

TANGGUNG JAWAB KETAT PENYELENGGARA E-WALLET ATAS HILANGNYA SALDO DANA

Fauzan Saputra^{1*}, Muhammad Iqbal², Fandini Putri³, Mahyal Iqbal⁴

^{1,2,3,4} Program Studi Hukum, Sekolah Tinggi Ilmu Hukum Al-Banna Lhokseumawe-Aceh, Indonesia

*Corresponding author: fauzanlsm749@gmail.com

Abstrak

Artikel ini menganalisis perlindungan hukum pengguna e-wallet atas hilangnya saldo pada aplikasi DANA dalam sistem pembayaran digital. Berbeda dari skripsi sumber yang menekankan kebijakan keamanan, layanan pengaduan, dan pengembalian saldo, artikel ini memperkuat analisis melalui konstruksi tanggung jawab ketat berbasis presumption of liability. Metode yang digunakan adalah penelitian hukum normatif dengan dukungan data empiris dari kasus dan wawancara dalam skripsi. Hasil kajian menunjukkan bahwa kehilangan saldo tidak cukup dipahami sebagai sengketa layanan, tetapi sebagai peristiwa hukum berlapis yang menyangkut perlindungan konsumen, keamanan sistem pembayaran, perlindungan data pribadi, dan pembuktian transaksi tidak sah. Penyelenggara e-wallet wajib membuktikan bahwa sistemnya aman, transaksi sah, dan kerugian bukan akibat kegagalan layanan. Artikel ini menawarkan model pemulihan saldo berbasis audit digital, pembalikan beban pembuktian, pengaduan berjenjang, dan pengawasan regulator.

Kata Kunci: e-wallet, DANA, perlindungan konsumen, kehilangan saldo, tanggung jawab ketat

Abstract

This article analyzes legal protection for e-wallet users whose balances disappear in the DANA digital payment application. Unlike the underlying thesis, which focused on security policies, customer service responses, and refund procedures, this article strengthens the legal analysis through a strict responsibility framework based on the presumption of liability. The study uses normative legal research supported by empirical data from cases and interviews discussed in the thesis. The findings show that lost balances should not be treated merely as service complaints, but as multilayered legal events involving consumer protection, payment system security, personal data protection, and proof of unauthorized transactions. E-wallet providers must be required to prove that their systems were secure, the transactions were valid, and the loss was not caused by service failure. The article proposes a recovery model based on digital audit trails, reversal of the burden of proof, tiered complaint handling, regulatory supervision, and proportional compensation to restore consumer confidence in digital payment systems.

Keywords: e-wallet, DANA, consumer protection, lost balance, strict liability

1. PENDAHULUAN

Transformasi digital telah mengubah sistem pembayaran dari transaksi tunai menuju transaksi berbasis aplikasi. Dompet elektronik atau e-wallet menjadi instrumen yang banyak digunakan karena mampu menyimpan nilai uang secara elektronik, memudahkan transfer dana, pembayaran QRIS, pembelian pulsa, belanja daring, dan pembayaran berbagai tagihan. Dalam skripsi yang menjadi sumber artikel ini, DANA dijelaskan sebagai salah satu penyedia dompet digital yang memperoleh izin Bank Indonesia dan mengalami pertumbuhan pengguna yang signifikan, namun pada saat yang sama menghadapi keluhan mengenai kehilangan saldo, keterlambatan tanggapan layanan, serta ketidakjelasan mekanisme pengembalian dana (Khoironnisa, 2024).

Permasalahan hilangnya saldo e-wallet tidak boleh dipandang hanya sebagai gangguan teknis atau sengketa privat antara pengguna dan aplikasi. Saldo yang tersimpan dalam e-wallet merupakan nilai ekonomi yang melekat pada hak konsumen. Ketika saldo hilang karena transaksi yang tidak diakui pengguna, pembobolan akun, kebocoran OTP, pengambilalihan perangkat, kegagalan autentikasi biometrik, atau kelemahan pemantauan fraud, maka peristiwa

tersebut menyentuh beberapa rezim hukum sekaligus. Pertama, rezim perlindungan konsumen karena pengguna merupakan pihak yang menerima jasa pembayaran. Kedua, rezim sistem pembayaran karena penyelenggara e-wallet adalah pelaku industri sistem pembayaran yang harus menjaga keamanan, keandalan, dan integritas pemrosesan dana. Ketiga, rezim perlindungan data pribadi karena akun e-wallet mengelola data identitas, nomor telepon, PIN, OTP, data biometrik, riwayat transaksi, dan data perangkat.

Skripsi sumber telah memberikan kontribusi penting dengan memetakan keluhan pengguna, kebijakan aplikasi DANA, peran Bank Indonesia dan OJK, serta jalur penyelesaian sengketa. Namun, agar dapat menjadi artikel jurnal yang memiliki kebaruan akademik, analisis perlu diperkuat dengan pertanyaan yang lebih tajam: siapa yang harus menanggung risiko hukum ketika transaksi tidak diakui oleh pengguna, bagaimana beban pembuktian dibagi antara konsumen dan penyelenggara, dan apakah klausul layanan yang membatasi tanggung jawab penyelenggara hanya pada kesalahan sistem dapat dibenarkan menurut perlindungan konsumen dan perlindungan data pribadi.

Artikel ini membedakan diri dari skripsi sumber dengan mengembangkan konstruksi tanggung jawab ketat terbatas atau *presumption of liability*. Konstruksi ini tidak berarti penyelenggara selalu harus mengganti setiap kehilangan saldo tanpa syarat. Maksudnya, dalam kasus transaksi tidak sah, penyelenggara yang menguasai sistem, log transaksi, rekaman autentikasi, data perangkat, dan mekanisme fraud monitoring harus terlebih dahulu membuktikan bahwa transaksi benar-benar sah, dilakukan oleh pengguna, dan tidak terjadi kelemahan sistem atau kegagalan pengamanan. Tanpa pembuktian yang transparan dan dapat diaudit, kerugian tidak adil apabila sepenuhnya dibebankan kepada konsumen yang secara teknis berada pada posisi lemah.

Penguatan analisis tersebut relevan dengan perkembangan regulasi. Bank Indonesia telah menata ulang industri sistem pembayaran melalui Peraturan Bank Indonesia Nomor 10 Tahun 2025 tentang Pengaturan Industri Sistem Pembayaran, yang mulai berlaku pada 31 Maret 2026 dan mencakup penyelenggara jasa sistem pembayaran, tata kelola, manajemen risiko, perilaku pasar, perlindungan konsumen, serta data sistem pembayaran (Bank Indonesia, 2025). Selain itu, Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Perlindungan Konsumen Bank Indonesia menegaskan prinsip perlindungan, hak dan kewajiban penyelenggara dan konsumen, penanganan pengaduan, pelaporan, pengawasan, dan koordinasi (Bank Indonesia, 2023). Sementara itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menempatkan perlindungan data pribadi sebagai upaya untuk menjamin hak konstitusional subjek data pribadi (Republik Indonesia, 2022).

Rumusan masalah artikel ini adalah bagaimana konstruksi pertanggungjawaban hukum penyelenggara e-wallet atas hilangnya saldo pengguna, dan bagaimana model penyelesaian hukum yang lebih adil agar berbeda dari penelitian skripsi yang lebih deskriptif. Tujuan artikel ini adalah menyusun argumentasi hukum yang lebih normatif dan operasional melalui pendekatan tanggung jawab ketat terbatas, pembalikan beban pembuktian, audit digital, serta pemulihan saldo yang proporsional.

2. METODE

Artikel ini menggunakan metode penelitian hukum normatif dengan dukungan data empiris yang berasal dari skripsi sumber. Pendekatan perundang-undangan digunakan untuk menelaah Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Undang-Undang Informasi dan Transaksi Elektronik, Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Perlindungan Konsumen Bank Indonesia, Peraturan Bank Indonesia Nomor 10 Tahun 2025 tentang Pengaturan Industri

Sistem Pembayaran, POJK Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, serta aturan mengenai penyelesaian sengketa di sektor keuangan.

Pendekatan konseptual digunakan untuk menganalisis perlindungan konsumen digital, tanggung jawab pelaku usaha jasa, presumption of liability, pembalikan beban pembuktian, audit trail, keamanan data pribadi, dan dispute resolution. Pendekatan kasus digunakan dengan membaca ulang kasus kehilangan saldo yang dikumpulkan dalam skripsi, termasuk contoh keluhan pengguna yang saldo DANA-nya hilang setelah akun diretas atau digunakan untuk transaksi yang tidak dikenali, serta hasil wawancara pengguna yang tidak memperoleh kejelasan pengembalian saldo. Analisis dilakukan secara kualitatif dengan menghubungkan norma hukum, posisi para pihak, karakter teknologi e-wallet, dan kebutuhan perlindungan konsumen.

3. HASIL DAN PEMBAHASAN

3.1. State of the Art dan Pembeda dengan Skripsi Sumber

Kebaruan utama artikel ini terletak pada pergeseran fokus dari deskripsi perlindungan pengguna menjadi rekonstruksi pertanggungjawaban hukum penyelenggara. Skripsi sumber telah mengidentifikasi empat masalah: kelemahan sistem keamanan, ketidakpuasan pengguna atas respons aplikasi, kurangnya perlindungan hukum ketika saldo hilang akibat peretasan atau kesalahan sistem, dan belum optimalnya implementasi regulasi perlindungan konsumen serta pengamanan transaksi digital (Khoironnisa, 2024). Artikel ini menerima temuan tersebut sebagai basis, tetapi tidak berhenti pada kesimpulan bahwa keamanan dan layanan pelanggan perlu diperbaiki.

Analisis artikel diarahkan pada penentuan standar hukum. Dalam hubungan e-wallet, pengguna hampir tidak mungkin membuktikan sendiri apakah transaksi terjadi karena phishing, malware, SIM swap, kelalaian menjaga OTP, kegagalan sistem, kebocoran data, atau lemahnya deteksi fraud. Semua data teknis berada pada penyelenggara. Oleh sebab itu, logika hukum yang adil harus menggeser sebagian beban pembuktian kepada penyelenggara. Inilah perbedaan penting artikel ini dengan skripsi sumber.

Tabel 1. Perbedaan fokus skripsi dan artikel

Aspek	Skripsi Sumber	Penguatan dalam Artikel
Fokus masalah	Perlindungan pengguna DANA, respons layanan pelanggan, dan prosedur pengembalian saldo.	Konstruksi tanggung jawab penyelenggara atas transaksi tidak sah dengan presumption of liability.
Dasar analisis	UUPK, UU ITE, UU PDP, peran BI dan OJK, serta wawancara pengguna.	Integrasi rezim perlindungan konsumen, PBI 10/2025, PBI 3/2023, UU PDP, audit digital, dan beban pembuktian.
Posisi konsumen	Konsumen sebagai pihak yang mengalami kerugian dan mengajukan pengaduan.	Konsumen sebagai pihak lemah secara informasi sehingga harus memperoleh perlindungan prosedural dan pembuktian.
Model penyelesaian	Pengaduan internal, LAPS, dan litigasi.	Model berjenjang: pembekuan cepat, audit transaksi, pembuktian penyelenggara, pemulihan sementara, LAPS, dan gugatan.
Kebaruan	Menyarankan penguatan keamanan dan transparansi.	Menawarkan uji tanggung jawab berbasis kendali sistem, risiko teknologi, dan perlindungan data pribadi.

3.2. E-Wallet sebagai Jasa Sistem Pembayaran dan Hubungan Hukum Konsumen

Dalam rezim hukum sistem pembayaran, e-wallet bukan sekadar aplikasi penyimpan saldo, tetapi bagian dari ekosistem pemindahan dana. DANA menyatakan diri sebagai Penyedia Jasa Pembayaran kategori I yang terdaftar dan diawasi oleh Bank Indonesia dan Kominfo, dengan layanan yang mencakup inisiasi transaksi, acquiring, dompet elektronik, payment gateway, penerbitan instrumen atau akun pembayaran, serta remitansi atau transfer dana (DANA, 2026). Status tersebut penting karena hubungan antara pengguna dan penyelenggara tidak dapat direduksi menjadi hubungan kontraktual biasa. Penyelenggara mengelola infrastruktur kepercayaan publik yang berkaitan dengan nilai uang, identitas digital, dan rekam transaksi.

PBI 10/2025 memperluas pendekatan pengaturan industri sistem pembayaran dengan menekankan tata kelola, manajemen risiko, praktik pasar, perilaku pelaku industri, perlindungan konsumen, serta data dan informasi sistem pembayaran (Bank Indonesia, 2025). Dengan demikian, perlindungan pengguna e-wallet tidak hanya diukur dari ada atau tidaknya menu bantuan dalam aplikasi, tetapi juga dari kualitas pengendalian risiko, keamanan autentikasi, integritas data, transparansi investigasi, dan efektivitas pengembalian kerugian.

Dalam perspektif perlindungan konsumen, pengguna e-wallet merupakan konsumen jasa. Pengguna berhak memperoleh keamanan, kenyamanan, informasi yang benar, layanan pengaduan yang layak, serta ganti rugi apabila mengalami kerugian akibat layanan. Sebaliknya, penyelenggara e-wallet berkewajiban beritikad baik, menyediakan layanan yang aman, menjelaskan risiko secara jujur, tidak mencantumkan klausul baku yang menghilangkan tanggung jawab, serta menyediakan mekanisme pemulihan yang mudah diakses.

Klausul bahwa penyelenggara hanya bertanggung jawab atas kerugian yang timbul karena kesalahan sistem, dan tidak bertanggung jawab atas kelalaian pengguna atau serangan pihak ketiga, perlu diuji secara ketat. Serangan pihak ketiga dalam layanan digital tidak selalu dapat dipisahkan dari kewajiban penyelenggara untuk membangun sistem deteksi fraud. Apabila transaksi mencurigakan tetap lolos, autentikasi tidak memadai, pengaduan terlambat diproses, atau tidak ada pemberitahuan risiko yang memadai, maka serangan pihak ketiga tidak otomatis menghapus tanggung jawab penyelenggara.

3.3. Konstruksi Presumption of Liability dalam Kasus Hilangnya Saldo

Dalam perkara kehilangan saldo e-wallet, posisi hukum yang paling proporsional adalah *presumption of liability*. Prinsip ini menempatkan penyelenggara sebagai pihak yang diasumsikan bertanggung jawab sampai ia dapat menunjukkan bukti teknis yang memadai bahwa transaksi dilakukan secara sah oleh pengguna dan tidak terdapat kelemahan sistem. Konstruksi ini selaras dengan karakter hubungan digital karena penyelenggara menguasai data log, waktu transaksi, perangkat yang digunakan, alamat IP, lokasi, jejak OTP, binding account, pola perilaku, dan parameter fraud detection.

Penerapan *presumption of liability* tidak mengabaikan kewajiban pengguna untuk menjaga PIN, OTP, perangkat, dan kerahasiaan akun. Namun, kewajiban tersebut tidak boleh dijadikan alasan umum untuk menolak semua klaim. Jika pengguna telah menggunakan fitur keamanan seperti PIN, OTP, atau biometrik, tetapi transaksi tetap terjadi tanpa persetujuannya, penyelenggara harus menjelaskan secara rinci bagaimana autentikasi berhasil dilalui, perangkat apa yang digunakan, apakah ada perubahan perangkat, apakah ada binding dengan merchant atau platform lain, dan mengapa sistem tidak mengidentifikasi transaksi sebagai transaksi berisiko.

Dalam skripsi sumber, salah satu pengguna bernama Novi mengalami kehilangan saldo Rp2.400.000 karena terdapat transaksi ke Bukalapak yang tidak dilakukan olehnya. Pengguna telah melaporkan kepada DANA Care, namun tanggapan akhir yang diterima hanya menyebutkan adanya aktivitas binding akun DANA dengan Bukalapak tanpa kejelasan mengenai pemulihan dana (Khoironnisa, 2024). Contoh ini menunjukkan masalah pembuktian. Jawaban seperti

“terdapat aktivitas binding” belum cukup untuk membebaskan penyelenggara dari tanggung jawab. Penyelenggara harus membuktikan apakah aktivitas binding tersebut sah, melalui perangkat pengguna, dengan autentikasi yang benar, tanpa anomali, dan setelah pemberitahuan risiko yang memadai.

UUPK memberikan dasar normatif untuk memperkuat argumentasi ini. Dalam gugatan ganti rugi konsumen, beban pembuktian mengenai ada atau tidaknya unsur kesalahan pada prinsipnya dapat dibebankan kepada pelaku usaha. Dalam layanan digital, penerapan pembalikan beban pembuktian menjadi semakin rasional karena data pembuktian berada pada penyelenggara. Oleh sebab itu, ketika konsumen mengajukan klaim kehilangan saldo dengan bukti awal berupa riwayat transaksi, tangkapan layar, notifikasi OTP yang tidak diminta, laporan pengaduan, atau keterangan rekening tujuan, penyelenggara wajib membuka ringkasan hasil investigasi yang dapat dipahami konsumen.

3.4. Hilangnya Saldo sebagai Peristiwa Perlindungan Data Pribadi

Hilangnya saldo e-wallet hampir selalu terkait dengan pemrosesan data pribadi. Akun e-wallet tidak hanya menyimpan saldo, tetapi juga mengolah data identitas, nomor ponsel, data perangkat, PIN, OTP, informasi biometrik, riwayat transaksi, rekening tujuan, data merchant, dan data perilaku pengguna. UU PDP menegaskan bahwa perlindungan data pribadi adalah keseluruhan upaya melindungi data pribadi dalam rangkaian pemrosesan data guna menjamin hak konstitusional subjek data pribadi (Republik Indonesia, 2022). Dengan demikian, kegagalan pengamanan akun tidak cukup dianalisis sebagai “saldo hilang”, tetapi harus dilihat pula sebagai kemungkinan kegagalan pengendalian data pribadi.

Dalam kerangka UU PDP, penyelenggara e-wallet dapat diposisikan sebagai pengendali data pribadi karena menentukan tujuan dan melakukan kendali pemrosesan data. Kewajiban pengendali data mencakup pemrosesan yang sah, terbatas, transparan, akurat, aman, dan bertanggung jawab. Apabila data autentikasi atau data transaksi diproses secara tidak aman sehingga memungkinkan pengambilalihan akun, maka kerugian finansial pengguna menjadi konsekuensi dari kegagalan perlindungan data.

Hal ini menjadi titik pembeda penting dari skripsi sumber. Skripsi telah membahas perlindungan data pribadi sebagai salah satu dasar hukum, tetapi artikel ini menempatkan data pribadi sebagai dasar konstruksi tanggung jawab. Jika penyelenggara menguasai data biometrik, perangkat, dan pola transaksi, maka ia tidak hanya berkewajiban menjaga kerahasiaan data, tetapi juga berkewajiban menggunakan data tersebut secara aktif untuk mencegah transaksi tidak sah. Data tidak boleh hanya menjadi alat verifikasi untuk kepentingan transaksi, tetapi juga harus menjadi alat perlindungan pengguna.

Dari sudut pandang hukum, kegagalan mencegah transaksi tidak sah dapat terjadi dalam tiga bentuk. Pertama, kegagalan preventif, yaitu lemahnya verifikasi login, OTP, atau perangkat baru. Kedua, kegagalan detektif, yaitu tidak berjalannya sistem pemantauan anomali transaksi. Ketiga, kegagalan korektif, yaitu lambatnya pembekuan akun, investigasi, dan pemulihan saldo setelah pengguna melapor. Ketiga bentuk kegagalan ini harus menjadi parameter tanggung jawab penyelenggara.

3.5. Peran Bank Indonesia, OJK, dan LAPS dalam Pengawasan dan Penyelesaian Sengketa

Bank Indonesia merupakan regulator utama sistem pembayaran. PBI 3/2023 tentang Perlindungan Konsumen Bank Indonesia mengatur prinsip perlindungan konsumen, hak dan kewajiban penyelenggara dan konsumen, penanganan pengaduan, pelaporan, pengawasan, dan koordinasi (Bank Indonesia, 2023). Ketentuan ini memperlihatkan bahwa perlindungan pengguna e-wallet adalah bagian dari stabilitas dan kepercayaan sistem pembayaran, bukan sekadar urusan layanan pelanggan.

OJK memiliki mandat perlindungan konsumen di sektor jasa keuangan dan mengatur prinsip, perilaku dasar pelaku usaha jasa keuangan, penyampaian informasi, layanan konsumen, pengaduan, penyelesaian sengketa, pengawasan perilaku pasar, pembinaan, dan sanksi melalui POJK 22/2023 (Otoritas Jasa Keuangan, 2023). Dalam konteks e-wallet, pembacaan kewenangan harus dilakukan hati-hati karena sistem pembayaran berada dalam pengaturan Bank Indonesia, tetapi praktik penyelesaian sengketa konsumen sektor keuangan dapat bersinggungan dengan mekanisme LAPS sektor keuangan dan prinsip perlindungan konsumen lintas otoritas.

Skripsi sumber telah menguraikan jalur penyelesaian internal, LAPS, dan litigasi. Artikel ini memperkuatnya dengan menekankan bahwa penyelesaian internal tidak boleh menjadi formalitas. Penyelenggara harus menyediakan nomor tiket laporan, membekukan transaksi berisiko, meminta bukti dari pengguna, melakukan audit digital, memberi ringkasan hasil investigasi, dan menyampaikan dasar penolakan atau pengembalian saldo secara tertulis. Jika penyelesaian internal tidak menghasilkan kesepakatan, pengguna harus diberi akses jelas menuju pengaduan regulator atau LAPS. PADG 18/2024 menegaskan bahwa penyelenggara wajib menangani pengaduan secara efektif, namun apabila tidak tercapai kesepakatan, diperlukan mekanisme penyelesaian sengketa melalui pengadilan atau di luar pengadilan (Bank Indonesia, 2024).

Tabel 2. Model tanggung jawab atas hilangnya saldo e-wallet

Tahap	Kewajiban Penyelenggara	Hak Pengguna	Akibat Hukum Jika Gagal
Pencegahan	Autentikasi berlapis, deteksi anomali, pengamanan data, edukasi risiko.	Informasi keamanan yang jelas dan akses pengaturan akun.	Kelalaian preventif dapat menjadi dasar tanggung jawab ganti rugi.
Laporan awal	Menerima pengaduan, memberi nomor tiket, membekukan akun/transaksi berisiko.	Menyampaikan bukti awal dan memperoleh tanggapan cepat.	Keterlambatan memperbesar kerugian dan dapat memperkuat klaim konsumen.
Investigasi	Membuka audit trail terbatas: perangkat, waktu, IP/lokasi, OTP, merchant, dan pola transaksi.	Memperoleh penjelasan yang dapat dipahami.	Penolakan tanpa bukti teknis tidak cukup untuk membebaskan tanggung jawab.
Pemulihan	Mengembalikan saldo jika tidak dapat membuktikan transaksi sah atau keamanan sistem memadai.	Ganti rugi proporsional dan perbaikan akun.	Dapat diajukan ke regulator, LAPS, atau pengadilan.

3.6. Model Pemulihan Berbasis Audit Digital dan Pembalikan Beban Pembuktian

Model perlindungan yang ditawarkan artikel ini terdiri atas lima tahap. Tahap pertama adalah early warning dan preventive control. Penyelenggara harus mengirim pemberitahuan real-time ketika terjadi login dari perangkat baru, binding akun dengan merchant, perubahan nomor ponsel, transaksi besar, atau pola transaksi yang tidak biasa. Tahap kedua adalah emergency response. Ketika pengguna melapor kehilangan saldo, penyelenggara wajib memberi opsi pembekuan sementara akun dan membatasi transaksi lanjutan agar kerugian tidak meluas.

Tahap ketiga adalah digital audit. Investigasi tidak cukup hanya menyatakan transaksi berhasil. Penyelenggara perlu memberikan ringkasan log yang dapat dipahami pengguna, tanpa membuka rahasia sistem yang dapat disalahgunakan. Ringkasan tersebut paling tidak memuat waktu transaksi, jenis transaksi, perangkat, status autentikasi, tujuan transaksi, apakah ada perubahan perangkat, dan alasan sistem tidak mengategorikan transaksi sebagai fraud. Tahap keempat adalah provisional recovery. Dalam kasus ketika bukti awal menunjukkan transaksi tidak dikenal dan penyelenggara belum dapat membuktikan keabsahan transaksi, perlu dipertimbangkan pemulihan saldo sementara sampai investigasi selesai. Tahap kelima adalah

external review, yaitu pengujian oleh regulator, LAPS, atau pengadilan jika hasil investigasi internal tidak diterima pengguna.

Model ini lebih kuat dibandingkan pendekatan skripsi yang cenderung menyarankan perbaikan keamanan dan respons layanan. Penguatan keamanan memang penting, tetapi perlindungan hukum membutuhkan standar pemulihan. Tanpa standar pembuktian dan ganti rugi, pengguna tetap berada pada posisi lemah meskipun ada banyak kanal pengaduan. Dengan presumption of liability, penyelenggara didorong untuk membangun sistem yang benar-benar aman karena risiko hukum tidak dapat dialihkan begitu saja kepada konsumen.

Konstruksi ini juga menjaga keseimbangan. Pengguna tetap berkewajiban menjaga OTP, PIN, dan perangkat. Akan tetapi, apabila penyelenggara tidak mampu membuktikan bahwa transaksi dilakukan dengan autentikasi yang sah dan tanpa anomali, maka risiko kerugian harus lebih banyak ditanggung penyelenggara sebagai pihak profesional. Prinsip ini sejalan dengan logika perlindungan konsumen: pihak yang menguasai teknologi, menentukan standar layanan, dan memperoleh keuntungan dari transaksi digital harus menanggung tanggung jawab lebih besar atas risiko sistemiknya.

Khusus untuk DANA, status sebagai PJP kategori I menunjukkan bahwa layanan yang diberikan bukan hanya dompet elektronik, tetapi juga inisiasi transaksi, acquiring, payment gateway, penerbitan akun pembayaran, dan transfer dana. Semakin luas cakupan layanan, semakin besar pula ekspektasi hukum terhadap tata kelola risiko, perlindungan konsumen, dan integritas data. Karena itu, penguatan sistem keamanan harus dibaca sebagai kewajiban hukum, bukan sekadar fitur bisnis.

3.7. Pengujian Klausul Baku dan Batas Pembebasan Tanggung Jawab

Klausul baku merupakan titik rawan dalam layanan e-wallet karena pengguna biasanya hanya diberi pilihan untuk menyetujui syarat dan ketentuan yang telah disiapkan sepihak. Dalam relasi seperti ini, persetujuan pengguna tidak selalu menggambarkan posisi tawar yang seimbang. Konsumen membutuhkan aplikasi untuk transaksi sehari-hari, sedangkan penyelenggara menentukan hampir seluruh isi perjanjian elektronik, termasuk batas tanggung jawab, cara pengaduan, penggunaan data, dan pembatasan ganti rugi.

Menurut UUPK, klausul baku yang mengalihkan tanggung jawab pelaku usaha atau meniadakan hak konsumen untuk memperoleh ganti rugi patut diuji keabsahannya. Dalam konteks e-wallet, klausul yang menyatakan bahwa penyelenggara tidak bertanggung jawab atas seluruh kerugian yang timbul akibat peretasan pihak ketiga harus dibaca secara terbatas. Peretasan pihak ketiga tidak selalu berada di luar kendali penyelenggara, terutama apabila serangan tersebut berhasil karena lemahnya autentikasi, tidak adanya deteksi transaksi tidak wajar, atau terlambatnya pembekuan akun setelah pengguna mengadukan transaksi yang tidak diakui.

Analisis ini penting karena banyak sengketa e-wallet berhenti pada jawaban layanan pelanggan yang menyatakan transaksi telah berhasil diproses. Padahal, keberhasilan pemrosesan transaksi secara teknis tidak sama dengan keabsahan transaksi secara hukum. Transaksi baru dapat dipandang sah apabila dilakukan oleh pemilik akun atau pihak yang berwenang, menggunakan autentikasi yang benar, dan tidak lahir dari manipulasi, pengambilalihan akun, atau kegagalan sistem. Oleh karena itu, dalam sengketa kehilangan saldo, penyelenggara harus membuktikan tidak hanya bahwa transaksi tercatat, tetapi juga bahwa transaksi tersebut lahir dari persetujuan pengguna yang valid.

Klausul pembebasan tanggung jawab juga tidak boleh menghalangi hak konsumen untuk mengajukan pengaduan, meminta audit transaksi, memperoleh penjelasan yang jelas, dan menuntut ganti rugi. Jika syarat dan ketentuan aplikasi menempatkan seluruh risiko digital pada konsumen, maka klausul tersebut tidak sejalan dengan prinsip keseimbangan, keadilan,

dan kepastian hukum. Relasi digital yang sehat justru membutuhkan pembagian risiko yang proporsional antara konsumen dan penyelenggara.

3.8. Standar Pembuktian Transaksi Tidak Sah

Agar perlindungan hukum tidak berhenti pada slogan, perlu dirumuskan standar pembuktian transaksi tidak sah. Artikel ini menawarkan empat indikator minimum. Pertama, indikator identitas, yaitu apakah transaksi dilakukan melalui perangkat, nomor ponsel, atau akun yang biasa digunakan pengguna. Kedua, indikator autentikasi, yaitu apakah PIN, OTP, biometrik, atau metode verifikasi lain digunakan secara wajar dan tidak didahului aktivitas mencurigakan. Ketiga, indikator perilaku, yaitu apakah transaksi sesuai dengan pola kebiasaan pengguna, baik dari sisi nominal, waktu, merchant, maupun tujuan transfer. Keempat, indikator respons, yaitu apakah penyelenggara melakukan notifikasi, pemblokiran, dan investigasi secara cepat setelah terdeteksi anomali atau setelah pengguna melapor.

Keempat indikator tersebut dapat digunakan sebagai dasar bagi regulator dan LAPS untuk menilai kewajaran penolakan klaim. Apabila penyelenggara hanya menyatakan bahwa transaksi sukses tanpa membuka analisis empat indikator tersebut, maka penolakan klaim tidak dapat dikatakan memadai. Penyelenggara harus menunjukkan bahwa sistemnya telah bekerja secara wajar dan pengguna memang melakukan atau menyetujui transaksi. Sebaliknya, apabila terdapat perangkat baru, transaksi tidak lazim, perubahan binding account, OTP yang tidak diminta, atau keterlambatan respons pengaduan, maka asumsi tanggung jawab penyelenggara menjadi semakin kuat.

Standar pembuktian ini juga dapat mencegah moral hazard dari dua arah. Di satu sisi, konsumen tidak dapat sembarangan mengklaim saldo hilang tanpa bukti awal. Di sisi lain, penyelenggara tidak dapat berlindung di balik kompleksitas teknologi. Bukti awal konsumen dapat berupa tangkapan layar riwayat transaksi, notifikasi OTP, laporan pengaduan, bukti komunikasi dengan layanan pelanggan, mutasi rekening, dan keterangan perangkat. Setelah bukti awal diberikan, penyelenggara wajib merespons dengan audit trail terbatas yang objektif.

Dalam praktik, audit trail tidak harus membuka seluruh rahasia keamanan sistem. Penyelenggara cukup memberikan informasi yang relevan dan aman, misalnya waktu transaksi, jenis perangkat, perubahan perangkat, merchant atau rekening tujuan, status autentikasi, serta apakah sistem mencatat anomali. Dengan cara ini, kepentingan keamanan sistem tetap terlindungi, tetapi hak pengguna atas penjelasan dan pemulihan juga terpenuhi.

Tabel 3. Indikator penilaian transaksi tidak sah

Indikator	Pertanyaan Uji	Relevansi Hukum
Identitas perangkat	Apakah transaksi berasal dari perangkat yang biasa digunakan atau perangkat baru?	Menilai kemungkinan pengambilalihan akun dan kewajiban notifikasi perangkat baru.
Autentikasi	Apakah PIN/OTP/biometrik digunakan secara wajar dan tidak didahului anomali?	Menentukan validitas persetujuan transaksi dan kecukupan keamanan.
Perilaku transaksi	Apakah nominal, waktu, merchant, atau tujuan transfer berbeda dari pola normal?	Menilai kelalaian sistem fraud detection.
Respons pengaduan	Apakah akun dibekukan dan investigasi dilakukan segera setelah laporan?	Menilai tanggung jawab korektif dan perluasan kerugian.

3.9. Implikasi De Lege Ferenda bagi Regulasi E-Wallet

Dari sudut pandang de lege ferenda, diperlukan pengaturan yang lebih eksplisit mengenai pemulihan saldo dalam kasus transaksi tidak sah. Regulasi saat ini telah memuat prinsip perlindungan konsumen, pengaduan, pengawasan, dan kewajiban tata kelola risiko. Namun, pengguna masih membutuhkan standar operasional yang lebih konkret, terutama mengenai

batas waktu pembekuan akun, bentuk ringkasan hasil investigasi, kondisi pemberian pengembalian saldo sementara, dan standar minimum kompensasi apabila keterlambatan penanganan memperbesar kerugian.

Bank Indonesia dapat mengembangkan pedoman teknis khusus untuk sengketa unauthorized transaction pada dompet elektronik. Pedoman tersebut dapat berisi kewajiban penyelenggara untuk menyediakan tombol darurat pemblokiran akun, memberikan nomor tiket otomatis, menunda atau membekukan transaksi yang mencurigakan, menyampaikan hasil investigasi dalam bahasa sederhana, serta menyediakan jalur eskalasi langsung kepada regulator apabila penyelesaian internal tidak jelas. Pedoman ini juga perlu menetapkan larangan klausul baku yang secara mutlak mengalihkan seluruh risiko keamanan kepada konsumen.

Selain itu, perlu ada koordinasi yang lebih kuat antara Bank Indonesia, Kementerian Komunikasi dan Digital, BSSN, OJK, kepolisian siber, dan LAPS. Kehilangan saldo e-wallet sering kali merupakan gabungan antara masalah sistem pembayaran, perlindungan data, penipuan elektronik, dan perlindungan konsumen. Koordinasi lintas lembaga diperlukan agar pengaduan pengguna tidak terfragmentasi. Pengguna tidak boleh dibebani untuk menentukan sendiri apakah kasusnya harus dilaporkan ke penyelenggara, regulator sistem pembayaran, otoritas data pribadi, kepolisian, atau lembaga sengketa. Sistem pengaduan terpadu akan meningkatkan efektivitas pemulihan.

Pada akhirnya, kepercayaan publik terhadap pembayaran digital bergantung pada kemampuan hukum memberi kepastian pemulihan. Inovasi pembayaran akan berjalan sehat apabila konsumen yakin bahwa saldo mereka tidak hanya mudah digunakan, tetapi juga mudah dilindungi dan dipulihkan ketika terjadi gangguan. Karena itu, tanggung jawab penyelenggara e-wallet harus dipahami sebagai tanggung jawab profesional atas risiko teknologi yang diciptakan dan dikendalikan oleh penyelenggara sendiri.

4. SIMPULAN DAN SARAN

Perlindungan pengguna e-wallet atas hilangnya saldo pada aplikasi DANA harus dipahami sebagai masalah hukum berlapis yang mencakup perlindungan konsumen, keamanan sistem pembayaran, perlindungan data pribadi, dan penyelesaian sengketa digital. Skripsi sumber telah membuktikan adanya keluhan pengguna, celah respons layanan, serta kebutuhan perbaikan keamanan dan pengembalian saldo. Artikel ini memperkuat analisis dengan menawarkan konstruksi presumption of liability, yaitu penyelenggara e-wallet harus terlebih dahulu membuktikan bahwa transaksi yang dipersoalkan sah, sistemnya aman, dan kerugian tidak timbul akibat kegagalan layanan atau kegagalan pengamanan data. Konstruksi ini penting karena konsumen tidak menguasai log teknis dan berada dalam posisi lemah secara informasi.

Penyelenggara e-wallet tidak cukup hanya menyediakan kanal pengaduan. Perlindungan yang efektif menuntut pembekuan cepat terhadap akun atau transaksi berisiko, audit digital yang transparan, penjelasan hasil investigasi yang dapat dipahami, pemulihan saldo yang proporsional, dan akses pengaduan eksternal apabila penyelesaian internal gagal. Bank Indonesia perlu memperkuat pengawasan perilaku pasar dan standar penanganan kehilangan saldo, sedangkan OJK dan LAPS dapat memperkuat akses penyelesaian sengketa konsumen sektor keuangan. Bagi penyelenggara, rekomendasi utama artikel ini adalah membangun standar pemulihan yang jelas, tidak menyandarkan penolakan klaim pada klausul baku semata, dan menerapkan pembalikan beban pembuktian secara adil. Bagi pengguna, kewajiban menjaga PIN, OTP, perangkat, dan bukti transaksi tetap penting, tetapi kewajiban tersebut tidak boleh menghapus tanggung jawab profesional penyelenggara atas keamanan sistem pembayaran digital.

5. UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada para pihak yang telah memberikan dukungan akademik dalam penyusunan artikel ini. Artikel ini dikembangkan dari skripsi yang membahas perlindungan pengguna e-wallet atas hilangnya saldo pada aplikasi DANA, dengan penguatan analisis hukum agar memiliki kebaruan akademik dan kontribusi normatif bagi pengembangan perlindungan konsumen digital.

6. DAFTAR RUJUKAN

- Bank Indonesia. (2023). Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Perlindungan Konsumen Bank Indonesia. Bank Indonesia.
- Bank Indonesia. (2024). Peraturan Anggota Dewan Gubernur Nomor 18 Tahun 2024 tentang Peraturan Pelaksanaan Lembaga Alternatif Penyelesaian Sengketa di Sektor Keuangan. Bank Indonesia.
- Bank Indonesia. (2025). Peraturan Bank Indonesia Nomor 10 Tahun 2025 tentang Pengaturan Industri Sistem Pembayaran. Bank Indonesia.
- Candrawati, N. N. A. (2014). Perlindungan hukum terhadap pemegang kartu e-money sebagai alat pembayaran dalam transaksi komersial. *Jurnal Magister Hukum Udayana*, 3(1), 1-18.
- DANA. (2026). PT Espay Debit Indonesia Koe. <https://www.dana.id/corporate/biz-group>
- Khoironnisa. (2024). Perlindungan terhadap pengguna e-wallet atas hilangnya saldo pada aplikasi DANA dalam sistem pembayaran digital. Skripsi, UIN Syarif Hidayatullah Jakarta.
- Latumahina, R. E. (2014). Aspek hukum perlindungan data pribadi di dunia maya. *Jurnal Gema Aktualita*, 2(3), 14-25.
- Otoritas Jasa Keuangan. (2023). POJK Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Otoritas Jasa Keuangan.
- Rahmatullah, I. (2021). *Pentingnya perlindungan data pribadi dalam masa pandemi*. Adalah: Buletin Hukum dan Keadilan, 5(1), 11-16.
- Republik Indonesia. (1999). Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
- 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.
- Soekanto, S. (2014). *Faktor-faktor yang mempengaruhi penegakan hukum*. RajaGrafindo Persada.
- Susanti, N. L. P. R., & Putra, I. M. P. D. (2023). Pengaruh persepsi kemudahan, kualitas layanan, dan risiko keamanan terhadap keputusan pengguna e-wallet dalam transaksi keuangan. *E-Jurnal Ekonomi dan Bisnis Universitas Udayana*, 12(3), 407-418.
- Widijantoro, J., et al. (2019). *Hukum perlindungan konsumen jasa keuangan di era Otoritas Jasa Keuangan*. Cahaya Atma Pustaka.