruksi pertanggungjawaban pelaku serta peran aparat penegak hukum dalam menangani kasus penipuan berbasis teknologi informasi.

Sedangkan dari sisi hukum bisnis, fokus diarahkan pada sejauh mana tanggung jawab penyedia layanan (dalam hal ini aplikasi DANA) dalam menjamin keamanan transaksi serta perlindungan data konsumen, termasuk implikasi hukumnya terhadap hubungan kontraktual dan regulasi bisnis digital yang berlaku.

TUJUAN PENELITIAN

Tujuan dari artikel ilmiah ini dengan judul “Menelisik Celah Hukum dalam Kasus Penipuan Aplikasi DANA: Antara Tanggung Jawab Konsumen, Penyedia Layanan, dan Aparat Penegak Hukum” adalah untuk mengidentifikasi dan menganalisis celah hukum secara mendalam aspek hukum yang terkait dengan kasus penipuan berbasis aplikasi digital, khususnya untuk aplikasi DANA.

Tujuan utama dari penelitian ini adalah untuk mengeksplorasi tanggung jawab yang dimiliki oleh pihak-pihak yang terlibat dalam penggunaan aplikasi dana, termasuk konsumen, penyedia layanan, dan aparat penegak hukum. Melalui pendekatan ini, diharapkan para pembaca dapat memahami dinamika hubungan antara konsumen dan penyedia layanan, serta bagaimana aparat hukum dapat berperan dalam menyelesaikan konflik yang muncul. Artikel ini bertujuan untuk memberikan rekomendasi.

MANFAAT PENELITIAN

Salah satu manfaat utama dari artikel ini adalah untuk memberikan wawasan mengenai keterlibatan berbagai pihak dalam ekosistem aplikasi keuangan. Konsumen memiliki tanggung jawab untuk mengedukasi diri mereka sendiri tentang risiko dan cara pencegahan penipuan, seperti mengenali tanda-tanda aplikasi yang mencurigakan. Sebagai contoh, konsumen dapat belajar untuk tidak memberikan informasi pribadi yang sensitif kepada pihak ketiga dan mengenali kebijakan perlindungan.

Manfaat yang terkandung dalam artikel ini adalah dengan mempelajari celah hukum, penulis berusaha menyusun kerangka teoritis yang dapat digunakan untuk menganalisis masalah hukum yang lebih luas dalam konteks teknologi finansial, sehingga dapat menjadi referensi bagi akademisi dan penelitian selanjutnya. Pemahaman ini memperkuat landasan akademis dan praktis dalam bidang hukum, khususnya yang berkaitan dengan teknologi informasi.

Di sisi lainnya, artikel ini menawarkan manfaat yang signifikan dalam pengimplementasian hukum. Dengan mengetahui celah hukum yang ada penyedia layanan dapat meningkatkan sistem keamanan mereka untuk melindungi konsumen dan mengurangi

potensi penipuan. Selain itu, aparat penegak hukum dapat menggunakan temuan dari penelitian ini untuk merumuskan strategi yang lebih efektif dalam menanggulangi kejahatan siber.

Manfaat ini mencakup peningkatan kesadaran masyarakat tentang risiko dan tanggung jawab saat menggunakan aplikasi keuangan digital, serta memberikan masukan untuk memperbaiki regulasi dan praktik perlindungan konsumen. Penelitian ini berpotensi membantu dalam menangani kasus-kasus serupa. Dengan demikian, hasil penelitian ini diharapkan dapat berkontribusi pada upaya pencegahan penipuan di dunia maya dan meningkatkan kepercayaan masyarakat terhadap aplikasi keuangan digital.

METODE PENELITIAN

Metode penelitian yang digunakan penelitian hukum normatif yang bertujuan untuk mengkaji perlindungan hukum terhadap pengguna aplikasi DANA yang menjadi penipuan digital, melalui pendekatan yang tidak hanya berpaku pada peraturan perundang-undangan, tetapi juga menganalisis konsep-konsep hukum yang berkembang dan studi kasus yang sesuai.

Populasi dan sampel dalam penelitian ini adalah karya-karya ilmiah dna sumber hukum yang membahas topik perlindungan konsumen, tanggung jawab penyedia layanan digital, dan peran aparat penegak hukum dalam kasus penipuan digital. Sumber-sumber tersebut dipilih secara *purposive*, yakni dengan mempertimbangkan relevansi dan kedalaman bahasan terhadap fokus penelitian.

Teknik pengumpulan data dilakukan dengan menelusuri dan mengumpulkan referensi dari berbagai platform jurnal ilmiah nasional, perpustakaan digital, serta peraturan perundang-undangan Indonesia yang berlaku, termasuk Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian juga menggunakan berita resmi dan laporan instansi terkait, seperti OJK dan BSSN, sebagai pelengkap data kontekstual.

Instrumen dalam penelitian ini adalah alat bantu kategorisasi dan analisis dokumen, yang digunakan untuk mengelompokkan isu-isu hukum ke dalam beberapa kategori utama, seperti tanggung jawab hukum penyedia layanan, hak-hak konsumen, dan peran aparat hukum.

Teknik analisis data yang digunakan adalah analisis isi (*content analysis*), dengan cara membaca secara cermat setiap sumber, mengidentifikasi isu hukum utama, dan membandingkan berbagai pendapat akademik serta regulasi yang berlaku. Analisis ini dilengkapi dengan pendekatan normatif, yakni menafsirkan norma-norma hukum dalam peraturan perundang-undangan yang relevan dengan kasus yang dikaji.

HASIL DAN PEMBAHASAN

Perlindungan Hukum Bagi Pengguna Aplikasi E-Wallet DANA Atas Kasus Penipuan dan Pencurian Data

Di Indonesia penggunaan aplikasi e-wallet menunjukkan memiliki peningkatan karena diiringi dengan meningkatnya kebutuhan masyarakat terhadap layanan keuangan digital yang dapat memberikan mereka pelayanan yang mudah, cepat dan efisien. Penggunaan dompet digital untuk pembayaran di Indonesia sudah mendapatkan izin resmi yang tercantum dalam Peraturan Bank Indonesia Nomor 18/17/PBI/2016 tentang uang elektronik.⁸ Aturan tersebut diharapkan dapat menjadi landasan hukum yang dapat meningkatkan masyarakat dalam transaksi non tunai.

DANA merupakan salah satu aplikasi e-wallet yang paling populer dikalangan masyarakat, digunakan jutaan pengguna dalam berbagai transaksi, seperti untuk pembayaran tagihan, pembelian produk digital, transaksi pengiriman uang, sampai dengan e-commerce. Menurut

⁸ Indriani, W. & Asih, S. P. (2024). Pengaruh Persepsi Kemudahan, Persepsi Risiko, Keamanan, dan Fitur Layanan terhadap Minat Penggunaan Dompet Digital pada Aplikasi DANA di Kabupaten Tulang Bawang Barat. 166.

data Bank Indonesia pada Januari 2024 lalu, transaksi elektronik meningkat sebanyak 39,28% (YoY) diikuti dengan nominal transaksi QRIS yang juga tumbuh mencapai 149,46 persen (YoY).

Dana memiliki fitur keamanan seperti autentikasi dua faktor, pengenalan wajah, dan juga sistem enkripsi data untuk melindungi penggunanya. Namun, meskipun DANA memiliki sistem keamanan yang terus diperbarui, ada celah keamanan yang dapat dimanfaatkan oleh para pelaku kejahatan siber untuk melakukan penipuan. Untuk aplikasi berbasis dompet digital seperti Dana, aspek keamanan sangat penting karena fiturnya dapat memengaruhi keputusan yang dibuat tentang transaksi berikutnya.⁹

Jenis penipuan yang sering terjadi dalam penggunaan aplikasi DANA berkaitan erat dengan rekayasa sosial (*social engineering*). Dalam hal ini pelaku memanipulasi psikologis korban untuk memberikan data pribadinya atau informasi sensitif. Salah satu modus yang paling sering digunakan adalah pelaku menyamar seolah-olah mereka customer service pihak DANA. Pelaku mengaku sebagai pihak resmi DANA dan meminta para korbannya untuk memberikan data login, kode OTP, atau bahkan PIN dengan berdalih verifikasi akun.

Banyak korban yang tertipu karena tampilan akun penipu dibuat sangat mirip dengan akun resmi pihak DANA seperti menggunakan profil logo DANA. Modus penipuan dana lainnya juga ada seperti phishing. Korban diminta untuk mengklik tautan palsu yang diberikan oleh pelaku yang menyerupai dengan situs resmi Dana. Setelah pengguna memasukkan informasi pribadinya, data tersebut kemudian disalahgunakan oleh pelaku untuk mengakses dan menguras saldo korban.

DANA sebagai penyedia layanan keuangan berbasis digital, seharusnya memiliki tanggung jawab hukum yang melekat dalam menjamin keamanan sistem dan juga melindungi data serta transaksi para pengguna. Pengelola situs seharusnya bertanggung jawab untuk menjaga keamanan data pribadi dan pribadi pelanggan.¹⁰ Tanggung jawab tidak hanya bersifat moral saja tetapi juga bersifat yuridis yang berdasarkan berbagai peraturan perundang-undangan yang berlaku di Indonesia.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) merupakan salah satu dasar hukum utama yang mengatur hubungan antara penyedia layanan dan pengguna. Dalam UU tersebut terdapat Pasal 4 yang menegaskan bahwa konsumen memiliki hak atas kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan/atau jasa, serta hak atas informasi yang benar, jelas, dan jujur. Artinya, penyedia layanan yaitu DANA wajib untuk memberikan informasi yang akurat mengenai fitur layanan, potensi risiko, dan kemudahan.

Pasal 4 huruf e UUPK menegaskan bahwa konsumen berhak mendapatkan advokasi, perlindungan, dan penyelesaian sengketa perlindungan konsumen secara patut. Ini menegaskan bahwa apabila konsumen mengalami kerugian termasuk seperti akibat penipuan aplikasi DANA maka mereka berhak untuk mengakses mekanisme penyelesaian sengketa yang adil dan dapat dipertanggungjawabkan. Konsumen menerima perlindungan hukum represif melalui penyelesaian sengketa, baik di pengadilan maupun di luar pengadilan.¹¹

Selain itu, Peraturan Otoritas Jasa Keuangan (POJK) No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital mengatur bagaimana pelaku industri fintech menjaga konsumen dan mengelola risiko teknologi. Menurut undang-undang tersebut, penyedia layanan harus mematuhi prinsip transparansi, perlindungan data, dan mekanisme keamanan sistem yang memadai. Penyedia layanan dapat dimintai pertanggungjawaban secara administratif maupun perdata jika terjadi pelanggaran yang merugikan pengguna.

⁹ Kirana, T., Roisah, R., Solihat, A., & Mauliyani, F. F. (2024). Pengaruh Tingkat Keamanan dan Kepercayaan Dompet Digital terhadap Kepuasan Konsumen (Studi Kasus di Kota Bandung), *Jurnal Sains Manajemen*, 6(2), 96.

¹⁰ *Ibid.*

¹¹ Pakasi, S. S., Muaja, H. S., Kermite, J. A. (2021). Tinjauan Hukum Terhadap Penggunaan Dompet Digital dalam Bertransaksi di Indonesia, *Lex Crimen*, 10(12), 69.

Peraturan Bank Indonesia juga mengatur sistem pembayaran berbasis teknologi, seperti persyaratan otorisasi ganda atau otorisasi faktor ganda, sertifikasi keamanan sistem, dan pelaporan insiden keamanan secara berkala. Autentikasi dua langkah dan notifikasi transaksi secara *real-time* adalah beberapa fitur keamanan yang digunakan DANA dalam praktiknya. Namun, masih saja sistem dapat dimasuki melalui manipulasi pengguna, ini menunjukkan betapa pentingnya mendidik sistem dan mendeteksi sejak awal.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mewajibkan pengendali data, termasuk DANA, untuk mengelola data pribadi dengan prinsip kehati-hatian, akuntabilitas, dan pencegahan kebocoran data. Jika seseorang melanggar ketentuan ini, mereka dapat dikenai sanksi administratif hingga pidana. Dalam kasus penipuan yang mengatasnamakan DANA, penyedia layanan bertanggung jawab untuk melakukan upaya pencegahan dan penanggulangan, serta memberikan informasi kepada pengguna secara cepat.

Penyedia layanan tetap memiliki tanggung jawab untuk menciptakan ekosistem digital yang aman, meskipun pelaku utama penipuan biasanya merupakan pihak ketiga. Tanggung jawab ini adalah membangun sistem yang dapat mendeteksi aktivitas mencurigakan, menangani pengaduan dengan responsif, dan bekerja sama dengan lembaga penegak hukum. Kegagalan untuk menyediakan sistem yang aman dan responsif dapat saja dianggap sebagai kelalaian, yang memungkinkan pelanggan yang dirugikan untuk mengambil tindakan hukum.

Namun, seiring berkembangnya sektor digital, termasuk sektor fintech, memperluas potensi kerentanan hukum. Sayangnya, perlindungan hukum bagi korban kejahatan di ranah digital, seperti pada aplikasi *e-wallet* atau platform pinjaman online, belum memiliki bentuk pengaturan yang spesifik dan terpadu.

Salah satu kelemahan utama dalam penanganan kasus penipuan digital melalui aplikasi DANA adalah pengaturan mengenai perlindungan data pribadi memang belum diatur secara merinci dan masih direncanakan dalam Rancangan Undang-Undang Perlindungan Data Pribadi. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen maupun UU ITE hanya memberikan kerangka umum, tanpa menyentuh tanggung jawab korporasi digital dalam konteks penipuan oleh pihak ketiga.

Meskipun DANA telah memiliki sistem keamanan seperti PIN dan OTP, banyak modus penipuan (*phishing*, *social engineering*, impersonasi, dsb.) masih bisa menembus perlindungan tersebut. Penyelenggara sering kali tidak mewajibkan verifikasi berlapis atau pengenalan aktivitas mencurigakan secara otomatis, padahal mereka memiliki akses teknologi dan data pengguna untuk melakukannya. Minimnya kewajiban hukum bagi platform untuk secara aktif mencegah terjadinya penipuan menjadikan konsumen sebagai pihak yang paling rentan.

Selain itu, Dalam praktiknya, korban penipuan digital mengalami kesulitan saat melapor ke pihak kepolisian. Laporan sering kali tidak diproses dengan cepat, apalagi jika nominal kerugian dianggap kecil. Hal ini diperparah dengan kurangnya koordinasi antara aparat penegak hukum dan penyelenggara aplikasi dalam mengusut pelaku penipuan.

Dalam praktiknya, korban penipuan digital mengalami kesulitan saat melapor ke pihak kepolisian. Laporan sering kali tidak diproses dengan cepat, apalagi jika nominal kerugian dianggap kecil. Hal ini diperparah dengan kurangnya koordinasi antara aparat penegak hukum dan penyelenggara aplikasi dalam mengusut pelaku penipuan.

Adanya celah perlindungan konsumen pengguna aplikasi DANA yang bersifat struktural dan praktis. Dari segi legal, hak-hak konsumen sudah diatur dalam undang-undang. Misalnya, Pasal 4 Undang-Undang Nomor 8 Tahun 1999 menegaskan hak konsumen atas “kenyamanan, keamanan, dan keselamatan” dalam mengkonsumsi barang/jasa serta hak mendapatkan informasi yang benar dan murni.¹² Prinsip ini diulang dalam peraturan Bank Indonesia tentang

¹² Aidill, A. M., Darmawan, M. A., Summa. (2025). Analisis Perlindungan Hukum Dalam Transaksi Transfer Melalui Aplikasi Dana. Jurnal Kajian Hukum dan Kebijakan Publik, 2(2), 741.

e-money (PBI 20/6/2018) yang mengharuskan pemisahan dana konsumen dan transparansi transaksi.¹³

Di sisi lain, Undang-Undang Informasi dan Transaksi Elektronik (Pasal 28, 29, Undang-Undang Nomor 19 Tahun 2016) mengkriminalisasi penipuan elektronik, termasuk melalui aplikasi seperti DANA.¹⁴ Regulasi baru Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022 bahkan memperkuat kewajiban penyedia kerahasiaan data pengguna.¹⁵

Namun demikian, praktik di lapangan mengekspos kekurangan serius. Terdapat banyak laporan pengguna yang mengalami kehilangan saldo karena penipuan daring, sementara prosedur pemulihan bergantung pada kebijakan internal DANA. Sebagai contoh, media konsumen mengunggah surat pembaca korban yang saldo DANA-nya hilang akibat akses tidak sah, dan *Customer Service* DANA terkesan lamban menanggapi serta sering menuntut dokumen yang memberatkan konsumen, seperti menyuruh konsumen untuk membuat tiket pelaporan.¹⁶

Kasus lainnya di media menunjukkan seorang pengguna hilang Rp6 juta karena terjebak tautan phishing pada media sosial.¹⁷ Viral cerita lhwat seseorang kehilangan uang sebesar Rp6 juta di salah satu platform dompet digital, DANA, milik PT Espay Debit Indonesia Koe. Dalam dua contoh tersebut, konsumen sudah menjalankan kewajiban dasar (tidak membagikan PIN/OTP) tetapi tetap mengalami kerugian. Temuan menunjukkan beberapa faktor penyebab utama:

- a. Pola serangan baru: Skema *phishing* modern (melalui QRIS palsu, SMS/WhatsApp palsu) yang terus berevolusi, sehingga teknis perlindungan seperti OTP saja belum memadai.
- b. Literasi pengguna rendah: Sesuai temuan riset internasional (WEF 2022), literasi digital di Indonesia masih dibawah rata-rata global, sehingga seringkali menjadi korban penipuan karena kurang memahami mekanisme keamanan yang tersedia.¹⁸ Banyak konsumen belum paham tanda-tanda penipuan sehingga rentan mengklik link asing.
- c. Beban pembuktian pada korban: Meskipun Undang-Undang Perlindungan Konsumen menjamin kompensasi atas kerugian material¹⁹, konsumen sering kesulitan membuktikan kelalaian penyedia. Dalam praktiknya syarat layanan e-wallet sering mengalihkan tanggung jawab ke konsumen (misalnya klausul bahwa pengguna wajib menjaga kerahasiaan OTP). DANA sendiri menegaskan bahwa pengembalian dana hanya melalui fitur *DANA Protection*, yang tidak mencakup kerugian akibat *phishing* atau kelalaian pengguna.²⁰ Panduan DANA juga mengimbau agar konsumen “jaga kerahasiaan PIN dan OTP” sebagai bagian dari pencegahan²¹, dengan implikasi korban dituntut menanggung risiko sendiri.

¹³ *Ibid*, 742.

¹⁴ Hartanto, Rosadi, V., & Yosmar, E. A. (2023). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana. *PATTIMURA Legal Journal*, 2(3), 273.

¹⁵ Aidill, A. M., et al., Op.Cit, 745.

¹⁶ RHEY. (2023). Pencurian di Akun DANA, Pihak DANA Lepas Tangan. *Mediakonsumen.com*. <https://mediakonsumen.com/2023/08/31/surat-pembaca/pencurian-di-akun-dana-pihak-dana-lepas-tangan>. Diakses 3 Juni 2025 Pukul 19.54 WIB.

¹⁷ Affan, S. I. (2024). Kronologi Nasabah Diduga Kebobolan Uang Rp6 Juta di Aplikasi DANA. *Bloombergtechnoz.com*. <https://www.bloombergtechnoz.com/detail-news/25873/kronologi-nasabah-diduga-kebobolan-uang-rp6-juta-di-aplikasi-dana>. Diakses 3 Juni 2025 Pukul 19.59 WIB.

¹⁸ Annur, C. M. (2023). Indeks Literasi Digital Indonesia (2020-2022). *Databoks.katadata.co.id*. <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/494c92f675bfffcc/literasi-digital-indonesia-naik-pada-2022-tapi-budaya-digital-turun#:~:text=Menurut%20laporan%20tersebut%2C%20indeks%20literasi,berada%20di%20level%203%2C49>. Diakses 3 Juni 2025 Pukul 20.19 WIB.

¹⁹ Hartanto, et al., Op.Cit, 277.

²⁰ DANA. Bagaimana Jika Uang di DANA Hilang? *Dana.id*. <https://www.dana.id/corporate/newsroom/bagaimana-jika-uang-di-dana-hilang>. Diakses 4 Juni 2025 Pukul 08.31 WIB.

²¹ *Ibid*.

- d. Keterbatasan penegakan: Kapasitas aparat penegak hukum dalam menindak penipuan siber masih terbatas. Meskipun KUHP (Pasal 378) dan Undang-Undang Informasi dan Transaksi Elektronik dapat digunakan, proses pembuktian kejahatan digital memakan waktu dan belum cepat menyelesaikan kasus.

Secara keseluruhan, dapat disimpulkan bahwa konsumen DANA memiliki hak yang jelas berdasarkan Undang-Undang Nomor 8 Tahun 1999 dan regulasi pendukung, tetapi kesenjangan antara aturan di atas kertas dan realitas teknologi menyebabkan perlindungan itu sulit terealisasi. Berikut rangkuman poin kunci perlindungan konsumen:

- a. Hak Konsumen (Pasal 4 Undang-Undang Perlindungan Konsumen): Hak atas keamanan, kenyamanan, dan informasi yang benar.²² Secara teoritis, konsumen dapat menuntut ganti rugi jika prinsip ini dilanggar.
- b. Kewajiban Penyelenggara: DANA diawasi Bank Indonesia (bukan OJK), sehingga tunduk pada PBI *e-money* yang ketat (misalnya keharusan menempatkan dana konsumen di rekening khusus).²³
- c. Kewajiban Administratif: DANA terkait Undang-Undang Informasi dan Teknologi Elektronik dan Undang-Undang Perlindungan Data Pribadi terbaru, yang memaksa penerapan enkripsi dan perlindungan data pribadi.²⁴
- d. Celah Praktis: Prosedur pengaduan DANA yang kompleks dan eksekusi hukum yang lambat membuat ganti rugi jarang terwujud. Penelitian lain juga menemukan kesulitan konsumen memperoleh pertanggungjawaban dari DANA saat kerugian terjadi.²⁵

Dari sudut bisnis dan hukum perusahaan, DANA sebagai penyedia layanan keuangan digital dihadapkan pada tanggung jawab ganda: memenuhi standar keamanan industri sekaligus mengelola risiko bisnis. Temuan penelitian dan literatur menunjukkan bahwa DANA telah menerapkan berbagai langkah teknis untuk melindungi pengguna. Contohnya, DANA menggunakan enkripsi *end-to-end*, sertifikasi ISO 27001 dan PCI-DSS untuk menjaga kerahasiaan data dan transaksi.²⁶

DANA juga mengaktifkan autentikasi ganda (PIN, sidik jari, OTP) dan sistem deteksi anomali yang mengirim peringatan saat ada percobaan login mencurigakan.²⁷ Dalam wawancara, pengembangan teknologi keamanan disebut cukup baik oleh sebagian pihak. Namun, laporan lain (IDC 2023) menggarisbawahi bahwa fitur-fitur ini masih bisa disusupi oleh *malware* atau *social engineering*.

Analisis menyimpulkan bahwa dari perspektif tanggung jawab sipil dan kontrak, DANA seharusnya memikul kewajiban memperbaiki kerugian pengguna bila terbukti kelalaiannya. Dalam teori hukum bisnis, penyedia keuangan digital dapat dianggap memiliki posisi fidusia atas dana konsumen (analogi bank), karena memegang uang pihak ketiga. Oleh karena itu, mereka berkewajiban menjalankan *due diligence* dan menjaga dana tersebut secara aman.

Hal ini sejalan dengan analisis hukum sebelumnya yang menyatakan bahwa "DANA harus bertanggung jawab atas kerugian yang dialami pengguna dan dapat memberikan ganti rugi".²⁸ Meskipun begitu, praktik penegakan tanggung jawab tersebut menemui hambatan. Temuan Pattimura Journal 2023 juga menekankan bahwa DANA sebagai penyedia *e-wallet*

²² Aidill, A. M., et al., Op.Cit, 741.

²³ DANA. Kenapa Aplikasi DANA Tidak Diawasi oleh OJK? *Dana.id*. <https://www.dana.id/corporate/newsroom/kenapa-dana-tidak-diawasi-ojk>. Diakses 4 Juni 2025 Pukul 08.41 WIB.

²⁴ Aidill, A. M., et al., Op.Cit, 739.

²⁵ Septia, G., et al., Op.Cit, 14.

²⁶ *Ibid*. Lihat juga Aidill, A. M., et al., Op.Cit, 744.

²⁷ Aidill, A. M., et al., Op.Cit, 745.

²⁸ Hartanto, et al., Op.Cit, 275.

“harus mematuhi ketentuan anti-pencucian uang, pencegahan penipuan, dan perlindungan konsumen”, termasuk teknologi enkripsi dan deteksi penipuan.²⁹

Di sisi kontrak, syarat dan ketentuan layanan DANA seringkali mengandung klausul-klausul eksklusif yang membatasi tanggung jawab perusahaan pada situasi tertentu. Misalnya, kebijakan resmi DANA menyatakan bahwa pengembalian dana bergantung pada fitur *DANA Protection*, yang secara eksplisit mengecualikan kerugian akibat “kelalaian pengguna” dan kasus penipuan (seperti skema investasi bodong, phishing, atau kiriman salah rekening).³⁰

Dalam panduan tersebut, DANA mendorong pengguna “jaga kerahasiaan PIN dan OTP” sebagai tanggung jawab mereka.³¹ Dengan demikian, perusahaan mengalihkan sebagian beban pencegahan ke konsumen, meskipun secara sistem hukum tanggung jawab utama atas keamanan siber seharusnya terletak pada penyedia jasa.

Temuan empiris menunjukkan bahwa ada perbedaan antara standar teknis yang diikuti DANA dan realita atas beban risiko yang ditanggung konsumen. Misalnya, meski DANA menerapkan ISO 27001 dan PCI-DSS, laporan PwC (2023) menemukan hanya 40% perusahaan teknologi di Asia Tenggara sepenuhnya patuh pada standar tersebut. Hal ini menimbulkan kekhawatiran bahwa implementasi masih belum merata.³²

Terlebih lagi, meskipun DANA memiliki fitur keamanan, kebocoran data pribadi dan teknik penyusupan digital terus meningkat. Menurut laporan BSSN (2023), kasus pencurian data pribadi meningkat drastis, sehingga legislasi seperti Undang-Undang Perlindungan Data Pribadi memang dibutuhkan untuk memaksa tindakan protektif tambahan.³³

Secara keseluruhan, analisis ini menunjukkan bahwa meskipun DANA secara formal tunduk pada regulasi ketat Bank Indonesia (misalnya PBI No.2/6/2018 tentang *e-money*)³⁴, kesesuaian antara kewajiban regulasi dan ekspektasi hukum sulit ditegakkan. Konsumen mengharapkan perlindungan maksimal, tetapi DANA menawarkan perlindungan yang bersyarat. Hal ini memperkuat temuan sebelumnya bahwa pencarian pertanggungjawaban nyata dari pihak DANA atas kerugian masih menemui hambatan.

Ketiadaan mekanisme yang terintegrasi dalam menangani penipuan digital memperjelas pentingnya keterlibatan lembaga pengawas yang memiliki mandat luas dalam sektor jasa keuangan. Dalam konteks ini, Otoritas Jasa Keuangan (OJK) memainkan peran penting sebagai pengawas utama stabilitas dan keamanan sistem keuangan digital di Indonesia.

Sebagai lembaga independen yang dibentuk berdasarkan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, OJK diberikan kewenangan untuk menyelenggarakan sistem pengawasan yang terintegrasi terhadap seluruh kegiatan di sektor jasa keuangan, termasuk fintech lending.

Salah satu dasar hukum utama yang digunakan OJK dalam mengawasi kegiatan fintech lending adalah Peraturan OJK (POJK) Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. Regulasi ini mencakup berbagai ketentuan penting, mulai dari prosedur pendaftaran dan perizinan, pengaturan tata kelola perusahaan, hingga kewajiban pelaporan rutin yang harus dipenuhi oleh penyelenggara layanan fintech lending.

²⁹ *Ibid.*

³⁰ DANA. Bagaimana Jika Uang di DANA Hilang? *Dana.id*. <https://www.dana.id/corporate/newsroom/bagaimana-jika-uang-di-dana-hilang>. Diakses 4 Juni 2025 Pukul 08.31 WIB.

³¹ *Ibid.*

³² Aidill, A. M., et al., Op.Cit, 744.

³³ *Ibid.*

³⁴ DANA. Kenapa Aplikasi DANA Tidak Diawasi oleh OJK? *Dana.id*. <https://www.dana.id/corporate/newsroom/kenapa-dana-tidak-diawasi-ojk>. Diakses 4 Juni 2025 Pukul 08.41 WIB.

Dalam pelaksanaan tugas pengawasannya, OJK turut mengadopsi pendekatan berbasis teknologi melalui penggunaan Aplikasi Monitoring Fintech. Dengan sistem ini, OJK dapat melakukan pemantauan terhadap aktivitas penyelenggara fintech secara waktu nyata (*real-time*), guna mengidentifikasi potensi pelanggaran, seperti praktik pemberian pinjaman yang melanggar ketentuan maupun indikasi penyalahgunaan data pribadi konsumen.

OJK turut berwenang menjatuhkan sanksi administratif terhadap penyelenggara fintech lending yang terbukti melanggar ketentuan. Merujuk pada POJK Nomor 77 Tahun 2016, bentuk sanksi yang dapat dikenakan meliputi teguran tertulis, pembekuan aktivitas operasional, hingga pencabutan izin usaha secara permanen.

Selain menjalankan fungsi regulasi dan pengawasan, OJK juga memiliki peran dalam meningkatkan pemahaman masyarakat terkait penggunaan layanan fintech lending secara cermat dan bertanggung jawab. Upaya edukatif ini dilaksanakan melalui berbagai program literasi keuangan, salah satunya melalui Strategi Nasional Literasi dan Inklusi Keuangan (SNLKI).³⁵

Salah satu permasalahan krusial yang kerap terjadi adalah maraknya praktik pinjaman ilegal yang beroperasi tanpa izin dan di luar pengawasan OJK, sehingga memicu berbagai kasus penyalahgunaan data pribadi serta tindak penipuan. Di sisi lain, rendahnya tingkat literasi keuangan di kalangan masyarakat semakin memperburuk situasi, karena meningkatkan potensi terjadinya kredit bermasalah dan penggunaan layanan yang tidak sesuai peruntukannya.

Tantangan lain yang dihadapi adalah bagaimana menjaga keseimbangan antara mendorong inovasi teknologi di sektor fintech lending dan memastikan perlindungan konsumen tetap menjadi prioritas. Mengingat fintech lending beroperasi dalam lanskap digital yang dinamis, diperlukan regulasi yang responsif dan fleksibel, namun tetap sejalan dengan prinsip-prinsip perlindungan hak konsumen sebagaimana tercantum dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.³⁶

OJK diharapkan melakukan revisi kebijakan yang lebih selaras dengan dinamika di lapangan, khususnya dalam konteks perkembangan industri fintech. POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan hingga kini belum secara eksplisit mengakomodasi keberadaan fintech berbasis *peer-to-peer* (P2P) lending sebagai bagian dari pelaku usaha jasa keuangan, sehingga menciptakan kekosongan pengaturan yang dapat berdampak pada lemahnya perlindungan konsumen di sektor ini.³⁷

Pelaku penipuan yang memanfaatkan fitur dompet digital untuk mengambil keuntungan secara melawan hukum dapat dijerat dengan Pasal 378 KUHP tentang penipuan. Pasal ini mengatur bahwa setiap orang yang dengan tipu muslihat atau rangkaian kebohongan menggerakkan orang lain untuk menyerahkan suatu barang atau uang dapat dipidana penjara paling lama empat tahun.

Kegiatan ini dilakukan melalui sarana elektronik, pelaku juga dapat dijerat dengan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pasal 28 ayat (1) UU ITE mengatur bahwa setiap orang yang dengan sengaja menyebarkan berita bohong dan menyesatkan yang merugikan konsumen dalam transaksi elektronik dapat dikenakan pidana.

Sanksi pidana atas perbuatan tersebut, sebagaimana diatur dalam Pasal 45A ayat (1), adalah pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah.

³⁵ Septia, G., et al.

³⁶ Gandasari, N. M., Hidayat, R. R., & Siswajanthry, F. Peran Otoritas Jasa Keuangan (OJK) dalam Mengawasi Fintech Lending sebagai Instrumen Ekonomi Digital. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*.

³⁷ Asmadi, E. (2023). Penyelewengan Data Pribadi dalam Pemanfaatan Aplikasi Financial Technology (Pinjaman Online). Sanksi: Seminar Nasional, Hukum, Sains, Ekonomi.

Tidak hanya itu, apabila penipuan dilakukan dengan cara meretas akun atau sistem DANA tanpa izin, maka pelaku juga dapat dikenai sanksi pidana berdasarkan Pasal 30 sampai 32 UU ITE, yang melarang akses ilegal ke sistem elektronik, pengambilalihan data, serta pengubahan atau penghapusan data digital.

Pengaturan Perlindungan Hukum Terhadap Korban Penipuan Digital di Masa Mendatang

Perkembangan teknologi digital di Indonesia mendorong meningkatnya transaksi keuangan melalui dompet digital seperti DANA. Namun, hal ini juga memicu peningkatan tindak pidana digital. Korban penipuan tidak hanya dirugikan secara materiil, tapi juga kehilangan kepercayaan terhadap ekosistem digital. Karena itu, penguatan perlindungan hukum bagi korban penipuan digital jadi sangat penting di tengah kompleksitas ekonomi digital saat ini.

Secara normatif, perlindungan terhadap korban penipuan digital di Indonesia sudah diatur dalam berbagai perangkat hukum, seperti dalam ranah hukum pidana, perlindungan konsumen, dan perlindungan data pribadi. Instrumen utama yang digunakan adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang sudah mengalami beberapa perubahan.

Pasal 28 ayat (1) UU ITE yang berbunyi "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.", dimana melarang penyebaran berita bohong yang merugikan konsumen dalam transaksi elektronik. Pelaku yang memenuhi unsur pasal ini dapat dipidana, dengan ancaman pidana diatur dalam Pasal 45 ayat (1), yaitu penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi pilar penting dalam membuat sistem perlindungan bagi setiap individu atas data pribadinya. UU ini secara gamblang memberikan hak kepada subjek data untuk memperoleh informasi apabila terjadi kebocoran data serta hak untuk mendapatkan kompensasi jika terjadi pelanggaran.³⁸

Dari sisi perlindungan konsumen, Otoritas Jasa Keuangan (OJK) sudah mengeluarkan Peraturan OJK (POJK) No. 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Regulasi ini menekankan tanggung jawab penyedia layanan jasa keuangan terhadap konsumen. Ini termasuk jika terjadi kerugian akibat tindakan *fraud* atau penipuan.

Dalam praktiknya, perlindungan hukum terhadap korban dibagi menjadi dua pendekatan utama, yaitu preventif dan represif. Perlindungan preventif ini berfokus pada upaya pencegahan sebelum terjadi tindak kejahatan. Salah satunya melalui peningkatan literasi digital masyarakat. Pemerintah, melalui Kementerian Komunikasi dan Informatika, OJK, dan Bank Indonesia secara rutin melakukan edukasi publik terkait dengan adanya bahaya penipuan digital, pentingnya menjaga kerahasiaan data pribadi, dan mengenali ciri-ciri modus penipuan.

Di sisi lain, bentuk pengawasan dan pengendalian juga diwujudkan melalui pembentukan Satgas Waspada Investasi yang tugasnya menindak penawaran investasi ilegal serta mengawasi layanan keuangan berbasis digital yang belum sepenuhnya terdaftar di bawah lembaga pengawasan resmi.

Sementara itu, perlindungan dengan bentuk represif diberikan pasca terjadinya kejahatan. Aparat Penegak Hukum memiliki peran penting untuk memastikan bahwa pelaku penipuan digital dapat dihukum sesuai dengan ketentuan yang berlaku, serta agar korban penipuan mendapat keadilan. Restitusi dan ganti rugi menjadi bagian dari upaya pemulihan hak-hak korban.

³⁸ Pomounda, Ika. "Perlindungan Hukum Bagi Korban Penipuan Melalui Media Elektronik (Suatu Pendekatan Viktimologi)". (2015). Legal Opinion, 3(4).

Tantangan utama dalam melindungi korban penipuan digital ada di dinamika modus operandi kejahatan yang semakin kompleks. Modus seperti *phishing*, *scam*, aplikasi palsu, hingga penyalahgunaan data pribadi menjadi sangat sulit untuk dideteksi dan ditindak secara cepat. Agar dapat memberikan perlindungan yang efektif terhadap korban, sistem regulasi dan peningkatan kapasitas para penegak hukum harus ditingkatkan dan diperbarui baik dalam hal digital forensik maupun kemampuan memahami pola kejahatan siber.

Di masa mendatang, regulasi akan lebih menekankan perlindungan hak-hak korban sebagai subjek utama. Penyesuaian dengan standar internasional seperti *General Data Protection Regulation* (GDPR) akan memperkuat hak atas penghapusan data, dilupakan, dan tuntutan ganti rugi akibat pelanggaran data. Teknologi seperti sistem pelaporan *online*, pemantauan transaksi, dan *AI* untuk deteksi potensi *fraud* akan menjadi elemen penting perlindungan. Penegak hukum juga perlu pelatihan khusus guna mengikuti perkembangan teknologi dan kejahatan digital.

Perlindungan korban penipuan melalui aplikasi DANA dan dompet digital lainnya merupakan isu mendesak yang memerlukan pendekatan holistik. Reformasi hukum dibutuhkan melalui revisi UU ITE, penguatan UU PDP, dan penyesuaian regulasi keuangan digital oleh OJK dan Bank Indonesia. Prinsip keadilan restoratif, penguatan kapasitas penegak hukum, dan sinergi antar pemangku kepentingan menjadi kunci membangun sistem perlindungan hukum yang responsif terhadap korban penipuan digital.

Dalam era digitalisasi ekonomi, layanan keuangan berbasis teknologi seperti dompet digital (*e-money*) semakin populer. Namun demikian, peningkatan transaksi online disertai pula resiko penipuan siber yang merugikan konsumen. Dari sudut pandang hukum bisnis, pelaku usaha penyedia layanan tersebut, misalnya penyelenggara dompet digital seperti DANA memiliki tanggung jawab besar untuk melindungi konsumen dan mencegah kejahatan digital.

Pemerintah Indonesia sudah mulai merespon dengan regulasi terkini, seperti Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022, serta aturan sektor keuangan, seperti Peraturan Bank Indonesia tentang uang elektronik. Meski begitu masih banyak tantangan, misalnya UU ITE hanya mengatur pidana pelaku penipu tanpa ketentuan kompensasi bagi korban.³⁹

Oleh karena itu, perlu dibahas bagaimana tanggung jawab hukum perusahaan digital dikaitkan dengan peraturan perlindungan korban, sekaligus bagaimana sistem hukum bisnis perlu dikembangkan untuk mengantisipasi kejahatan digital di masa depan.

Pelaku usaha digital, khususnya penyelenggara dompet digital *e-money*, wajib menerapkan berbagai langkah preventif dan protektif. Pertama, menurut Peraturan Bank Indonesia Nomor 20/6/PBI/2018, penerbit uang elektronik harus menerapkan manajemen risiko yang efektif dan standar keamanan sistem yang informasi yang tinggi.⁴⁰ Artinya, perusahaan wajib membangun sistem TI (Teknologi Informasi) tahan serangan, mengenkripsi data, dan mengelola resiko penipuan secara proaktif.

Kedua, dari sudut perlindungan konsumen, OJK menegaskan bahwa perusahaan fintech harus menjaga transparansi informasi kepada pengguna, termasuk kejelasan hak dan kewajiban, biaya, serta potensi resiko dan mitigasinya.⁴¹ Misalnya, informasi tentang resiko penipu dan kebijakan perlindungan data harus disampaikan dengan jelas kepada konsumen (hak konsumen atas informasi benar sesuai Pasal 4 huruf c UUPK).

³⁹ Indrawan, M. & Permatasari, P. (2022). Perlindungan Hukum Korban Penipuan Transaksi Jual Beli Online Melalui Ganti Rugi. *Jurnal Kewarganegaraan*, 6(3), 6488-6489.

⁴⁰ Elias, J. I. P., Rumengan, H. Y. & Midu, S. Tanggung Jawab Penerbit dan Pengguna *E-money* dalam Transaksi Perdagangan Menurut Hukum Perbankan di Indonesia. *Jurnal Fakultas Hukum Unsrat*, 16(1).

⁴¹ Iswandhi, C. O. (2025). Perlindungan Hukum untuk Pelaku Usaha di Era Digital: Jangan Asal Posting Produk! *News.sah.co.id*. <https://news.sah.co.id/perlindungan-hukum-untuk-pelaku-usaha-di-era-digital-jangan-asal-posting-produk/>. Diakses 8 Juni 2025 Pukul 19.31 WIB.

Ketiga, pengelolaan data pribadi konsumen menjadi kewajiban penting. Dengan berlakunya Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022, perusahaan fintech diwajibkan menunjuk Pejabat Perlindungan Data dan memastikan data pengguna diproses hanya sesuai tujuan yang sah.⁴²

Sebelum itu, Permenkominfo Nomor 20 Tahun 2016 dan PP Nomor 82 Tahun 2012 juga menegaskan bahwa penyelenggara sistem elektronik “diharuskan menjaga kerahasiaan data pribadi” dan hanya menggunakan data dengan izin pemiliknya.⁴³ Dengan demikian, pelaku usaha wajib meminimalkan pengumpulan data, melindungi privasi pengguna, dan mendapatkan persetujuan eksplisit ketika data ingin digunakan (sejalan dengan prinsip GDPR).⁴⁴

Keempat, terdapat kewajiban pemulihan bagi korban penipuan. Bank Indonesia bahkan mensyaratkan agar penyelenggara *e-money* memiliki mekanisme kompensasi finansial bagi pengguna yang dirugikan akibat kesalahan sistem atau tindakan kriminal, selama bukan kesalahan pengguna.⁴⁵ Hal ini sesuai pasal 43 PBI 20/6/2018 yang eksplisit mengatur mekanisme penggantian kerugian tersebut. Apabila penyelenggara gagal memenuhi kewajiban ini, ia dapat dikenai sanksi administratif (teguran, denda, penghentian izin) oleh Bank Indonesia.⁴⁶

Secara lebih umum, hak konsumen Indonesia untuk mendapatkan ganti rugi diatur dalam Undang-Undang Perlindungan Konsumen Nomor 8 Tahun 1999 Pasal 4.⁴⁷ Meskipun demikian, praktik penagakannya masih lemah, khususnya dalam kasus penipuan online karena UU ITE belum mengatur ganti rugi korban secara khusus.⁴⁸

Secara ringkas, tanggung jawab pelaku usaha digital meliputi penguat keamanan dan anti-*fraud* (sesuai PBI 20/6/2018), perlindungan konsumen (transparansi dan kepatuhan pada UUPK), pengelolaan data pribadi (UU PDP), serta kewajiban memberikan pemulihan berupa kompensasi kepada korban (mekanisme penggantian kerugian dalam PBI). Inisiatif swasta juga muncul untuk mendukung misalnya asosiasi AFTECH menerbitkan pedoman pelaksanaan UU PDP agar perusahaan meningkatkan keamanan data dan kepercayaan konsumen.⁴⁹

Untuk merespon dinamika kejahatan digital, sistem hukum bisnis Indonesia perlu berevolusi melalui reformasi regulasi dan harmonisasi internasional. Regulasi domestik saat ini sedang diperkuat, misalnya pemberlakuan UU PDP Nomor 27 Tahun 2022 merupakan tonggak baru perlindungan data pribadi bagi konsumen digital.⁵⁰

⁴² Administrator. (2024). Era Baru Perlindungan Data Pribadi. *Indonesia.go.id*. <https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1>. Diakses 8 Juni 2025 Pukul 19.59 WIB.

⁴³ Septia, G., et al., Op.Cit, 10 & 14.

⁴⁴ Administrator. (2024). Era Baru Perlindungan Data Pribadi. *Indonesia.go.id*. <https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1>. Diakses 8 Juni 2025 Pukul 19.59 WIB.

⁴⁵ Elias, J. I. P., Rumengan, H. Y. & Midu, S. Tanggung Jawab Penerbit dan Pengguna *E-money* dalam Transaksi Perdagangan Menurut Hukum Perbankan di Indonesia. *Jurnal Fakultas Hukum Unsrat*, 16(1).

⁴⁶ *Ibid*.

⁴⁷ Iswandhi, C. O. (2025). Perlindungan Hukum untuk Pelaku Usaha di Era Digital: Jangan Asal Posting Produk! *News.sah.co.id*. <https://news.sah.co.id/perlindungan-hukum-untuk-pelaku-usaha-di-era-digital-jangan-asal-posting-produk/>. Diakses 8 Juni 2025 Pukul 19.31 WIB.

⁴⁸ Indrawan, M., et al., Op.Cit, 6488.

⁴⁹ Pratama, R. (2025). Press Release - Dissemination of Personal Data Protection (PDP) Guidelines in the Fintech Industry. *Fintech.id*. <https://fintech.id/en/education-and-literacy/latest-news/siaran-pers-aftech-sosialisasi-pedoman-pdp-di-industri-fintech>. Diakses 8 Juni 2025 Pukul 20.18 WIB.

⁵⁰ Administrator. (2024). Era Baru Perlindungan Data Pribadi. *Indonesia.go.id*. <https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1>. Diakses 8 Juni 2025 Pukul 19.59 WIB.

Pemerintah tengah merumuskan aturan turunan (PP dan Perpres) serta Badan Pengawas Perlindungan Data Pribadi untuk menjalankan UU ini.⁵¹ Di samping itu, perlu dilakukan revisi atau penyempurnaan undang-undang lain seperti UU ITE dan PP Nomor 82 Tahun 2012 untuk memasukkan kewajiban perlindungan korban dan standar keamanan yang lebih tegas. Misalnya, UU ITE saat ini hanya mengancam pidana pelaku penipuan tanpa mengatur ganti rugi korban⁵²; ke depan perlu tambah kewajiban kompensasi sebagai tanggung jawab sosial perusahaan digital.

Dengan demikian, regulasi perdagangan elektronik (PP Nomor 80 Tahun 2019) dan aturan *e-commerce* layak diperkuat agar kewajiban perlindungan konsumen di ranah online lebih jelas.

Harmonisasi internasional menjadi kunci agar regulasi nasional sejalan dengan praktik global. UU PDP dirancang meniru prinsip-prinsip GDPR Uni Eropa yang dikenal ketat.⁵³ Banyak ahli menyarankan Indonesia mencontoh penerapan GDPR, termasuk pembentukan otoritas independen untuk memastikan kepatuhan perusahaan teknologi.⁵⁴

Selain itu, standar perlindungan konsumen lintas batas (misalnya Omnibus Directive UE) atas konvensi internasional tentang kejahatan siber perlu dipantau agar kebijakan domestik adaptif terhadap tren global. Dalam konteks ini, pemeriksaan dan pengawasan bersama (misalnya kerjasama OJK dengan regulator asing) dapat memperkuat efektivitas penegakan hukum siber.

Peran sektor swasta juga sangat penting dalam keamanan digital. Selain mematuhi regulasi, perusahaan digital dituntut proaktif membangun ekosistem yang aman. OJK, misalnya, sudah mendorong lembaga keuangan untuk menerapkan strategi anti-*fraud* menyeluruh (melibatkan dewan komisaris, direksi, kebijakan internal, dan pengawasan ketat).

Di tingkat industri, AFTECH menyelenggarakan sosialisasi pedoman perlindungan data untuk anggota fintech guna meningkatkan keamanan dan kepercayaan pengguna.⁵⁵ Seperti yang sudah disebut perusahaan juga dapat menerapkan praktik terbaik global (misal ISO 27001), PCI DSS) dan menggunakan teknologi deteksi penipuan terkini. Kolaborasi publik-swasta, misalnya lewat pusat inovasi OJK maupun forum seperti Indonesia Fintech Summit, dimana memperkuat pertukaran informasi ancaman siber dan pengembangan solusi bersama.

Pergeseran paradigma hukum bisnis turut diperlukan. Bisnis tidak lagi hanya melihat hubungan kontraktual semata, tetapi juga tanggung jawab sosial dan etika digital. Konsep Tanggung Jawab Digital Perusahaan (Corporate Digital Responsibility - CDR) berkembang sebagai kelanjutan CSR tradisional.⁵⁶

Dalam CDR, perusahaan bertanggung jawab atas konsekuensi proses digitalnya terhadap semua pemangku kepentingan (karyawan, pemasok, konsumen, masyarakat) dan lingkungan.⁵⁷ Contohnya, Twitter Indonesia membantu korban kekerasan berbasis gender melalui layanan digital sebagai bentuk CDR.⁵⁸ Di Indonesia, implementasi CDR masih menghadapi tantangan

⁵¹ *Ibid.*

⁵² Indrawan, M., et al., Op.Cit, 6488.

⁵³ Administrator. (2024). Era Baru Perlindungan Data Pribadi. *Indonesia.go.id*. <https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1>. Diakses 8 Juni 2025 Pukul 19.59 WIB.

⁵⁴ *Ibid.*

⁵⁵ Pratama, R. (2025). Press Release - Dissemination of Personal Data Protection (PDP) Guidelines in the Fintech Industry. *Fintech.id*. <https://fintech.id/en/education-and-literacy/latest-news/siaran-pers-aftech-sosialisasi-pedoman-pdp-di-industri-fintech>. Diakses 8 Juni 2025 Pukul 20.18 WIB.

⁵⁶ Solihin. (2023). Tanggung Jawab Digital Perusahaan di Indonesia: Sebuah Tinjauan Konseptual. *Medkom: Jurnal Media dan Komunikasi*, 3(2), 76.

⁵⁷ *Ibid*, 78.

⁵⁸ *Ibid*, 85.

(misalnya belum ada payung hukum).⁵⁹ Oleh karenanya, pengembangan norma dan budaya bisnis yang menekankan kejujuran, tanggung jawab sosial, dan etika digital sangat krusial.

Regulasi di masa depan mungkin mencakup kewajiban pelaporan dampak sosial digital, audit etika AI, dan insentif bagi perusahaan yang menerapkan tata kelola digital bertanggung jawab. Dengan demikian, sistem hukum bisnis bergeser dari sekadar menegakkan kontrak menuju menegakkan nilai-nilai sosial dan kepercayaan publik dalam ekonomi digital.

KESIMPULAN

Fokus penelitian ini adalah masalah hukum terkait dengan *financial technology* (fintech), khususnya layanan dompet digital DANA, yang sangat populer di Indonesia. Selama penggunaan aplikasi DANA, masih ada celah hukum yang membuat konsumen kurang dilindungi dari penipuan digital dan pencurian data pribadi.

Pelaku pelanggaran digital dapat dijerat oleh Pasal 378 KUHP, Pasal 28 ayat (1) jo. Pasal 45A Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dan Pasal-Pasal terkait dalam UU Perlindungan Data Pribadi. Keterbatasan penegak hukum dalam menangani kejahatan siber yang kompleks dan cepat berkembang sering menghambat pelaksanaan dasar hukum.

Penyedia layanan fintech seperti DANA diwajibkan oleh hukum bisnis untuk memastikan keamanan sistem, transparansi data, dan perlindungan data pengguna. Meskipun diatur oleh berbagai undang-undang, seperti UU Perlindungan Konsumen, UU PDP, dan peraturan Bank Indonesia, penyedia layanan sering membatasi tanggung jawabnya melalui klausul eksklusif, dan mekanisme pengaduan belum sepenuhnya membantu korban.

Penelitian ini menunjukkan bahwa industri fintech Indonesia membutuhkan regulasi lebih kuat, tata kelola yang lebih transparan, dan kerja sama dari semua pemangku kepentingan. Hukuman saat ini tidak cukup untuk menangani kompleksitas transaksi digital dan melindungi korban penipuan di era fintech. Oleh karena itu, untuk membuat ekosistem keuangan digital yang adil dan aman, pendekatan yang mengintegrasikan kebijakan publik.

Saran

Pemerintah perlu memperkuat integrasi antara Undang-Undang Perlindungan Konsumen, Undang-Undang ITE, dan Undang-Undang Perlindungan Data Pribadi untuk memastikan perlindungan hukum yang efektif bagi korban jika mereka ingin menciptakan ekosistem fintech yang aman dan adil. Pembaruan regulasi secara menyeluruh diperlukan untuk menjawab tantangan penipuan digital dalam layanan dompet elektronik seperti DANA.

Penyedia layanan fintech harus meningkatkan sistem keamanan teknologi mereka dan memperjelas mekanisme ganti rugi, bukan hanya mengalihkan tanggung jawab kepada pelanggan. Disisi lain, penegak hukum harus memperkuat kemampuan digital forensik dan kejahatan siber melalui kerja sama lintas lembaga dan pelatihan yang berkelanjutan.

Selain itu, literasi digital masyarakat harus diperluas untuk memberi pengguna pemahaman yang cukup tentang hak dan risiko mereka sebagai konsumen fintech. Perlindungan hukum dalam industri fintech dapat berhasil dan berkelanjutan jika regulasi, penegakan hukum, tanggung jawab penyedia layanan, dan kesadaran konsumen bekerja sama.

⁵⁹ *Ibid*, 89-90.

DAFTAR PUSTAKA

- Administrator. (2024). *Era Baru Perlindungan Data Pribadi*. Indonesia.go.id. <https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=en>. Diakses 8 Juni 2025, pukul 19.59 WIB.
- Affan, S. I. (2024). *Kronologi Nasabah Diduga Kebobolan Uang Rp6 Juta di Aplikasi DANA*. Bloombergtechnoz.com. <https://www.bloombergtechnoz.com/detail-news/25873/kronologi-nasabah-diduga-kebobolan-uang-rp6-juta-di-aplikasi-dana>. Diakses 3 Juni 2025, pukul 19.59 WIB.
- Aidill, A. M., Darmawan, M. A., & Summa. (2025). Analisis Perlindungan Hukum Dalam Transaksi Transfer Melalui Aplikasi Dana. *Jurnal Kajian Hukum dan Kebijakan Publik*, 2(2), 741.
- Annur, C. M. (2023). *Indeks Literasi Digital Indonesia (2020-2022)*. Databoks.katadata.co.id. <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/494c92f675bfffcc/literasi-digital-indonesia-naik-pada-2022-tapi-budaya-digital-turun>. Diakses 3 Juni 2025, pukul 20.19 WIB.
- Asmadi, E. (2023). Penyelewengan Data Pribadi dalam Pemanfaatan Aplikasi Financial Technology (Pinjaman Online). *SANKSI: Seminar Nasional, Hukum, Sains, Ekonomi*.
- DANA. *Bagaimana Jika Uang di DANA Hilang?* Dana.id. <https://www.dana.id/corporate/newsroom/bagaimana-jika-uang-di-dana-hilang>. Diakses 4 Juni 2025, pukul 08.31 WIB.
- DANA. *Kenapa Aplikasi DANA Tidak Diawasi oleh OJK?* Dana.id. <https://www.dana.id/corporate/newsroom/kenapa-dana-tidak-diawasi-ojk>. Diakses 4 Juni 2025, pukul 08.41 WIB.
- Elias, J. I. P., Rumengan, H. Y., & Midu, S. (n.d.). Tanggung Jawab Penerbit dan Pengguna E-money dalam Transaksi Perdagangan Menurut Hukum Perbankan di Indonesia. *Jurnal Fakultas Hukum Unsrat*, 16(1).
- Gandasari, N. M., Hidayat, R. R., & Siswajanthi, F. (n.d.). Peran Otoritas Jasa Keuangan (OJK) dalam Mengawasi Fintech Lending sebagai Instrumen Ekonomi Digital. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*.
- Hartanto, Rosadi, V., & Yosmar, E. A. (2023). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana. *PATTIMURA Legal Journal*, 2(3), 273.
- Indrawan, M., & Permatasari, P. (2022). Perlindungan Hukum Korban Penipuan Transaksi Jual Beli Online Melalui Ganti Rugi. *Jurnal Kewarganegaraan*, 6(3), 6488-6489.
- Indriani, W., & Asih, S. P. (2024). Pengaruh Persepsi Kemudahan, Persepsi Risiko, Keamanan, dan Fitur Layanan terhadap Minat Penggunaan Dompot Digital pada Aplikasi DANA di Kabupaten Tulang Bawang Barat. *Tanpa nama jurnal*, 166.
- Iswandhi, C. O. (2025). *Perlindungan Hukum untuk Pelaku Usaha di Era Digital: Jangan Asal Posting Produk!* News.sah.co.id. <https://news.sah.co.id/perlindungan-hukum-untuk-pelaku-usaha-di-era-digital-jangan-asal-posting-produk/>. Diakses 8 Juni 2025, pukul 19.31 WIB.
- Kirana, T., Roisah, R., Solihat, A., & Mauliyan, F. F. (2024). Pengaruh Tingkat Keamanan dan Kepercayaan Dompot Digital terhadap Kepuasan Konsumen (Studi Kasus di Kota Bandung). *Jurnal Sains Manajemen*, 6(2), 96.
- Pakasi, S. S., Muaja, H. S., & Kermite, J. A. (2021). Tinjauan Hukum Terhadap Penggunaan Dompot Digital dalam Bertransaksi di Indonesia. *Lex Crimen*, 10(12), 69.
- Paridah, N., Yunitasari, K., Putri, R. A. A., & Sahrir, I. F. (2024). Perlindungan Hukum Terhadap Nasabah Bank Dalam Penggunaan Aplikasi Dana Di Indonesia. *Tanpa nama jurnal*, 47.
- Pomounda, I. (2015). Perlindungan Hukum Bagi Korban Penipuan Melalui Media Elektronik (Suatu Pendekatan Viktimologi). *Legal Opinion*, 3(4).

- Pratama, R. (2025). *Press Release - Dissemination of Personal Data Protection (PDP) Guidelines in the Fintech Industry*. Fintech.id. <https://fintech.id/en/education-and-literacy/latest-news/siaran-pers-aftech-sosialisasi-pedoman-pdp-di-industri-fintech>. Diakses 8 Juni 2025, pukul 20.18 WIB.
- RHEY. (2023, 31 Agustus). *Pencurian di Akun DANA, Pihak DANA Lepas Tangan*. Mediakonsumen.com. <https://mediakonsumen.com/2023/08/31/surat-pembaca/pencurian-di-akun-dana-pihak-dana-lepas-tangan>. Diakses 3 Juni 2025, pukul 19.54 WIB.
- Septia, G., Ningsih, R. A., Lindawati, Faadhilah, S. D. N., & Anugrah, D. (2024). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana Atas Kejahatan Link Phising dan Hacking Pada Layanan Digital. *LETTERLIJK: Jurnal Hukum Perdata*, 1(1), 4.
- Solihin. (2023). Tanggung Jawab Digital Perusahaan di Indonesia: Sebuah Tinjauan Konseptual. *Medkom: Jurnal Media dan Komunikasi*, 3(2), 76.
- Ummi, A. Y., Pinasti, S. A., & Ramadhani, S. P. (2024). Hukum Perlindungan Konsumen dalam Produk Perbankan Digital (Studi Kasus Dana). *Tanpa nama jurnal*, 118.