



## Perlindungan Hukum Terhadap Nasabah Bank Dalam Penggunaan Aplikasi Dana Di Indonesia

Nor Paridah<sup>1\*</sup>, Karina Yunitasari<sup>2</sup>, Rachma Arrini Aprilia Putri<sup>3</sup>, Igund Farhan Sahrir<sup>4</sup>

<sup>1,2,3,4</sup> Program Studi Hukum, Fakultas Hukum, Universitas Mulawarman

<sup>4\*</sup> [igund22@gmail.com](mailto:igund22@gmail.com)

### Abstrak

Sistem perbankan sangat bergantung pada kepercayaan pelanggannya, sehingga peran Lembaga Penjamin Simpanan (LPS) sangat penting dalam menjaga kepercayaan ini. Sementara itu, memerangi kejahatan siber dan memastikan perlindungan hukum bagi pelanggan adalah aspek penting dalam menjaga keamanan sistem keuangan. Penelitian ini mengkaji peran LPS dan penyedia dompet digital DANA dalam melindungi pelanggan dan memberlakukan langkah-langkah hukum terhadap kejahatan siber. Melalui metode deskriptif kualitatif, penelitian ini menganalisis literatur dan regulasi yang relevan mengenai perlindungan pelanggan dan keamanan siber. Temuan penelitian menegaskan peran penting LPS dalam menjaga kepercayaan, mekanisme perlindungan hukum, penegakan hukum terhadap kejahatan siber, dan upaya DANA untuk mencegah dan menanggulangi kejahatan siber. Kolaborasi antara lembaga keuangan, penegak hukum, dan sektor swasta sangat penting dalam meningkatkan kepercayaan pelanggan dan memastikan keamanan sistem keuangan digital.

**Kata Kunci :** Perlindungan Pelanggan, Keamanan Siber, Dompet Digital, Penegakan Hukum

### Abstract

*The banking system relies heavily on trust from its customers, making the role of the Deposit Insurance Corporation (LPS) pivotal in maintaining this trust. Meanwhile, combating cybercrimes and ensuring legal protection for customers are crucial aspects of safeguarding the financial system. This study examines the roles of LPS and e-wallet provider DANA in protecting customers and enforcing legal measures against cybercrimes. Through a descriptive qualitative method, this research analyzes relevant literature and regulations concerning customer protection and cybersecurity. The findings underscore LPS's significant role in preserving trust, legal protection mechanisms, law enforcement against cybercrimes, and DANA's efforts to prevent and mitigate cybercrimes. Collaboration between financial institutions, law enforcement agencies, and the private sector is vital in enhancing customer trust and ensuring the security of digital financial systems.*

**Keyword :** Customer Protection, Cybersecurity, E-Wallet, Legal Enforcement

## PENDAHULUAN

Teknologi pada masa kini telah menghadirkan kemudahan yang belum pernah terbayangkan sebelumnya dalam berbagai aspek kehidupan, terutama dalam hal melakukan transaksi keuangan. Perkembangan pesat teknologi digital telah mengubah pola pikir dan gaya hidup masyarakat secara signifikan. Sekarang, seseorang dapat melakukan pembayaran, pembelian, atau pemesanan barang atau jasa tanpa perlu mengeluarkan uang tunai dari dompetnya. Cukup dengan memiliki gawai dan mengunduh aplikasi dompet elektronik yang tersedia di dalamnya, semua aktivitas transaksi dapat dilakukan dengan mudah dan cepat (Anrova & Sembiring, 2022). Dalam inovasi yang terus berkembang di era digital ini, transaksi keuangan melalui aplikasi menjadi pilihan utama bagi banyak orang. Fenomena ini tidak hanya memudahkan akses terhadap layanan keuangan, tetapi juga memperluas cakupan layanan keuangan bagi masyarakat, terutama di negara-negara berkembang seperti Indonesia (Bongomin, Yourougou, & Munene, 2019). Terobosan terbaru dalam sektor finansial adalah munculnya e-wallet atau dompet digital, yang telah menjadi alat pembayaran esensial dan sehari-hari bagi masyarakat modern (Halim & Orleans, 2023).

Salah satu contoh yang mencuat sebagai *platform* e-wallet unggulan di Indonesia adalah DANA. Dengan menyajikan solusi transaksi yang cepat, mudah, dan efisien, DANA telah berhasil menarik minat masyarakat untuk menggunakan layanannya (Kamila & Efendi, 2023). Namun, di balik kemudahan tersebut, juga terdapat risiko keamanan yang semakin meningkat. Menurut laporan yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber di Indonesia per April tahun 2023 mencapai angka yang mencengangkan, yakni 27 juta kasus. Fenomena ini menunjukkan betapa rentannya keamanan dalam transaksi digital di Indonesia (Surya *et al.*, 2023). Salah satu contoh konkret dari risiko keamanan dalam transaksi digital adalah kasus pembobolan dana nasabah yang terjadi di berbagai



platform dompet digital, termasuk DANA. Kejadian ini menunjukkan bahwa meskipun telah ada upaya untuk meningkatkan keamanan sistem, namun masih terdapat celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan tindakan kriminal (Rabbani *et al.*, 2023). Selain itu, munculnya kasus-kasus penipuan melalui customer care palsu, phishing dengan mengirimkan link palsu terkait aplikasi DANA, hingga pembuatan kartu fisik palsu, semakin menambah kompleksitas masalah keamanan dalam transaksi digital (Wardani, 2023).

Oleh karena itu, diperlukan analisis yang mendalam mengenai perlindungan hukum bagi nasabah dalam konteks transaksi keuangan digital (Panjaitan & Pramono, 2023). Perlindungan hukum yang efektif menjadi kunci utama dalam menjaga keamanan dan kepercayaan masyarakat terhadap sistem keuangan digital. Melalui analisis tersebut, diharapkan dapat ditemukan solusi-solusi yang tepat guna untuk mengatasi masalah-masalah keamanan yang sering terjadi dalam transaksi digital, khususnya pada platform e-wallet seperti DANA (Haliwela, 2023). Penelitian mengenai perlindungan hukum bagi nasabah bank hukum dalam konteks aplikasi digital seperti DANA menjadi sangat penting mengingat maraknya kasus-kasus kejahatan siber yang menimpa nasabah (Syahputra & Sejati, 2023). Hal ini tidak hanya berdampak pada kerugian finansial bagi nasabah, tetapi juga merusak kepercayaan masyarakat terhadap sistem keuangan digital secara keseluruhan (Azhari, 2021).

Berdasarkan uraian latar belakang tersebut, untuk meneliti mengenai perlindungan hukum bagi nasabah bank, maka rumusan masalah yang akan dibahas adalah peran Lembaga Penjamin Simpanan (LPS) terhadap kepercayaan nasabah, perlindungan hukum atas nasabah, penegakan hukum terhadap kejahatan siber, serta upaya DANA untuk mencegah dan menanggulangi kasus-kasus kejahatan siber terhadap nasabah. Tujuan dari penelitian ini adalah untuk menganalisis peran Lembaga Penjamin Simpanan (LPS) dalam menjaga kepercayaan nasabah, perlindungan hukum atas nasabah, penegakan hukum terhadap kejahatan siber, serta upaya untuk mencegah dan menanggulangi kasus-kasus kejahatan siber terhadap nasabah, dengan studi kasus pada aplikasi e-wallet DANA.

## METODOLOGI PENELITIAN

Metode penelitian yang akan digunakan dalam penelitian ini adalah metode kualitatif deskriptif. Penelitian kualitatif merupakan pendekatan yang bertujuan untuk mendalami dan memahami fenomena tertentu, seperti perilaku, persepsi, motivasi, dan tindakan yang dialami oleh partisipan. Metode ini menyediakan data deskriptif yang relevan dari partisipan yang terlibat dalam penelitian (Soesanto *et al.*, 2023). Pendekatan kualitatif akan digunakan untuk mendapatkan pemahaman yang mendalam tentang bagaimana nasabah bank hukum mengalami dan merespons permasalahan keamanan dalam transaksi digital, khususnya terkait dengan aplikasi DANA. Penelitian kualitatif akan mengandalkan data sekunder yang diperoleh melalui studi literatur terdahulu yang relevan dengan topik penelitian. Studi literatur merupakan teknik pengumpulan data yang dilakukan dengan melakukan telaah mendalam terhadap berbagai sumber, termasuk buku, jurnal ilmiah, catatan, dan laporan yang memiliki kaitan dengan masalah yang sedang diteliti (Soesanto *et al.*, 2023).

Melalui analisis studi literatur, peneliti akan memperoleh wawasan yang lebih luas tentang konteks hukum dan keamanan dalam transaksi digital di Indonesia, serta berbagai pendekatan yang telah diambil dalam menanggulangi kasus kejahatan siber yang melibatkan nasabah aplikasi DANA. Data akan dikumpulkan melalui teknik dokumentasi studi literatur, yang mencakup penelitian-penelitian sebelumnya yang telah dilakukan oleh para ahli di bidang hukum dan keamanan digital, regulasi-regulasi hukum terkait transaksi keuangan digital di Indonesia, serta studi kasus yang relevan dengan masalah yang sedang diteliti

## HASIL DAN PEMBAHASAN

### Peran Lembaga Penjamin Simpanan (LPS) Terhadap Kepercayaan Nasabah

Sistem keuangan merupakan suatu sistem yang terdiri dari berbagai komponen, termasuk lembaga jasa keuangan, pasar keuangan, infrastruktur keuangan, dan sistem pembayaran. Keseluruhan sistem ini saling berinteraksi untuk memfasilitasi pengumpulan dana dari masyarakat dan pengalokasiannya guna mendukung aktivitas perekonomian nasional. Definisi ini sejalan dengan yang dijelaskan dalam Pasal 1 angka 7 Peraturan Bank Indonesia (PBI) tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran, yang menjelaskan bahwa Dompet Elektronik adalah layanan elektronik yang digunakan untuk menyimpan data instrumen pembayaran, seperti alat pembayaran dengan menggunakan kartu dan/atau uang elektronik, serta dapat menampung dana untuk melakukan pembayaran (Anrova & Sembiring, 2022).

Penyelenggaraan e-wallet atau dompet elektronik merupakan bagian penting dari sistem pembayaran yang berlaku di Indonesia saat ini. Hal ini sesuai dengan regulasi yang mengatur pihak-pihak yang dapat menjadi penyelenggara dompet elektronik. Menurut Putra & Nugroho (2020), penyelenggaraan dompet elektronik di Indonesia dapat dilakukan oleh bank atau lembaga selain bank yang telah memperoleh izin dari Bank Indonesia. Salah satu syarat lain yang diatur dalam PBI Penyelenggaraan Pemrosesan Transaksi Pembayaran adalah bentuk hukum dari penyelenggara dompet elektronik, di mana lembaga selain bank harus berbentuk perseroan terbatas. Salah satu contoh penyelenggara dompet elektronik di Indonesia adalah PT Espay Debit Indonesia Koe (EDIK), yang merupakan lembaga selain bank yang telah memperoleh izin penyelenggaraan dompet elektronik DANA dari Bank Indonesia. Fakta ini menegaskan bahwa pemberian izin dari Bank Indonesia memegang peranan penting dalam regulasi dan pengawasan terhadap penyelenggaraan dompet elektronik di Indonesia, sesuai dengan kewenangan yang diamanatkan oleh Undang-Undang Bank Indonesia.



Prinsip kepercayaan memiliki peran yang sangat penting dalam industri perbankan. Kehadiran bank sangat bergantung pada kepercayaan masyarakat sebagai pemilik dana. Sebagaimana diungkapkan oleh Anrova & Sembiring, (2022), fungsi bank sebagai lembaga kepercayaan terutama berkaitan dengan kegiatan bank dalam menghimpun dana simpanan dari masyarakat. Tanpa adanya kepercayaan tersebut, masyarakat tidak akan bersedia menyimpan uangnya di bank tersebut, yang berpotensi mengganggu stabilitas dan kelangsungan operasional bank tersebut.

Prinsip kepercayaan ini mencakup berbagai aspek, termasuk kepercayaan terhadap keamanan dan kredibilitas penyelenggara dompet elektronik. Nasabah akan lebih memilih menggunakan layanan dompet elektronik yang dioperasikan oleh lembaga yang memiliki reputasi baik dan telah memperoleh izin resmi dari otoritas yang berwenang. Oleh karena itu, peran Bank Indonesia dalam memberikan izin kepada penyelenggara dompet elektronik seperti PT EDIK sangatlah penting dalam membangun dan memelihara kepercayaan masyarakat terhadap sistem pembayaran elektronik di Indonesia. Selain membangun kepercayaan, Bank Indonesia juga memiliki peran dalam memastikan kestabilan dan efisiensi sistem pembayaran secara keseluruhan. Melalui regulasi dan pengawasan yang cermat, Bank Indonesia berusaha untuk mencegah terjadinya gangguan atau kegagalan dalam sistem pembayaran yang dapat merugikan nasabah dan perekonomian secara luas.

Lembaga Penjamin Simpanan (LPS) memiliki peran yang sangat penting dalam menjaga kepercayaan nasabah terhadap sistem perbankan. Sebagai lembaga yang dibentuk dengan tujuan utama melindungi kepentingan nasabah, LPS memiliki beberapa fungsi utama yang bertujuan untuk menjaga stabilitas sistem perbankan serta meningkatkan kepercayaan masyarakat terhadap lembaga keuangan. Undang-Undang (UU) LPS adalah manifestasi nyata dari perhatian pemerintah terhadap kepercayaan nasabah terhadap kegiatan perbankan. Keterlibatan perbankan yang signifikan dalam mempercepat pertumbuhan investasi di suatu negara menjadi alasan utama mengapa pemerintah turut serta dalam menjaga kepercayaan masyarakat terhadap operasional perbankan (Anrova & Sembiring, 2022). Pembentukan UU LPS berasal dari amanah yang diatur dalam Undang-Undang Nomor 10 tahun 1998 tentang Perbankan, yang menuntut pembentukan lembaga independen khusus untuk menjamin dana nasabah di sektor perbankan guna meningkatkan kepercayaan masyarakat setelah krisis moneter tahun 1998. Berdasarkan Pasal 4 UU LPS, fungsi utama LPS adalah untuk menjamin simpanan nasabah dan juga berperan aktif dalam menjaga stabilitas sistem perbankan sesuai dengan wewenangnya.

LPS berperan sebagai penjamin atas simpanan nasabah. LPS memberikan jaminan kepada nasabah bahwa simpanan mereka akan aman dan terlindungi, meskipun terjadi kegagalan atau kebangkrutan bank tempat mereka menyimpan uang. Adanya jaminan membuat nasabah merasa lebih percaya diri untuk menyimpan dananya di bank, tanpa khawatir kehilangan uang mereka akibat risiko-risiko yang mungkin terjadi. LPS juga bertindak sebagai pengawas terhadap bank-bank yang beroperasi di Indonesia. Melalui fungsi pengawasannya, LPS memastikan bahwa bank-bank mematuhi peraturan dan standar yang telah ditetapkan dalam menjalankan operasinya. LPS memiliki peran dalam memberikan edukasi dan informasi kepada masyarakat tentang pentingnya menjaga keamanan dananya di bank. Melalui program-program penyuluhan dan kampanye informasi, LPS berusaha meningkatkan literasi keuangan masyarakat, sehingga mereka lebih memahami risiko-risiko yang terkait dengan penyimpanan dana di bank dan langkah-langkah yang dapat diambil untuk melindungi kepentingan mereka. LPS berperan dalam menangani klaim-klaim nasabah dalam kasus kegagalan bank. Apabila suatu bank dinyatakan gagal dan tidak mampu memenuhi kewajibannya kepada nasabah, LPS akan bertindak sebagai penjamin dan membayar klaim-klaim nasabah sesuai dengan ketentuan yang berlaku. LPS juga berperan dalam mempromosikan stabilitas sistem perbankan secara keseluruhan. Melalui berbagai kebijakan dan langkah-langkah yang diambil, LPS berusaha menjaga agar sistem perbankan tetap stabil dan terhindar dari risiko-risiko yang dapat mengganggu kepercayaan masyarakat.

Dalam menjaga kepercayaan nasabah terhadap transaksi dalam e-wallet, mencapai kesepahaman tentang proses transaksi yang dilakukan melalui *platform* tersebut adalah sesuatu yang harus tercapai. Sebagai aktivitas yang serupa dengan transaksi perbankan, perlindungan dari lembaga seperti LPS juga menjadi penting. Menurut Purbaya Yudhi, Ketua Dewan Komisiner LPS, menjaga kepercayaan masyarakat pada *platform* digital melibatkan perlindungan data digital dalam sistem Informasi dan Teknologi (ICT), pengembang aplikasi, serta kebutuhan akan SDM yang kompeten. UU LPS dan UU PPKSK memberikan wewenang kepada LPS untuk menangani bank yang mengalami kesulitan, termasuk dalam hal penjaminan dan penggantian simpanan nasabah hingga batas tertentu per nasabah per bank. Namun, e-wallet seperti DANA bukanlah produk perbankan dan tidak diatur oleh UU Perbankan atau UU LPS. Pengaturan mengenai dompet elektronik terbatas pada Peraturan Bank Indonesia (PBI). Meskipun demikian, berdasarkan Undang-Undang Pembentukan Peraturan Perundang-Undangan, peraturan Bank Indonesia tidak memiliki kedudukan atau kekuatan yang sama dengan UU Perbankan atau UU LPS, sehingga tidak dapat menggantikan atau mengesampingkan peraturan yang telah ditetapkan dalam kedua undang-undang tersebut (Anrova & Sembiring, 2022).

#### **Perlindungan Hukum Atas Nasabah**

Sebuah dompet elektronik adalah sebuah layanan digital yang memfasilitasi pengguna untuk menyimpan informasi pembayaran, seperti data kartu atau uang elektronik, dan juga memungkinkan mereka untuk menyimpan dana serta melakukan pembayaran melalui *platform* tersebut. Untuk mendirikan layanan e-wallet, sebuah perusahaan harus memenuhi beberapa persyaratan khusus (Kamila & Efendi, 2023). Salah satunya adalah memperoleh izin yang sesuai, yang dapat diperoleh melalui bank, lembaga non-bank, atau perseroan terbatas. Selain itu, perusahaan harus memiliki



legalitas yang jelas, profil yang transparan, serta kesesuaian dengan semua peraturan hukum yang berlaku. Perusahaan penyedia dompet elektronik harus memiliki kesiapan operasional yang baik dan sistem yang aman serta handal. Selama proses pembayaran, perusahaan tersebut harus menerapkan manajemen risiko yang efektif dan standar keamanan informasi yang tinggi. Hal ini penting untuk memastikan bahwa data dan dana pengguna tetap aman selama digunakan dalam transaksi.

Dalam hal apabila terjadi pembatalan transaksi atau permintaan pengembalian dana dari pengguna, penyedia e-wallet harus segera mengambil langkah-langkah untuk mengembalikan dana tersebut kepada pengguna. Selain itu, perusahaan tersebut harus memiliki prosedur yang jelas dan efisien untuk memastikan bahwa proses pengembalian dana berjalan dengan lancar dan sesuai dengan ketentuan yang berlaku. Dana yang dikembalikan harus berasal dari sumber asli yang digunakan dalam transaksi tersebut, sehingga memastikan bahwa proses pengembalian berjalan dengan transparan dan adil bagi semua pihak yang terlibat.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan dasar hukum bagi hak-hak konsumen dalam mengkonsumsi barang dan jasa. Di dalamnya termaktub hak untuk memperoleh kenyamanan dan keamanan dalam mengonsumsi barang dan/atau jasa, serta hak untuk memperoleh ganti rugi sebagaimana diatur dalam Pasal 4 huruf (a). Selain itu, Pasal 4 huruf (d) dari undang-undang tersebut juga memberikan hak kepada konsumen untuk mengemukakan pendapat dan keluhan atas barang dan/atau jasa yang digunakan. Aturan ini memberikan kesempatan bagi nasabah e-wallet untuk menyampaikan kekurangan dari layanan dompet digital yang diberikan oleh penyelenggara e-wallet (Kamila & Efendi, 2023).

Sebagai respons terhadap hak-hak ini, para pelaku usaha yang merupakan pihak dari e-wallet berkewajiban untuk mendengarkan pendapat atau keluhan konsumennya. Salah satu aspek yang sangat berkaitan dengan kepercayaan dari pihak nasabah adalah privasi data. Privasi ini harus dijaga oleh penyelenggara e-wallet sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, khususnya di Pasal 26 Ayat (1) yang secara singkat mengatur mengenai perlindungan data pribadi. Hal ini juga dibahas dalam Undang-Undang No. 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang No. 7 Tahun 1992 Tentang Perbankan, yang mengatur mengenai rahasia bank dalam Pasal 40 Ayat (1) dan (2). Rahasia bank, menurut Pasal 1 Angka 28 Undang-Undang No. 10 Tahun 1998, adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya. Peraturan Bank Indonesia Nomor 7/6/PBI/2005 Tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah menekankan pentingnya kejujuran dalam penggunaan data pribadi nasabah atau konsumen untuk melindungi hak-hak nasabah selaku konsumen yang berkaitan dengan bank. Perlindungan data pribadi ini juga merupakan langkah untuk mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Pasal 18 Peraturan Bank Indonesia 18/40/PBI/2016 menetapkan bahwa penyelenggara dompet elektronik yang menyediakan layanan penyimpanan informasi pembayaran dan menampung dana memiliki tanggung jawab tambahan yang harus dipenuhi (Kamila & Efendi, 2023).

Dalam pelaksanaan transaksi pembayaran, setiap penyelenggara jasa sistem pembayaran harus menjalankan manajemen risiko dengan efektif dan konsisten serta menerapkan standar keamanan sistem informasi. Sebagai pembuat aplikasi, perusahaan juga harus mengambil tanggung jawab atas kerugian yang mungkin terjadi karena disfungsi aplikasi yang dimilikinya atau kesalahan manusia. Apabila perusahaan menolak untuk bertanggung jawab atas kerugian yang dialami oleh konsumennya, perusahaan tersebut dapat dikenai sanksi sesuai dengan ketentuan yang tercantum dalam Peraturan Bank Indonesia. Pasal 36 dalam Peraturan Bank Indonesia 18/40/PBI/2016 menyatakan bahwa jika setelah berlalunya jangka waktu yang ditentukan dalam Pasal 39 atau setelah berlakunya peraturan ini, ada pihak yang menyelenggarakan jasa sistem pembayaran tanpa izin dari Bank Indonesia, maka Bank Indonesia memiliki kewenangan untuk memberikan peringatan tertulis dan/atau merekomendasikan kepada otoritas yang berwenang untuk menghentikan operasi usaha atau mencabut izin usaha yang telah diberikan (Kamila & Efendi, 2023). Penyelenggara dompet elektronik juga diharapkan untuk menerapkan prinsip perlindungan konsumen sesuai dengan yang dijelaskan dalam Pasal 24 dari Peraturan Bank Indonesia 18/40/PBI/2016.

Hal ini mencakup langkah-langkah untuk menjaga keamanan dan hak-hak konsumen dalam penggunaan dompet elektronik. Jika dana dalam dompet elektronik atau digital disimpan dan dikelola oleh pengguna sendiri, tanggung jawab atas dana tersebut sepenuhnya berada di tangan pemilik dompet. Namun, jika kesalahan atau kerugian terjadi karena kelalaian dari penyelenggara dompet elektronik, maka penyelenggara wajib bertanggung jawab. Dalam skenario di mana dana di dompet digital disimpan oleh penyelenggara dompet elektronik, mereka harus memikul tanggung jawab atas setiap kehilangan atau kerusakan yang mungkin terjadi.

Berdasarkan Pasal 21 ayat (4) UU ITE No. 11 Tahun 2008, dijelaskan bahwa jika kerugian transaksi elektronik terjadi karena kesalahan atau kelalaian pengguna jasa layanan, maka pengguna tersebut bertanggung jawab atas segala kerugiannya. Pada POJK No.1/POJK.07/2013 tentang perlindungan konsumen sektor jasa keuangan, Pasal 29 menjelaskan bahwa Pelaku Usaha Jasa Keuangan wajib bertanggung jawab atas kerugian konsumen yang timbul akibat kesalahan dan/atau kelalaian, pengurus, pegawai Pelaku Usaha Jasa Keuangan dan/atau pihak ketiga (Kamila & Efendi, 2023). Hal ini menegaskan bahwa penyelenggara dompet elektronik harus bertanggung jawab dan wajib memberikan ganti rugi sesuai dengan kerugian yang dialami oleh pengguna layanan jika kerugian tersebut terjadi karena kelalaian dari pihak penyelenggara.



### Penegakan Hukum Terhadap Kejahatan Siber

Perkembangan ilmu pengetahuan dan teknologi telah membawa dampak yang signifikan dalam berbagai aspek kehidupan manusia. Sayangnya, bersamaan dengan kemajuan tersebut, ada pula penyalahgunaan teknologi sebagai instrumen untuk melakukan kejahatan. Fenomena ini menuntut adanya prediksi kebijakan hukum yang tepat agar kejahatan dunia maya dapat ditindak secara efektif, baik dalam penegakan hukum maupun dalam sistem pengadilan. Pentingnya peran sistem penegakan hukum, termasuk petugas polisi, tidak bisa dipandang remeh. Indonesia telah memiliki regulasi yang mengatur kejahatan dunia maya, yang tertuang dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, yang merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008. Regulasi ini memberikan landasan hukum yang kuat bagi penegakan hukum terhadap kejahatan cyber. Namun, implementasi dan penegakan hukum ini membutuhkan kerja keras dari lembaga penegak hukum, terutama kepolisian.

Penegakan hukum merupakan bagian integral dari sistem hukum suatu negara. Petugas polisi adalah ujung tombak dari penegakan hukum, mereka yang berpartisipasi secara langsung atau tidak langsung dalam kegiatan kepolisian. Dalam menjalankan tugasnya, petugas polisi harus memahami nilai-nilai, aturan, dan perilaku yang menjadi dasar dari hukum. Mereka juga harus senantiasa mengambil tindakan dan berupaya mencapai tujuan keadilan dalam setiap kasus yang mereka tangani. Sikap anggota polisi dalam menjalankan tugasnya seringkali didasarkan pada penilaian. Proses penilaian ini merupakan suatu proses yang kompleks dan penting dalam menangani masalah yang timbul di lapangan. Petugas polisi harus mampu melakukan penilaian yang cermat dan adil dalam setiap situasi yang mereka hadapi. Hal ini membutuhkan kepekaan terhadap konteks dan situasi yang berkembang, serta kemampuan untuk mengambil keputusan dengan cepat dan tepat.

Namun, tantangan dalam penegakan hukum terhadap kejahatan cyber tidaklah mudah. Kejahatan dunia maya seringkali tidak terlihat secara langsung dan dapat dilakukan dari jarak jauh, membuatnya sulit untuk dilacak dan ditindak oleh aparat penegak hukum. Selain itu, para pelaku kejahatan cyber seringkali menggunakan teknik-teknik yang canggih untuk menyembunyikan jejak digital mereka, menambah kompleksitas dalam proses penyelidikan dan penegakan hukum. Oleh karena itu, diperlukan kerja sama yang erat antara berbagai pihak terkait, termasuk lembaga penegak hukum, pemerintah, sektor swasta, dan masyarakat sipil, dalam upaya untuk memerangi kejahatan cyber. Kerja sama ini meliputi pertukaran informasi, pelatihan, pengembangan teknologi keamanan, dan pembentukan kebijakan yang mendukung penegakan hukum yang efektif.

Peran teknologi juga sangat penting dalam mendukung penegakan hukum terhadap kejahatan cyber. Penggunaan teknologi seperti analisis data besar (big data), kecerdasan buatan (artificial intelligence), dan teknologi blockchain dapat membantu dalam mendeteksi dan mencegah kejahatan cyber, serta dalam mengumpulkan bukti yang kuat untuk proses penyelidikan dan pengadilan. Namun, penggunaan teknologi juga memiliki tantangan tersendiri, termasuk masalah privasi dan keamanan data. Oleh karena itu, penting bagi pemerintah dan lembaga terkait untuk mengembangkan regulasi yang memadai untuk mengatur penggunaan teknologi dalam penegakan hukum, serta untuk melindungi privasi dan keamanan data masyarakat. Selain penegakan hukum yang efektif, pendidikan dan kesadaran masyarakat juga merupakan faktor penting dalam memerangi kejahatan cyber. Masyarakat perlu diberikan pemahaman yang lebih baik tentang risiko dan konsekuensi dari kejahatan cyber, serta tentang langkah-langkah yang dapat mereka ambil untuk melindungi diri mereka sendiri secara online.

### Upaya DANA Untuk Mencegah dan Menanggulangi Kasus Kejahatan Siber Terhadap Nasabah

DANA, sebagai salah satu *platform* e-wallet unggulan di Indonesia, memiliki tanggung jawab besar dalam melindungi nasabahnya dari ancaman kejahatan siber. Berbagai upaya telah dilakukan oleh DANA untuk mencegah dan menanggulangi kasus kejahatan siber demi menjaga keamanan dan kepercayaan masyarakat terhadap sistem keuangan digital. Salah satu upaya utama yang dilakukan oleh DANA adalah peningkatan keamanan sistem. DANA terus mengembangkan infrastruktur teknologi dan sistem keamanan yang canggih untuk melindungi data dan transaksi nasabahnya dari serangan siber. Hal ini mencakup implementasi enkripsi data, proteksi terhadap malware dan virus, serta penggunaan mekanisme otentikasi ganda untuk memastikan bahwa hanya pemilik akun yang sah yang dapat mengaksesnya. Selain itu, DANA juga secara rutin melakukan pemantauan dan pembaruan sistem keamanan sesuai dengan perkembangan teknologi dan ancaman kejahatan siber yang terbaru.

Selain meningkatkan keamanan sistem, DANA juga aktif dalam memberikan edukasi dan kesadaran kepada nasabahnya tentang praktik keamanan digital yang baik. Melalui berbagai kampanye dan materi edukasi, DANA menyampaikan informasi tentang risiko kejahatan siber yang mungkin dihadapi oleh nasabah, serta langkah-langkah yang dapat diambil untuk melindungi diri mereka sendiri. Ini termasuk praktik-praktik seperti tidak membagikan informasi pribadi atau rahasia kepada pihak lain, menghindari mengklik tautan yang mencurigakan, dan menggunakan kata sandi yang kuat dan unik untuk akun mereka. DANA secara aktif memantau dan merespons adanya indikasi atau laporan kejahatan siber yang terjadi terhadap nasabahnya. Tim keamanan DANA bekerja sama dengan lembaga penegak hukum dan pihak berwenang untuk menyelidiki kasus-kasus kejahatan siber, serta memberikan bantuan dan dukungan kepada nasabah yang menjadi korban. Langkah-langkah penegakan hukum juga diambil untuk menindak pelaku kejahatan siber dan mencegah terjadinya kejahatan serupa di masa mendatang.

Selain upaya-upaya teknis dan operasional, DANA juga menjalin kerja sama dengan berbagai pihak terkait, termasuk lembaga pemerintah, lembaga penegak hukum, dan sektor swasta lainnya, dalam rangka memperkuat upaya



pengecanaan dan penanggulangan kejahatan siber. Kerja sama ini mencakup pertukaran informasi, pelatihan bersama, dan pengembangan solusi keamanan yang inovatif untuk mengatasi ancaman kejahatan siber secara efektif. Untuk mengantisipasi kemungkinan terulangnya kejadian penipuan ataupun pembobolan di masa mendatang, DANA telah mengimplementasikan berbagai langkah preventif dan teknologi keamanan terkini. DANA secara aktif berkomitmen untuk memberikan perlindungan yang optimal kepada seluruh penggunanya. Dengan mengadopsi teknologi berbasis AI, teknologi biometrik, two-factor authentication, dan fitur DANA VIZ, serta menyediakan DANA PROTECTION sebagai bentuk jaminan proteksi, DANA berusaha memastikan bahwa nasabahnya dapat melakukan transaksi dengan aman dan tanpa khawatir akan risiko kejahatan siber (Fadila, 2023).

## KESIMPULAN

Lembaga Penjamin Simpanan (LPS) memiliki peran yang krusial dalam memelihara kepercayaan nasabah terhadap sistem perbankan, sementara perlindungan hukum dan penegakan hukum terhadap kejahatan siber menjadi pilar penting dalam menjaga integritas dan keamanan nasabah. Di samping itu, upaya aktif dari *platform* e-wallet seperti DANA dalam mencegah dan menanggulangi kasus kejahatan siber terhadap nasabahnya menunjukkan komitmen industri finansial terhadap keamanan sistem keuangan digital. Dengan kerja sama yang solid antara lembaga keuangan, pemerintah, dan sektor swasta, kepercayaan nasabah dapat terus ditingkatkan, menghasilkan sistem keuangan yang stabil dan aman bagi masyarakat

## DAFTAR PUSTAKA

- Anrova, Y., & Sembiring, A. (2022). Peran Lembaga Penjamin Simpanan Terhadap Saldo Uang Elektronik Pada Dompet Elektronik Dana. *Jurnal Res Justitia: Jurnal Ilmu Hukum*, 2(1), 149-161.
- Azhari, A. (2021). Legal Review Of Consumer Law Protection On Personal Data On Digital Platform. *Indonesia Private Law Review*, 2, 59-72. <https://doi.org/10.25041/IPLR.V2I1.2189>.
- Bongomin, G., Yourougou, P., & Munene, J. (2019). Digital financial innovations in the twenty-first century. *Journal of Economic and Administrative Sciences*. <https://doi.org/10.1108/jeas-01-2019-0007>.
- Fadila, S. N. (2023). Marak Kasus Pembobolan pada Dompet Digital DANA, Begini Tanggapan DANA. Diakses pada 6 Mei 2024, dari <https://keuangan.kontan.co.id/news/marak-kasus-pembobolan-pada-dompet-digital-dana-begini-tanggapan-dana>
- Halim, E., & Orleans, B. (2023). The Impact of Digital Payment on Customer Purchasing Satisfaction in Online Market Transaction. *2023 International Conference on Digital Business and Technology Management (ICONDBTM)*, 1-6. <https://doi.org/10.1109/ICONDBTM59210.2023.10326754>.
- Haliwela, N. (2023). The Essence of Legal Protection of Personal Data of Customers In Banking Transactions. *SASI*. <https://doi.org/10.47268/sasi.v29i3.1528>.
- Kamila, Z., & Efendi, R. (2023). Perlindungan Hukum Atas Kehilangan Saldo Pengguna E-Wallet Dana di Tinjau Dari Fatwa DSN MUI No. 16/Dsn Mui/Ix/2017 Tentang Uang Elektronik Syariah (Studi Kasus Pengguna E-Wallet Dana di Kecamatan Medan Tembung, Kota Medan). *UNES Law Review*, 6(2), 7185-7193.
- Panjaitan, H., & Pramono, N. (2023). Legal Protection Of Consumers In Digital Transactions. *Russian Law Journal*. <https://doi.org/10.52783/rlj.v11i3.1622>.
- Putra, M. F., & Nugroho, L. D. (2020). Perlindungan hukum pengguna dompet elektronik atas hilangnya uang elektronik. *PROHUTEK*, 1(1).
- Rabbani, M., Wijaya, J., Kusuma, R., Purba, W., & Tajib, R. (2023). Digital Payments in Indonesia: Understanding the Effect of Application Security on User Trust. *Indonesian Journal of Computer Science*. <https://doi.org/10.33022/ijcs.v12i5.3426>.
- Soesanto, E., Utami, A. S., Chantica, J. A., Nabila, R. A., & Ricki, T. S. (2023). Keamanan Data Pribadi Dalam Sistem Pembayaran Via OVO Terhadap Ancaman dan Pengelabuan (Cybercrime). *IJM: Indonesian Journal of Multidisciplinary*, 1(2), 424-435.
- Surya, S., Jagtap, S., Ramnarayan, R., Priyadarshini, M., Ibrahim, R., & Alazzam, M. (2023). Protecting Online Transactions: A Cybersecurity Solution Model. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2630-2634. <https://doi.org/10.1109/ICACITE57410.2023.10183282>.
- Syahputra, A., & Sejati, H. (2023). Legal Protection of Banking Customers in the Perspective of Law 8 of 1999. *Journal Research of Social Science, Economics, and Management*. <https://doi.org/10.59141/jrssem.v2i11.475>.
- Wardani, A. S. (2023). Waspada, DANA Ungkap Deretan Modus Kejahatan yang Manfaatkan Platform Digital. Liputan6. Diakses pada 6 Mei 2024, dari <https://www.liputan6.com/teknoread/5403998/waspada-dana-ungkap-deretan-modus-kejahatan-yang-manfaatkan-platform-digital?page=2>