

PERLINDUNGAN HUKUM KONSUMEN ATAS PENYALAHGUNAAN AKUN OLEH HACKER DALAM TRANSAKSI DOMPET DIGITAL

Guska Maulinda; Indah Maulani, S.H., M.H.

Program Studi Ilmu Hukum, Fakultas Hukum dan Ilmu Politik, Universitas Muhammadiyah Surakarta

Abstrak

Penelitian ini mengkaji perlindungan hukum konsumen atas penyalahgunaan akun oleh hacker dalam transaksi dompet digital, dengan fokus pada pengaturan hukum perlindungan konsumen serta bentuk tanggung jawab hukum penyelenggara dompet digital terhadap kerugian akibat penyalahgunaan akun oleh pihak ketiga. Isu ini penting mengingat penggunaan dompet digital terus meningkat, sementara risiko phishing, peretasan, account takeover, dan transaksi tidak sah masih menimbulkan kerugian finansial serta ketidakpastian pemulihan hak konsumen. Penelitian ini menggunakan metode penelitian hukum normatif yang bersifat deskriptif-analitis, dengan pendekatan perundang-undangan, konseptual, dan kasus. Bahan hukum primer, sekunder, dan tersier diperoleh melalui studi kepustakaan dan dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa perlindungan konsumen dalam transaksi dompet digital telah diatur melalui Undang-Undang Perlindungan Konsumen, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, serta peraturan sektor sistem pembayaran. Namun, pengaturan tersebut masih bersifat umum dan belum sepenuhnya memberikan batas tanggung jawab yang tegas ketika kerugian terjadi akibat penyalahgunaan akun oleh hacker. Penyelenggara tetap berkewajiban menyediakan sistem yang aman, menjaga data pribadi, menindaklanjuti pengaduan, melakukan investigasi, dan memberikan mekanisme penyelesaian serta ganti kerugian apabila kerugian terbukti terjadi karena kelemahan sistem atau kelalaian penyelenggara. Oleh karena itu, diperlukan penguatan regulasi, peningkatan standar keamanan, dan mekanisme pengaduan yang lebih transparan agar perlindungan hukum konsumen dapat berjalan efektif.

Kata Kunci: dompet digital, hacker, perlindungan konsumen, tanggung jawab hukum.

Abstract

This study examines consumer legal protection against account misuse by hackers in digital wallet transactions, focusing on the legal framework governing consumer protection and the legal liability of digital wallet providers for losses arising from misuse by third parties. The issue is significant because the use of digital wallets continues to increase, while phishing, hacking, account takeover, and unauthorized transactions still cause financial losses and uncertainty in the recovery of consumer rights. This study applies a normative legal method with a descriptive-analytical character, using statutory, conceptual, and case approaches. Primary, secondary, and tertiary legal materials were obtained through library research and analyzed qualitatively. The findings show that consumer protection in digital wallet transactions is regulated under the Consumer Protection Law, the Electronic Information and Transactions Law, the Personal Data Protection Law, and payment-system regulations. Nevertheless, these rules remain general and have not fully established clear limits of liability when losses arise from account misuse by hackers. Digital wallet providers remain legally obliged to maintain a secure system, protect personal data, follow up complaints, conduct investigations, and provide dispute-resolution and compensation mechanisms when losses are proven to result from system weaknesses or provider negligence. Stronger regulation, improved security standards, and more transparent complaint mechanisms are therefore required to

ensure effective consumer protection.

Keywords: consumer protection, digital wallet, hacker, legal liability.

1. PENDAHULUAN

Perkembangan teknologi digital di Indonesia telah membawa perubahan signifikan dalam kehidupan ekonomi dan sosial. Peningkatan penggunaan internet serta perangkat digital mempermudah masyarakat melakukan transaksi dan mengakses layanan keuangan. Dompot digital (e-wallet) menjadi salah satu instrumen pembayaran yang paling dekat dengan aktivitas sehari-hari karena menawarkan proses pembayaran yang cepat, praktis, dan efisien. Perubahan tersebut mencerminkan pergeseran menuju cashless society, yaitu masyarakat semakin terbiasa melakukan transaksi secara non-tunai melalui aplikasi digital (Aulia, 2020).

Perkembangan layanan keuangan digital juga diikuti peningkatan risiko kejahatan siber. Data yang dikemukakan dalam skripsi menunjukkan bahwa Indonesia Anti-Scam Centre mencatat 166.258 laporan penipuan sejak 22 November 2024 sampai 30 Juni 2025, dengan kerugian mencapai Rp3,4 triliun dan dana yang berhasil diblokir sebesar Rp558,7 miliar. Angka tersebut memperlihatkan bahwa kejahatan digital tidak hanya menasar layanan perbankan, tetapi juga dompet digital dan berbagai instrumen keuangan berbasis elektronik.

Dompot digital memungkinkan pengguna menyimpan data instrumen pembayaran dan dana elektronik untuk keperluan transfer, pembayaran tagihan, pembelian barang, transportasi, maupun transaksi daring lainnya. Di balik kemudahan tersebut terdapat risiko keamanan yang berkaitan dengan data pribadi dan akses terhadap akun. Modus yang umum terjadi antara lain phishing, social engineering, peretasan, pengambilalihan akun atau account takeover (ATO), penggunaan kode OTP tanpa hak, serta transaksi yang tidak dikenali oleh pemilik akun.

Pelaku kejahatan pada umumnya memanfaatkan kelemahan pengetahuan pengguna, menyamar sebagai pihak resmi, atau menggunakan tautan dan komunikasi palsu untuk memperoleh username, kata sandi, PIN, serta kode OTP. Dalam kasus lain, ancaman juga dapat berasal dari kelemahan sistem maupun penyalahgunaan akses oleh pihak internal. Keadaan ini menyebabkan perlindungan konsumen dalam layanan dompet digital tidak hanya berkaitan dengan keamanan saldo, tetapi juga mencakup keamanan sistem elektronik, kerahasiaan data pribadi, transparansi informasi, dan efektivitas mekanisme pengaduan.

Permasalahan yang muncul tidak berhenti pada kerugian finansial. Konsumen yang menjadi korban sering mengalami kesulitan memperoleh penjelasan mengenai penyebab transaksi, hasil investigasi, dan kepastian pengembalian saldo. Penyelenggara pada sisi lain dapat menyatakan bahwa kerugian timbul karena kelalaian pengguna dalam menjaga data pribadi. Perbedaan posisi tersebut

menunjukkan adanya persoalan mengenai pembagian beban tanggung jawab antara pengguna dan penyelenggara ketika penyalahgunaan akun dilakukan oleh pihak ketiga.

Secara normatif, perlindungan konsumen telah diatur melalui Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Undang-undang tersebut menjamin hak konsumen atas kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan/atau jasa, serta hak untuk memperoleh kompensasi atau ganti kerugian apabila layanan yang diterima tidak sesuai dengan perjanjian atau menimbulkan kerugian. Dalam konteks dompet digital, penyelenggara berkedudukan sebagai pelaku usaha yang wajib memberikan informasi yang benar, menjaga mutu dan keamanan layanan, serta bertanggung jawab terhadap kerugian yang timbul karena kesalahan atau kelalaiannya.

Perlindungan juga diberikan melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya. Penyelenggara sistem elektronik diwajibkan menyelenggarakan sistem secara andal, aman, dan bertanggung jawab. Penggunaan data pribadi dalam media elektronik juga harus didasarkan pada persetujuan pemilik data. Ketentuan tersebut diperkuat oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang mewajibkan pengendali data menjaga kerahasiaan dan keamanan data serta mencegah akses dan penggunaan tanpa hak.

Penyelenggaraan dompet digital sebagai bagian dari sistem pembayaran berada dalam kewenangan Bank Indonesia. Pengaturan mencakup perizinan, tata kelola, manajemen risiko, keamanan sistem, dan perlindungan konsumen. Meskipun telah tersedia beberapa lapis regulasi, ketentuan yang ada belum secara khusus menguraikan batas tanggung jawab penyelenggara apabila kerugian terjadi akibat account takeover, peretasan, phishing, atau transaksi tidak sah oleh pihak ketiga. Akibatnya, mekanisme ganti rugi dan pembagian tanggung jawab belum selalu memberikan kepastian yang sama bagi setiap konsumen.

Kasus dugaan penyalahgunaan data pribadi pengguna oleh petugas OVO menunjukkan bahwa akses internal terhadap data dapat menimbulkan pelanggaran privasi. Sementara itu, kasus kehilangan saldo pada aplikasi DANA akibat transaksi tidak dikenal menunjukkan persoalan lain, yaitu efektivitas fitur keamanan, transparansi investigasi, serta kepastian pemulihan dana. Kedua kasus tersebut memperlihatkan bahwa perlindungan preventif dan represif harus berjalan bersama: pencegahan melalui sistem dan pengawasan yang kuat harus diikuti penanganan pengaduan, investigasi, pemulihan, dan penegakan tanggung jawab ketika pelanggaran telah terjadi.

Berdasarkan permasalahan tersebut, penelitian ini membahas dua persoalan utama. Pertama, bagaimana pengaturan hukum mengenai perlindungan konsumen dalam transaksi dompet digital. Kedua, bagaimana bentuk tanggung jawab hukum penyelenggara dompet digital terhadap kerugian

konsumen akibat penyalahgunaan akun oleh hacker. Analisis diarahkan untuk menilai kecukupan perlindungan hukum preventif maupun represif dan menemukan bagian pengaturan yang masih memerlukan penguatan

2. METODE (STYLE HEADING)

Penelitian ini merupakan penelitian hukum normatif yang bersifat deskriptif-analitis. Penelitian hukum normatif berfokus pada pengkajian norma hukum dalam peraturan perundang-undangan, doktrin, serta bahan hukum lain yang relevan dengan perlindungan konsumen dan transaksi dompet digital. Sifat deskriptif-analitis digunakan untuk memaparkan ketentuan yang berlaku sekaligus menganalisis kesesuaiannya dengan persoalan penyalahgunaan akun oleh pihak ketiga.

Pendekatan penelitian meliputi pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Pendekatan perundang-undangan digunakan untuk menelaah Undang-Undang Perlindungan Konsumen, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Pelindungan Data Pribadi, serta peraturan Bank Indonesia di bidang sistem pembayaran. Pendekatan konseptual digunakan untuk mengkaji perlindungan hukum, tanggung jawab hukum, dan kepastian hukum. Pendekatan kasus digunakan untuk menganalisis dugaan penyalahgunaan data pribadi pengguna OVO dan kehilangan saldo pengguna DANA akibat account takeover, peretasan, atau transaksi tidak sah.

Bahan penelitian terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer berupa peraturan perundang-undangan yang mengikat. Bahan hukum sekunder meliputi buku, jurnal ilmiah, hasil penelitian, dan pemberitaan yang relevan dengan kasus. Bahan hukum tersier digunakan untuk menjelaskan istilah serta konsep yang digunakan. Seluruh bahan dikumpulkan melalui studi kepustakaan, kemudian dianalisis secara kualitatif dengan cara menguraikan, menafsirkan, dan menghubungkan norma hukum dengan fakta kasus untuk memperoleh argumentasi hukum yang menjawab rumusan masalah

3. HASIL DAN PEMBAHASAN (STYLE HEADING)

3.1 Pengaturan Hukum Perlindungan Konsumen dalam Transaksi Dompet Digital

3.1.1 Kedudukan Dompet Digital dalam Sistem Pembayaran

Dompet digital merupakan instrumen sistem pembayaran elektronik yang menyimpan data instrumen pembayaran dan dana elektronik untuk melakukan transaksi secara digital. Dalam sistem hukum Indonesia, penyelenggaraan dompet digital berada di bawah kewenangan Bank Indonesia sebagai otoritas yang mengatur dan menjaga kelancaran sistem pembayaran nasional. Kedudukan tersebut berbeda dengan perbankan, perusahaan pembiayaan, asuransi, dan lembaga jasa keuangan

lain yang secara umum berada dalam lingkup pengawasan Otoritas Jasa Keuangan.

Kewenangan Bank Indonesia didasarkan pada Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia sebagaimana telah beberapa kali diubah, terakhir melalui Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan. Bank Indonesia berwenang menetapkan dan melaksanakan kebijakan sistem pembayaran, mengatur instrumen pembayaran, serta memastikan keamanan, efisiensi, dan keandalan penyelenggaraan sistem pembayaran. Dengan demikian, penyelenggara dompet digital wajib memperoleh izin dan menjalankan kegiatan sesuai ketentuan yang ditetapkan oleh Bank Indonesia.

Pengaturan lebih spesifik terdapat dalam Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran beserta peraturan pelaksanaannya. Regulasi tersebut mencakup perizinan, tata kelola, manajemen risiko, keamanan sistem, perlindungan konsumen, dan pengawasan terhadap penyelenggara. Tujuannya adalah membentuk sistem pembayaran yang aman, efisien, andal, dan mampu melindungi kepentingan masyarakat sebagai pengguna layanan digital.

Dompot digital ditempatkan sebagai instrumen pembayaran, bukan lembaga penghimpun dana atau lembaga intermediasi seperti bank. Oleh karena itu, pengaturan diarahkan pada keamanan transaksi, perlindungan data pengguna, manajemen risiko operasional, dan stabilitas sistem pembayaran. Penyelenggara wajib menerapkan prinsip kehati-hatian, menyediakan mekanisme penanganan pengaduan, dan melakukan mitigasi terhadap phishing, account takeover, social engineering, serta akses tidak sah. Pengaturan tersebut merupakan bentuk perlindungan hukum preventif karena bertujuan mencegah kerugian sebelum pelanggaran terjadi.

3.1.2 Perlindungan Konsumen, Sistem Elektronik, dan Data Pribadi

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menjadi dasar umum hubungan hukum antara pengguna dan penyelenggara. Konsumen berhak memperoleh kenyamanan, keamanan, keselamatan, informasi yang benar, serta ganti kerugian. Penyelenggara sebagai pelaku usaha berkewajiban beritikad baik, memberikan informasi yang jelas, menjamin mutu layanan, dan bertanggung jawab apabila kerugian timbul karena layanan yang tidak sesuai atau karena kelalaiannya.

Undang-Undang Informasi dan Transaksi Elektronik memberikan dasar kewajiban keamanan sistem. Penyelenggara sistem elektronik harus menyelenggarakan sistem secara andal, aman, dan bertanggung jawab. Ketentuan mengenai data pribadi juga mensyaratkan persetujuan pemilik data terhadap penggunaan informasi yang berkaitan dengan dirinya. Dalam layanan dompet digital, kewajiban tersebut mencakup pengamanan akun, pencatatan transaksi yang akurat, autentikasi yang layak, penyimpanan data secara aman, dan pencegahan akses tanpa hak.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memperkuat kewajiban penyelenggara sebagai pengendali atau pemroses data. Data hanya boleh digunakan berdasarkan dasar pemrosesan yang sah dan sesuai tujuan pengumpulannya. Penyelenggara wajib menjaga kerahasiaan, membatasi akses, menerapkan pengamanan teknis dan organisasi, serta bertanggung jawab apabila terjadi pemrosesan tanpa hak. Dengan demikian, perlindungan konsumen dalam dompet digital mencakup harta berupa saldo elektronik dan hak privasi atas data identitas, nomor telepon, KTP, swafoto, data biometrik, serta riwayat transaksi.

Ketiga kelompok pengaturan tersebut membentuk perlindungan berlapis. Undang-Undang Perlindungan Konsumen mengatur hak dan kewajiban dalam hubungan pelaku usaha dengan konsumen. Undang-Undang Informasi dan Transaksi Elektronik menekankan keandalan sistem serta legalitas penggunaan data di ruang elektronik. Undang-Undang Pelindungan Data Pribadi mengatur tata kelola dan pertanggungjawaban pemrosesan data. Peraturan Bank Indonesia melengkapi seluruhnya melalui standar penyelenggaraan sistem pembayaran. Kendala utamanya adalah belum adanya ketentuan yang secara rinci membagi tanggung jawab dalam kasus penyalahgunaan akun oleh pihak ketiga.

3.1.3 Analisis Kasus Dugaan Penyalahgunaan Data Pribadi Pengguna OVO

Dalam kasus dugaan penyalahgunaan data pribadi pengguna OVO, subjek hukum terdiri atas pengguna sebagai konsumen, OVO sebagai penyelenggara layanan, dan oknum petugas yang diduga menggunakan akses data untuk kepentingan pribadi. Objek hukumnya adalah nomor telepon, foto KTP, swafoto dengan KTP, dan informasi identitas yang diserahkan ketika pengguna meningkatkan akun menjadi OVO Premier. Data tersebut merupakan bagian dari hak privasi pengguna dan hanya boleh diproses sesuai tujuan verifikasi.

Kasus bermula ketika seorang pengguna yang melakukan peningkatan akun diduga dihubungi secara pribadi oleh seseorang yang mengaku sebagai petugas OVO. Orang tersebut diketahui memiliki akses terhadap nomor telepon, foto KTP, dan swafoto pengguna. Peristiwa tersebut menimbulkan dugaan bahwa data digunakan di luar tujuan pengumpulan tanpa persetujuan pemiliknya. Tindakan semacam itu bertentangan dengan hak konsumen atas keamanan dan privasi serta prinsip pembatasan tujuan dalam perlindungan data pribadi.

Undang-Undang Perlindungan Konsumen mewajibkan pelaku usaha menjamin keamanan dalam penggunaan jasa. Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik mensyaratkan persetujuan pemilik data, sedangkan Undang-Undang Pelindungan Data Pribadi mewajibkan pengendali data menjaga kerahasiaan dan mencegah penyalahgunaan oleh pihak internal maupun eksternal. Kewajiban OVO karena itu tidak berhenti pada penyediaan aplikasi yang aman, tetapi juga

mencakup pembatasan akses pegawai, pencatatan aktivitas akses, audit internal, dan penindakan terhadap penyimpangan.

Setelah kasus menjadi perhatian publik, OVO melakukan investigasi internal. Menurut bahan kasus dalam skripsi, tindakan menghubungi pengguna untuk kepentingan pribadi dinyatakan sebagai pelanggaran terhadap kebijakan privasi perusahaan. OVO berkomunikasi dengan pengguna, menyampaikan permintaan maaf, dan memberhentikan petugas yang bersangkutan. Penyelesaian dilakukan melalui mekanisme internal tanpa informasi mengenai gugatan perdata atau proses litigasi. Tindakan perusahaan tersebut menunjukkan pelaksanaan tanggung jawab internal, tetapi kasus ini juga membuktikan bahwa kebijakan tertulis belum cukup tanpa pengawasan akses yang efektif. Perlindungan hukum yang memadai memerlukan pengendalian akses berdasarkan kebutuhan kerja, pemantauan penggunaan data, audit berkala, prosedur pelaporan insiden, dan sanksi tegas. Dengan demikian, penyalahgunaan data oleh pihak internal harus dipandang sebagai kegagalan tata kelola yang wajib dievaluasi, bukan hanya sebagai kesalahan individu.

3.1.4 Analisis Kasus Kehilangan Saldo Pengguna DANA

Dalam kasus kehilangan saldo DANA akibat account takeover, peretasan, atau transaksi tidak sah, subjek hukum terdiri atas pengguna sebagai konsumen dan PT Espay Debit Indonesia Koe sebagai penyelenggara. Objek hukumnya adalah saldo elektronik yang tersimpan dalam akun pengguna dan digunakan untuk transfer, pembayaran tagihan, pembelian pulsa, maupun transaksi daring. Hilangnya saldo melalui transaksi yang tidak dikenali menunjukkan adanya gangguan terhadap hak konsumen atas keamanan dana dan layanan.

Apabila kehilangan terjadi karena kelemahan sistem atau kelalaian penyelenggara, peristiwa tersebut bertentangan dengan Pasal 4 huruf a dan Pasal 7 Undang-Undang Perlindungan Konsumen. Kewajiban penyelenggaraan sistem yang andal dan aman juga diatur dalam Pasal 15 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik. Apabila account takeover berkaitan dengan lemahnya perlindungan data, Undang-Undang Pelindungan Data Pribadi juga relevan. Kewajiban manajemen risiko dan keamanan transaksi selanjutnya diperkuat melalui Peraturan Bank Indonesia Nomor 20/6/PBI/2018 dan Peraturan Bank Indonesia Nomor 18/40/PBI/2016.

Bahan penelitian menunjukkan beberapa pengguna mengalami kehilangan saldo setelah muncul transaksi yang tidak dikenal. Pengguna menyatakan tidak pernah memberikan OTP atau PIN kepada pihak lain, tetapi saldo tetap berkurang. Ketika laporan disampaikan kepada layanan pelanggan, jawaban yang diterima dinilai belum memberikan solusi konkret dan belum menjelaskan secara transparan dasar penentuan penyebab kerugian. Sebagian pengguna juga belum memperoleh kepastian mengenai pengembalian dana.

Permasalahan utama mencakup keamanan akun, proses penyelesaian yang lambat, ketidakjelasan hasil investigasi, dan belum pastinya penggantian kerugian. Kondisi tersebut menunjukkan adanya kesenjangan antara perlindungan normatif dan pelaksanaannya. Regulasi telah memberi hak kepada konsumen dan membebankan kewajiban keamanan kepada penyelenggara, tetapi efektivitas perlindungan bergantung pada kemampuan penyelenggara membuktikan penyebab transaksi, menjelaskan hasil pemeriksaan, dan memberikan pemulihan yang proporsional.

DANA telah menerapkan DANA Protection, verifikasi wajah atau DANA Viz, autentikasi biometrik, notifikasi aktivitas akun, dan sistem pemantauan transaksi mencurigakan. Penyelenggara juga membedakan kerugian karena kesalahan sistem internal dari kerugian akibat phishing, scam, atau malware pada perangkat pengguna. Pembedaan ini secara operasional diperlukan, tetapi tidak boleh digunakan sebagai penolakan otomatis. Setiap laporan harus diperiksa berdasarkan bukti teknis agar dapat ditentukan apakah kerugian timbul karena kelalaian pengguna, serangan pihak ketiga, atau kelemahan sistem.

3.2 Tanggung Jawab Hukum Penyelenggara Dompot Digital terhadap Konsumen

3.2.1 Tanggung Jawab Preventif

Tanggung jawab preventif merupakan kewajiban penyelenggara untuk mencegah kerugian sebelum terjadi. Bentuknya meliputi penerapan sistem autentikasi yang memadai, enkripsi dan pengamanan data, pembatasan akses internal, notifikasi aktivitas mencurigakan, pencatatan jejak akses, pemantauan transaksi, edukasi konsumen, dan pembaruan sistem secara berkala. Kewajiban tersebut merupakan perwujudan hak konsumen atas keamanan serta kewajiban penyelenggara sistem elektronik untuk menjalankan sistem secara andal dan bertanggung jawab.

Dalam kasus OVO, tanggung jawab preventif menuntut pengawasan terhadap pegawai yang memiliki akses terhadap data verifikasi. Pembatasan kewenangan harus disesuaikan dengan fungsi pekerjaan dan setiap penggunaan data harus dapat ditelusuri. Dalam kasus DANA, tanggung jawab preventif diwujudkan melalui fitur keamanan akun dan deteksi transaksi. Namun, keberadaan fitur tidak dengan sendirinya membuktikan bahwa seluruh kewajiban telah selesai. Efektivitas fitur harus diukur dari kemampuannya mencegah akses ilegal, mendeteksi anomali, dan melindungi saldo pengguna.

Penyelenggara juga wajib memberikan informasi yang mudah dipahami mengenai cara menjaga PIN, password, OTP, dan perangkat. Edukasi diperlukan karena banyak serangan memanfaatkan manipulasi psikologis pengguna. Meski demikian, tanggung jawab keamanan tidak dapat seluruhnya dialihkan kepada konsumen. Penyelenggara tetap memegang kendali atas infrastruktur, desain autentikasi, proses pemulihan akun, dan mekanisme validasi transaksi sehingga

mempunyai tanggung jawab lebih besar terhadap risiko yang berada dalam ruang kendalinya.

3.2.2 Penanganan Pengaduan, Investigasi, dan Pemulihan

Ketika insiden terjadi, tanggung jawab penyelenggara beralih pada perlindungan represif. Penyelenggara harus menerima pengaduan, mengamankan akun, menghentikan transaksi lanjutan, menjaga bukti elektronik, dan melakukan investigasi. Hasil investigasi harus disampaikan secara jelas agar konsumen memahami waktu, perangkat, metode autentikasi, dan jalur transaksi yang dipersoalkan. Transparansi tersebut penting untuk menentukan hubungan kausal antara kelemahan sistem, tindakan pihak ketiga, dan perilaku pengguna.

Dalam kasus OVO, perusahaan melakukan investigasi internal, berkomunikasi dengan pengguna, menyampaikan permintaan maaf, dan menjatuhkan pemutusan hubungan kerja kepada petugas. Langkah tersebut merupakan bentuk pemulihan non-finansial dan penegakan disiplin internal. Apabila penyalahgunaan menimbulkan kerugian yang dapat dinilai, konsumen tetap berhak menuntut pemulihan sesuai ketentuan hukum.

Dalam kasus DANA, pengaduan dapat disampaikan melalui DANA Care, live chat, email, atau call center. Setelah laporan diterima, penyelenggara melakukan investigasi terhadap transaksi. Apabila penyelesaian internal tidak mencapai kesepakatan, sengketa dapat dilanjutkan melalui lembaga alternatif penyelesaian sengketa, Badan Penyelesaian Sengketa Konsumen, atau pengadilan. Keberadaan jalur tersebut menunjukkan bahwa mekanisme penyelesaian tersedia secara normatif, tetapi pelaksanaannya harus cepat, transparan, dan dapat memberikan kepastian mengenai pengembalian saldo.

Ganti kerugian seharusnya diberikan apabila bukti menunjukkan kerugian timbul karena kelemahan sistem, kegagalan pengamanan, penyalahgunaan akses yang berada dalam tanggung jawab penyelenggara, atau kelalaian dalam penanganan insiden. Sebaliknya, apabila kerugian sepenuhnya terbukti timbul karena pengguna secara sadar menyerahkan kredensial kepada pelaku, pembagian tanggung jawab dapat berbeda. Penentuan tersebut harus didasarkan pada pemeriksaan objektif, bukan pada klausul baku yang langsung menyalahkan konsumen.

3.2.3 Sanksi dan Bentuk Pertanggungjawaban

Pelaku yang memperoleh, menggunakan, atau mengungkapkan data pribadi tanpa hak dapat dimintai pertanggungjawaban berdasarkan Undang-Undang Pelindungan Data Pribadi. Dalam bahan skripsi disebutkan ancaman pidana penjara paling lama lima tahun dan/atau denda paling banyak Rp5.000.000.000,00 untuk perbuatan tertentu yang dilakukan secara melawan hukum. Apabila perbuatan dilakukan melalui akses tanpa hak terhadap sistem elektronik, ketentuan pidana dalam

Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang Informasi dan Transaksi Elektronik dapat diterapkan sesuai unsur yang terpenuhi. Penyelenggara yang terbukti lalai dapat dikenai tanggung jawab perdata berupa ganti kerugian dan sanksi administratif. Sanksi administratif dapat berupa teguran tertulis, denda administratif, kewajiban memperbaiki sistem keamanan dan tata kelola, penghentian sementara pemrosesan data, pembatasan kegiatan usaha, hingga pencabutan izin apabila pelanggaran berat atau berulang. Tujuan sanksi tidak hanya menghukum, tetapi juga memulihkan hak konsumen dan mendorong perbaikan sistem.

Dalam kasus OVO, sanksi yang diketahui dalam bahan penelitian berupa pemutusan hubungan kerja terhadap petugas. Tindakan tersebut tidak menutup kemungkinan pertanggungjawaban lain apabila unsur pidana atau perdata terpenuhi. Dalam kasus DANA yang dianalisis, belum terdapat indikasi sanksi administratif atau hukum terhadap penyelenggara. DANA melakukan langkah perbaikan melalui peningkatan layanan pelanggan, penguatan keamanan biometrik, peningkatan transparansi investigasi, dan kerja sama dengan regulator.

Pertanggungjawaban penyelenggara dengan demikian dapat berbentuk tanggung jawab preventif, tanggung jawab kontraktual dan perdata, tanggung jawab administratif, serta tanggung jawab pidana apabila terpenuhi unsur tindak pidana. Bentuk yang diterapkan bergantung pada sumber kerugian, tingkat kesalahan, hubungan kausal, dan bukti yang tersedia. Penyelenggara tidak otomatis bertanggung jawab atas seluruh kejahatan pihak ketiga, tetapi juga tidak dapat melepaskan tanggung jawab hanya dengan menyatakan bahwa keamanan kredensial merupakan kewajiban pengguna.

3.2.4 Kepastian Batas Tanggung Jawab Penyelenggara

Berdasarkan teori perlindungan hukum Satjipto Rahardjo, unsur kepastian hukum telah tersedia karena terdapat Undang-Undang Perlindungan Konsumen, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, dan peraturan Bank Indonesia. Hak atas keamanan transaksi, perlindungan data pribadi, serta mekanisme pengaduan merupakan perlindungan preventif yang penting.

Meskipun demikian, perlindungan represif dan tanggung jawab penyelenggara belum sepenuhnya memberikan kepastian. Belum terdapat pengaturan yang secara khusus merinci batas tanggung jawab ketika kerugian terjadi akibat account takeover, peretasan, atau penyalahgunaan akun oleh pihak ketiga. Regulasi juga belum menjelaskan secara seragam standar pembuktian, waktu penyelesaian pengaduan, pembagian beban kerugian, dan kondisi yang mewajibkan pengembalian dana.

Kekosongan tersebut menempatkan konsumen dalam posisi yang lebih lemah karena penyelenggara menguasai data teknis dan hasil investigasi. Untuk mencapai perlindungan yang

seimbang, perlu ditetapkan kewajiban penyelenggara menyimpan serta membuka informasi transaksi yang relevan, batas waktu penyelesaian pengaduan, standar investigasi, dan mekanisme keberatan terhadap keputusan internal. Pengaturan juga perlu membedakan kerugian akibat kelalaian konsumen, kelemahan sistem, penyalahgunaan pihak internal, dan serangan pihak ketiga yang tidak dapat dicegah secara wajar. Dengan demikian, perlindungan hukum konsumen dalam dompet digital telah tersedia secara normatif, tetapi belum sepenuhnya memadai dari aspek pemulihan dan kepastian pertanggungjawaban. Penguatan regulasi perlu diarahkan pada mekanisme ganti rugi, pembagian tanggung jawab berbasis bukti, transparansi investigasi, dan pengawasan yang efektif. Pada saat yang sama, penyelenggara harus terus meningkatkan keamanan, sedangkan konsumen perlu menjaga kredensial dan meningkatkan literasi digital.

4. PENUTUP

4.1 Kesimpulan

Pengaturan perlindungan hukum konsumen dalam transaksi dompet digital telah dibentuk melalui Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta peraturan Bank Indonesia mengenai sistem pembayaran. Keseluruhan pengaturan tersebut memberikan dasar bagi hak konsumen atas keamanan, perlindungan data, informasi, pengaduan, dan ganti kerugian. Namun, ketentuannya masih bersifat umum dan belum merinci batas tanggung jawab penyelenggara ketika kerugian terjadi akibat account takeover, peretasan, atau transaksi tidak sah oleh pihak ketiga.

Penyelenggara dompet digital bertanggung jawab menyediakan sistem yang aman, menjaga kerahasiaan data, membatasi akses internal, melakukan mitigasi risiko, menerima dan menindaklanjuti pengaduan, melakukan investigasi, memberikan penjelasan yang transparan, serta menyediakan pemulihan atau ganti kerugian apabila kerugian terbukti disebabkan kelemahan sistem atau kelalaian penyelenggara. Analisis kasus OVO menunjukkan pentingnya pengawasan akses internal terhadap data pribadi, sedangkan kasus DANA menunjukkan perlunya kepastian hasil investigasi dan pengembalian saldo. Perlindungan preventif telah tersedia, tetapi perlindungan represif masih memerlukan penguatan agar konsumen memperoleh kepastian dan keadilan.

4.2 Saran

Pemerintah dan regulator perlu menyusun pengaturan yang lebih spesifik mengenai tanggung jawab penyelenggara dompet digital dalam kasus penyalahgunaan akun, termasuk standar investigasi, batas waktu penyelesaian pengaduan, pembagian beban pembuktian, dan mekanisme ganti rugi. Pengawasan terhadap keamanan sistem elektronik dan tata kelola data pribadi juga perlu ditingkatkan.

Penyelenggara dompet digital perlu memperkuat autentikasi, deteksi transaksi mencurigakan, pengawasan akses pegawai, audit keamanan, serta perlindungan data pengguna. Penanganan pengaduan harus lebih cepat, transparan, dan responsif. Hasil investigasi perlu disampaikan dalam bahasa yang mudah dipahami dan harus tersedia mekanisme keberatan apabila konsumen tidak menerima keputusan penyelenggara.

Konsumen perlu meningkatkan literasi digital dan kewaspadaan dengan menjaga PIN, kata sandi, OTP, data identitas, serta keamanan perangkat. Konsumen juga perlu menyimpan bukti transaksi dan segera melapor apabila menemukan aktivitas yang tidak dikenal agar pemblokiran, investigasi, dan pemulihan dapat dilakukan secepat mungkin.

DAFTAR PUSTAKA (styleHeading Daftar Pustaka)

- Aidil, Andi Muhammad, dan Muh Arya Darmawan. (2025). Analisis perlindungan hukum dalam transaksi transfer melalui aplikasi DANA, 2(2).
- Ananda Clarissa, Ika Dwi Maya Roza, Ashira Naila Susanti, Devi Riani, dan Muthia Salsabila. (2026). Efektivitas implementasi perlindungan hukum konsumen dalam transaksi digital pada marketplace di Indonesia. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, 3(1), 158–168.
- Andarningtyas, Natisha. (2020, 3 Juli). Petugas OVO diduga salahgunakan data pribadi pengguna. *Antara*.
- Atmaja, Yustisiana Susila, dan Darminto Hartono Paulus. (2022). Partisipasi Bank Indonesia dalam pengaturan digitalisasi sistem pembayaran Indonesia. *Masalah-Masalah Hukum*, 51(3), 271–286.
- Aulia, Sisca. (2020). Pola perilaku konsumen digital dalam memanfaatkan aplikasi dompet digital. *Jurnal Komunikasi*, 12(2), 311.
- Bodhi, Surya, dan David Tan. (2022). Keamanan data pribadi dalam sistem pembayaran e-wallet terhadap ancaman penipuan dan pengelabuan (cybercrime). *UNES Law Review*, 4(3), 297–308.
- Candra, Yesaya Michael. (2026). Pertanggungjawaban hukum penyelenggara e-wallet atas hilangnya saldo konsumen di Indonesia, 8.
- Clevalda, Damasha Khoiri, dan Dona Budi Kharisma. (2021). Perlindungan hukum terhadap nasabah dompet digital oleh Bank Indonesia. *Privat Law*, 9(1).
- Damayanti, Miranda, dan Ery Agus Priyono. (2022). Legal consequences for LDMO disclosing personal data of transacting parties: A study of legal protection. *Sign Jurnal Hukum*, 4(2), 221–232.
- DM, Mohd Yusuf, dan Jasmine Lim. (2022). Kejahatan phishing dalam dunia cyber crime dan sistem hukum di Indonesia. *Jurnal Pendidikan dan Konseling*, 4(5).
- Fauzi, Elfian, dan Nabila Alif Radika Shandy. (2022). Hak atas privasi dan politik hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Jurnal Lex Renaissance*, 7(3), 445–461.
- Febrian, Febrian, Indrawan Yoswanda Saputra, dan Diana R. W. Napitupulu. (2025). Implikasi hukum terhadap perlindungan data pribadi dalam transaksi fintech. *Rechtsnormen Jurnal Komunikasi dan Informasi Hukum*, 4(1), 21–30.
- Fista, Yanci Libria, Aris Machmud, dan Suartini Suartini. (2023). Perlindungan hukum konsumen

dalam transaksi e-commerce ditinjau dari perspektif Undang-Undang Perlindungan Konsumen. *Binamulia Hukum*, 12(1), 177–189.

- Habibi, Miftakhur Rokhman, dan Isnatul Liviani. (2020). Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qanun*, 23(2), 400–426.
- Hartanto, Hartanto, Vincent Rosadi, dan Ervin Alvaro Yosmar. (2023). Perlindungan hukum terhadap pengguna aplikasi e-wallet DANA. *Pattimura Legal Journal*, 2(3), 267–279.
- Hidayat, Topik, Jeffry A. Ch. Likadja, dan Petrus E. Derozari. (2023). Perlindungan hukum data pribadi konsumen dalam perdagangan elektronik. *Journal of Comprehensive Science*, 2(5), 1087–1103.
- Iermansyah, Agus, Dhian Indah Astanti, dan B. Rini Heryanti. (2023). Perlindungan hukum bagi konsumen dalam jasa layanan keuangan digital. *Semarang Law Review*, 4(1), 51–59.
- Ibrahim, Johnny. (2013). Teori dan metodologi penelitian hukum normatif. Jakarta: Bayu Media.
- Kamila, Zahra, dan Rahmad Efendi. (t.t.). Perlindungan hukum atas kehilangan saldo pengguna e-wallet DANA ditinjau dari Fatwa DSN-MUI No. 116/DSN-MUI/IX/2017 tentang uang elektronik syariah. *UNES Law Review*, 6(2).
- Kusnadi, Sekaring Ayumeida. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Al Wasath Jurnal Ilmu Hukum*, 2(1), 9–16.
- Matasari, Lala Nur. (2025). Perlindungan konsumen terhadap hilangnya saldo uang elektronik berbasis server: Studi kasus aplikasi DANA di Kota Jambi. *Zaaken: Journal of Civil and Business Law*, 6(2).
- Marzuki, Peter Mahmud. (2017). Penelitian hukum: Edisi revisi (Ed. 5). Jakarta: Kencana.
- Octora, Rahel. (2021). Regulation on electronic system security for e-wallet in order to protect consumers from financial loss due to cyber fraud based on Indonesian law. *International Journal of Social Science and Human Research*, 4(9).
- Perdana, Jelang Fajar Putra, I Gusti Ayu Ketut Rachmi Handayani, dan Lego Karjoko. (2020). Perlindungan konsumen atas hak penggantian kerugian. *Jurnal Discretie*, 1(1), 42.
- Pitriani, Zufriani, dan Darlius. (2025). Pendekatan preventif dan represif terhadap perlindungan hak-hak konsumen dalam transaksi e-commerce. *Jurnal Hukum Lex Generalis*, 6(4).
- Putra, Ferdy Arliyanda, dan Lucky Dafira Nugroho. (2021). Perlindungan hukum terhadap penyalahgunaan akun dalam transaksi elektronik melalui Traveloka. *Inicio Legis*, 2(1).
- Rahardjo, Satjipto. (2014). Ilmu hukum (Cet. 8). Bandung: PT Citra Aditya Bakti.
- Rahardjo, Satjipto, Karolus Kopong Medan, dan Frans J. Rengka. (2003). Sisi-sisi lain dari hukum di Indonesia. Jakarta: Penerbit Buku Kompas.
- Rosmawati. (2017). Pokok-pokok hukum perlindungan konsumen. Jakarta: Kencana.
- Sakinah, Alsendi, Muryanto Lanontji, dan Rima Anggriyani. (2026). Perlindungan konsumen dalam sistem fintech: Tanggung gugat pihak aplikasi DANA terhadap kehilangan dana nasabah. *Qistie*, 18(2), 316–328.
- Setiawan, Wawan, Dede Sunaryo, dan Khorida AR. (2022). Analisis fitur layanan dan keamanan terhadap penggunaan dompet digital (ShopeePay). *Digital Business Journal*, 1(1), 52.
- Shidarta. (t.t.). Hukum perlindungan konsumen Indonesia (Ed. revisi). PT Gramedia Widiasarana Indonesia.
- Soekanto, Soerjono. (2006). Pengantar penelitian hukum. Jakarta: UI Press.
- Soekanto, Soerjono. (2006). Penelitian hukum normatif.

- Stevani, Winnie, dan Lu Sudirman. (2021). Urgensi perlindungan data pengguna financial technology terhadap aksi kejahatan online di Indonesia. *Journal of Judicial Review*, 23(2), 197–216.
- Sylviana, Glory, Dwiki Alif Setiawan, Carmelita Listyani, Elisya Karina, dan Linda Apriliana Peryoga Putri. (2024). Perlindungan hukum data pengguna e-wallet atas kebocoran data yang disalahgunakan oleh pinjaman online, 3(3).
- Wahid, Abdul, dan Mohammad Labib. (2010). *Kejahatan mayaantara (cyber crime) (Cet. 2)*. Bandung: Refika Aditama.
- Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
- Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 4 Tahun 2023.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Peraturan Bank Indonesia Nomor 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran.
- Peraturan Bank Indonesia Nomor 20/6/PBI/2018 tentang Uang Elektronik.
- Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran.

UMS LIBRARY
-TERAKREDITASI A-