Jurnal De Jure Muhammadiyah Cirebon
Vol. 9 No. 1 (2025)

PERTANGGUNGJAWABAN HUKUM TERHADAP KEJAHATAN *CYBER* DALAM DOMPET DIGITAL DI ERA *FINTECH* PADA APLIKASI DANA

Raymond Marhehetua Hutahaean[1], Ridho Waridan Gumilar[2], F. Rizky Maulana[3], M. Arsya Al' Daffa[4], Lindryani Sjofjan[5]

[1 2 3 4 5] *Fakultas Hukum, Universitas Pakuan Bogor*

Email: [1] raymondhutahaean994@gmail.com ,[2] Welldhone14@gmail.com , [3] fferi0189@gmail.com ,[4] arsyaesiella@gmail.com, [5] lindryani.sjofjan@unpak.ac.id

Abstract

The rapid development of information technology has driven the transformation of financial systems into more digital forms through innovations in financial technology (fintech). One of the most popular fintech products in Indonesia is digital wallets, such as the DANA application. However, the convenience of digital transactions also creates vulnerabilities to cybercrime, which can harm users. This study aims to analyze the legal liability for cybercrime in the use of the DANA digital wallet, as well as to evaluate the effectiveness of existing regulations in protecting consumers. The research method used is normative juridical, with a statutory and case study approach. Data were obtained through literature review, documentation, and analysis of cybercrime cases involving the DANA application. The results of the study indicate that perpetrators of cybercrime involving digital wallets can be sanctioned under the Law on Electronic Information and Transactions (ITE Law), the Consumer Protection Law, and other relevant regulations. However, there are still weaknesses in law enforcement, particularly in tracking down perpetrators and providing compensation to victims. In addition, digital wallet providers are also responsible for enhancing their security systems and ensuring transparency in user data protection. In conclusion, legal accountability for cybercrime in digital wallets is not yet fully effective, and synergy between regulators, law enforcement agencies, and fintech industry players is needed to create a secure and trustworthy digital financial ecosystem.

Keywords: *Cybercrime, Digital Wallet, Legal Liability*

Jurnal
De Jure
Muhammadiyah Cirebon
Vol. 9 No. 1 (2025)

Abstrak

Perkembangan teknologi informasi yang pesat telah mendorong transformasi sistem keuangan menjadi lebih digital melalui inovasi *financial technology (fintech)*. Salah satu produk *fintech* yang populer di Indonesia adalah dompet digital, seperti aplikasi DANA. Namun, kemudahan transaksi digital ini juga menimbulkan kerentanan terhadap kejahatan siber *(cybercrime*) yang merugikan pengguna. Penelitian ini bertujuan untuk menganalisis bentuk pertanggungjawaban hukum terhadap tindak pidana siber dalam penggunaan dompet digital DANA, serta mengevaluasi efektivitas regulasi yang berlaku dalam melindungi konsumen. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan studi kasus. Data diperoleh melalui studi pustaka, dokumentasi, serta analisis kasus kejahatan siber yang terjadi pada aplikasi DANA. Hasil penelitian menunjukkan bahwa pelaku kejahatan siber dalam dompet digital dapat dikenai sanksi berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Perlindungan Konsumen serta peraturan lainnya. Namun, masih terdapat kelemahan dalam penegakan hukum, terutama dalam pelacakan pelaku dan pemberian ganti rugi kepada korban. Selain itu, perusahaan penyedia dompet digital juga memiliki tanggung jawab untuk meningkatkan sistem keamanan dan transparansi perlindungan data pengguna. Kesimpulannya, pertanggungjawaban hukum terhadap kejahatan *cyber* dalam dompet digital belum sepenuhnya efektif, dan diperlukan sinergi antara regulator, aparat penegak hukum, serta pelaku industri *fintech* dalam menciptakan ekosistem keuangan digital yang aman dan terpercaya.

Kata Kunci: Kejahatan Siber, Dompet Digital, Pertanggungjawaban Hukum

A. Pendahuluan

Het recht hinkt achter de feiten aan (Hukum tertatih-tatih mengikuti perkembangan zaman). sebuah adagium klasik dalam ilmu hukum, menggambarkan realitas bahwa hukum sering kali tertinggal dalam merespons dinamika masyarakat yang terus bergerak cepat. Namum dibalik itu semua Hukum harus tetap memjamin tujuan Hukum itu sendiri sebagaimana dikemukakan oleh Gustav Radbruch yaitu untuk keadilan, kepastian dan kemanfaatan dalam bukunya einführung *in die rechtswissenschaften.*

Perkembangan teknologi finansial *(fintech)* di Indonesia telah membawa perubahan signifikan dalam sistem pembayaran dan transaksi keuangan. Salah satu inovasi yang paling menonjol adalah dompet digital, seperti DANA, yang memudahkan pengguna dalam melakukan transaksi non-tunai secara praktis dan efisien. Namun, seiring dengan kemajuan teknologi, muncul pula berbagai risiko keamanan siber yang mengancam data pribadi dan dana pengguna. Kasus-kasus seperti *phishing*, *hacking*, dan penyalahgunaan data pribadi semakin marak terjadi, menimbulkan kerugian meteril dan immateril bagi pengguna.[1]

Menurut data, serangan siber di Indonesia mencapai angka yang mencengangkan, yakni rata-rata 13.733.440 serangan siber per hari, atau 158 serangan per detik.[2] Fenomena ini mengindikasikan betapa rapuhnya keamanan dalam transaksi digital di Indonesia. Kejadian seperti pembobolan dana nasabah pada *platform* dompert digital, Termasuk DANA, hal ini menunjukkan adanya celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan tindakan kriminal.

Dalam menghadapi ancaman tersebut DANA telah mengambil langkah proaktif dengan mengembangkan fitur keamanan, seperti Dana *Protetion*, yang mencakup autentikasi pengguna dan perlindungan transaksi. Selain itu, DANA juga berencana menambahkan fitur edukasi terkait serangan siber, *scam*, dan *phishing* untuk meningkatkan kesadaran pengguna. Upaya menunjukkan komitmen DANA dalam melindungi pengguna dari potensi ancaman siber.

Namun, upaya perlindungan dari penyelenggara dompet digital saja tidak cukup. Perlindungan hukum terhadap pengguna juga menjadi aspek penting yang perlu diperhatikan. Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) telah

[1] ELVI CHAERANI, "Penerapan Peraturan Perlindungan Konsumen Terhadap Kasus Cyber Crime Dalam Transaksi Non-Tunai Menggunakan Dompet Digital." (Universitas Pelita Harapan, 2024).

[2] Muhammad Fikrie. "Serangan Siber Ke RI Naik 6 Kali Lipat Pada H1 2024, Mayoritas Dari Dalam Negeri". tersedia di : https: www.kumparan.com. diakses tanggal 6 Mei 2025.

memberikan landasan hukum bagi perlindungan konsumen dalam pertanggungjawaban pidana korporasi penyelenggara *fintech*, terutama dalam kasus kejahatan siber yang melibatkan penyalahgunaan data pribadi pengguna.[3]

Selain itu, urgensi pembentukan Undang-Undang khusus mengenai *fintech* menjadi semakin jelas. Hal ini bertujuan untuk mengisi kekosongan hukum terkait pertanggungjawaban pidana korporasi dalam kasus kejahatan siber dan penyalahgunaan data pribadi. Dengan adanya regulasi yang jelas, diharapkan hak-hak konsumen dapat terlindungi dengan lebih baik, dan penyelenggara *fintech* memiliki pedoman yang tegas dalam mengelola data pengguna serta mencegah penyalahgunaan.

Dengan pendekatan yang komprehensif dan kolaboratif, diharapkan perlindungan dan pertanggungjawaban hukum terhadap kejahatan siber dalam dompet digital di era fintech, khususnya pada aplikasi DANA, dapat ditingkatkan. Hal ini tidak hanya akan melindungi hak-hak konsumen tetapi juga memperkuat ekosistem *fintech* Indonesia secara keseluruhan dan sesuai dengan tujuan hukum itu sendiri.

B. Metode Penelitian

Metode penelitian yang digunakan dalam penulisan jurnal ini adalah penelitian normatif, yang berfokus pada studi literatur dan analisis yuridis terhadap berbagai ketentuan peraturan perundang-undangan yang relevan dengan kejahatan siber dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 1 Tahun 2024 perubahan atas Undang-Undang Nomor 8 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Penelitian ini melibatkan pengumpulan data sekunder dari berbagai sumber, termasuk Undang-Undang, peraturan pelaksana, Buku, Jurnal ilmiah, artikel dan dokumen lainnya yang berkaitan dengan kejahatan siber. Tahapan penelitian dimulai dengan pengumpulan dan pengolahan data dari sumber-sumber hukum tersebut, dilanjutkan dengan analisis terhadap pertanggungjawaban hukum terhadap kejahatan *cyber* dalam dompet digital di era *fintech* pada aplikasi dana. Analisis ini juga didukung oleh pendapat ahli dan studi kasus yang memberikan gambaran yang komperensif mengenai isu yang dibahas.

C. Rumusan Masalah

1. Apa saja bentuk-bentuk kejahatan *cyber* yang sering terjadi pada aplikasi DANA?
2. Bagaimana perlindungan dan pertanggungjawaban Hukum apabila terjadi kejahatan c*yber* yang terjadi pada aplikasi DANA?

[3] ibid

D. Hasil dan Pembahasan

1. Bentuk-bentuk kejahatan *cyber* yang sering terjadi pada aplikasi DANA.

Cybercrime merupakan kejahatan atau tindakan kriminal yang menggunakan sistem komputer yang dilakukan secara online untuk perampokan dan kejahatan siber lainnya.[4] Kejahatan ini bersifat lintas waktu dan tidak mengenal batas target yang tentunya dapat menyerang siapa saja, kapan saja, dan di mana saja. Pelaku dari kejahatan siber ini biasa disebut sebagai *Hacker* atau *Cracker*, mereka melakukan hal tersebut dengan alasan yang beragam, seperti sekedar iseng, mencuri aset digital atau merusak sistem untuk keuntungan pribadi. Seiring dengan perubahan pola hidup di masyarakat yang kini serba digital, frekuensi dan jenis kejahatan siber atau *cybercrime* turut mengalami peninhkatan. Berikut beberapa bentuk umum dari tindak kejahatan siber, antara lain;

a. *unauthorized access*

Kejahatan siber yang dilakukan dengan cara mengakses sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan pemilik sistem tersebut.[5]

b. penyebaran virus secara sengaja

Penyebaran virus ini umumnya terjadi melalui email, di mana penerima sering kali tidak menyadari bahwa email tersebut mengandung ancaman. Setelah terinfeksi, virus tersebut secara otomatis menyebar ke alamat email lain melalui akun korban.

c. *illegal content*

Kejahatan siber ini dilakukan dengan mengunggah data atau informasi ke internet yang bersifat tidak akurat, tidak etis, menyesatkan, dan melanggar hukum karena dapat merugikan pihak lain serta mengganggu ketertiban umum. Contohnya adalah penyebaran konten pornografi.

d. *data forgery*

Merupakan bentuk kejahatan yang bertujuan memanipulasi atau memalsukan data dalam dokumen-dokumen penting yang tersedia secara daring (*online*). Dokumen-dokumen penting tersebut umumnya dimiliki oleh institusi atau lembaga yang mengelola situs berbasis basis data web.

e. *cyber espionage*

Kejahatan ini dilakukan dengan memanfaatkan jaringan internet untuk melakukan aktivitas pemantauan atau spionase terhadap pihak tertentu, dengan

[4] Siti Kurnia Rahayu et al., "Cybercrime Dan Dampaknya Pada Teknologi E-Commerce," *Journal of Information System, Applied, Management, Accounting and Research* 5, no. 3 (2021): 632.

[5] Christian Henry. Ratulangi, Dr. Anna S. Wahongan, and Franky R. Mewengkang, "Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan," *Lex Privatum* IX, no. 5 (2021): 179–87.

cara menyusup ke dalam sistem jaringan komputer milik target.

f. *cyberstalking*

Kejahatan siber ini dilakukan dengan tujuan mengganggu atau melecehkan individu tertentu melalui pemanfaatan perangkat komputer, seperti mengirim email secara berulang-ulang. *Cyberstalking* mirip dengan bentuk teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal ini dapat terjadi karena kemudahan dalam membuat alamat email tertentu tanpa perlu mencantumkan identitas asli.

g. *Carding*

Carding adalah jenis kejahatan yang dilakukan dengan mencuri nomor kartu kredit milik orang lain dan menggunakannya untuk transaksi jual beli di internet.[6]

Selain bentuk-bentuk umum *cybercrime* di atas, perlu disadari bahwa platform dompet digital seperti DANA juga menjadi sasaran empuk dalam praktik kejahatan ini. Banyak pelaku siber memanfaatkan kerentanan sistem dan kelengahan pengguna untuk melakukan tindakan penipuan atau pencurian data. Selain metode penipuan yang mengandalkan manipulasi terhadap perilaku pengguna, terdapat pula bentuk kejahatan lain yang menyasar platform seperti DANA melalui teknik eksploitasi sistem demi mendapatkan akses tidak sah ke akun atau informasi pengguna. Dua teknik yang sering digunakan antara lain;

a. *phising*

Merupakan metode penipuan yang dilakukan dengan menipu korban untuk mencuri akun mereka. Istilah "*phishing*" berasal dari kata "*fishing*", yang berarti "memancing" korban untuk terjebak dalam perangkap penipuan. *Phishing* dapat dianggap sebagai upaya pencurian informasi penting dengan cara mengakses akun korban untuk tujuan tertentu. [7]

b. *Hacking*

Merupakan metode yang digunakan oleh hacker atau cracker untuk menyerang jaringan, sistem, dan aplikasi dengan memanfaatkan kelemahan atau kerentanannya, dengan tujuan untuk memperoleh akses terhadap data dan sistem. Istilah "*Hacking*" dalam konteks keamanan informasi merujuk pada upaya menyerang kerentanannya dalam suatu sistem, yang mengancam keamanan dengan tujuan memperoleh akses dan kontrol ilegal atas sumber daya sistem.

[6] Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime*, ed. Gedeon Soerja (Malang: Media Nusa Creative, 2018).

[7] Azani Cempaka Sari, "PengenalanTeknologi Informasi : Mengenal Apa Itu Phising Penyebab, Dan Mengatasinya," Binus University School of Computer Science, 2018.

Tujuan dari *hacking* ini meliputi modifikasi sumber daya sistem, mengganggu fitur dan layanan, dengan tujuan untuk mencapai sasaran tertentu. [8]

Lebih lanjut, berbagai modus penipuan digital yang mengatasnamakan DANA juga banyak ditemukan dan patut diwaspadai. Beberapa di antaranya adalah;

a. oknum yang mengatasnamakan dana

Maraknya penipuan digital melalui media sosial ditandai dengan adanya pihak-pihak tidak bertanggung jawab yang menyamar sebagai *customer service* (CS) DANA untuk menawarkan bantuan terkait permasalahan transaksi. Apabila pengguna mengalami kendala, sangat disarankan untuk menghubungi layanan resmi DANA melalui fitur DIANA yang tersedia di aplikasi. Selain itu, pengguna juga perlu meningkatkan kewaspadaan terhadap pesan atau panggilan yang mengatasnamakan DANA. Penting untuk memverifikasi terlebih dahulu keaslian akun media sosial, nomor telepon, maupun alamat email yang digunakan untuk menghubungi. Informasi kontak resmi DANA dapat dicek langsung melalui kanal resmi perusahaan. Perlu diperhatikan pula bahwa akun WhatsApp resmi DANA hanya digunakan untuk pengiriman informasi satu arah dari pihak DANA kepada pengguna, dan tidak dapat menanggapi pesan maupun keluhan.

b. link dana kaget palsu

Fitur DANA Kaget sering kali dimanfaatkan sebagai sarana penipuan oleh oknum tidak bertanggung jawab yang menyebarkan tautan palsu dengan mengatasnamakan DANA. Meskipun fitur ini dirancang untuk memberikan keuntungan atau kejutan kepada pengguna, terdapat risiko keamanan apabila pengguna tidak waspada terhadap keaslian tautan yang diterima. Tautan palsu tersebut kerap kali menjadi media untuk mencuri informasi sensitif seperti *Personal Identification Number* (PIN) dan kode *One Time Password* (OTP). Oleh karena itu, penting bagi pengguna untuk selalu memastikan bahwa tautan DANA Kaget yang diakses berasal dari sumber resmi yang dikeluarkan oleh DANA Indonesia.

c. link palsu untuk memulihkan akun yang dibekukan

Salah satu modus penipuan yang marak terjadi adalah pesan langsung dari pihak tidak dikenal yang mengklaim bahwa akun DANA pengguna telah dibekukan. Pelaku kemudian

[8] Ahmad Ridha Kelrey and Aan Muzaki, "Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan," *Cyber Security Dan Forensik Digital* 2, no. 2 (2019): 77–81.

membujuk korban untuk mengklik tautan pemulihan akun yang sebenarnya merupakan link palsu dengan tujuan mencuri data pribadi. Untuk menghindari risiko kebocoran data, pengguna disarankan untuk tidak langsung mempercayai pesan semacam itu dan melakukan verifikasi secara mandiri terkait status akun mereka. Apabila ditemukan bahwa akun benar-benar dibekukan, langkah yang tepat adalah segera menghubungi layanan resmi DANA melalui fitur DIANA yang tersedia dalam aplikasi.

d. kartu fisik dana palsu

Munculnya informasi palsu yang menyebutkan bahwa DANA mengeluarkan kartu ATM fisik merupakan bentuk lain dari modus penipuan yang bertujuan untuk menyesatkan pengguna. Perlu ditegaskan bahwa hingga saat ini, DANA tidak pernah menerbitkan kartu fisik dalam bentuk apa pun. Sebagai dompet digital, DANA beroperasi melalui aplikasi dan menjalin kemitraan dengan berbagai bank di Indonesia untuk mendukung layanan transaksinya. Dengan demikian, penting bagi pengguna untuk tetap waspada terhadap berbagai bentuk penipuan digital yang mengatasnamakan DANA. Mengenali berbagai modus yang beredar menjadi langkah preventif untuk memastikan keamanan serta kenyamanan dalam bertransaksi secara digital.[9]

2. Perlindungan dan Pertanggung jawaban Hukum apabila terjadi kejahatan *cyber* yang terjadi pada aplikasi DANA.

Perlindungan hukum dapat dipahami melalui dua aspek, yakni perlindungan dan hukum. Perlindungan merujuk pada tindakan atau upaya untuk memberikan rasa aman, sementara hukum diartikan sebagai seperangkat aturan yang bersifat mengikat dan memiliki kekuatan memaksa. Perlindungan hukum adalah usaha yang dilakukan oleh pemerintah atau pihak berwenang untuk memastikan dan melindungi hak-hak masyarakat melalui peraturan hukum yang berlaku. Unsur-unsur dalam perlindungan hukum meliputi tindakan yang bertujuan untuk memberikan perlindungan, pihak yang berperan dalam memberikan perlindungan, serta mekanisme atau metode yang digunakan dalam proses perlindungan tersebut.[10]

Memberikan perlindungan kepada masyarakat merupakan salah satu tujuan utama dari hukum.

[9] DANA. "Awas Jebakan Badman! Yuk, Cek Berbagai Modus Penipuan" tersedia di : https: www.dana.id. diakses tanggal 6 Mei 2025.

[10] Fiona Pappano Naomi and I Made Dedy Priyanto, "Perlindungan Hukum Pengguna E-Wallet Dana Ditinjau Dari Undang-Undang Perlindungan Konsumen," *Kertha Semaya : Journal Ilmu Hukum* 9, no. 1 (2020): 24.

Hukum berfungsi sebagai alat utama untuk mengatur dan mengendalikan dinamika perubahan dalam masyarakat, sehingga perubahan tersebut dapat diarahkan untuk mendukung kemajuan dan pembangunan bangsa serta negara ke arah yang lebih positif. Undang-undang berperan dalam memberikan landasan untuk pemanfaatan ilmu pengetahuan dan teknologi secara optimal demi kepentingan dan keberlangsungan hidup manusia. Dalam konteks transaksi elektronik, hukum bertujuan untuk memberikan perlindungan kepada konsumen.[11]

DANA, sebagai aplikasi yang menyediakan berbagai kemudahan, telah menjadi salah satu E-Wallet pilihan utama di tengah masyarakat. Melalui satu aplikasi, pengguna dapat melakukan berbagai jenis pembayaran seperti listrik, air, pulsa, layanan hiburan, dan lainnya. Meskipun menawarkan berbagai kemudahan dan keunggulan, aplikasi E-Wallet DANA masih memiliki potensi untuk menimbulkan kerugian bagi penggunanya. Kerugian yang dapat terjadi bisa berupa kerugian finansial maupun non-finansial. Contoh kerugian material yang dapat terjadi akibat penggunaan aplikasi DANA meliputi berkurangnya saldo pengguna secara tiba-tiba tanpa ada transaksi yang dilakukan, atau saldo yang terpotong saat proses transfer namun tidak terkirim ke akun atau rekening tujuan. Sementara itu, contoh kerugian non-material biasanya berkaitan dengan rasa ketidakpuasan atau ketidaknyamanan terhadap layanan yang diberikan oleh penyedia DANA, seperti akibat respons yang lambat.[12]

DANA tidak hanya memberikan kemudahan, tetapi juga menyediakan berbagai diskon atau promo menarik bagi pelanggannya. Meskipun aplikasi DANA memiliki banyak keunggulan, masih banyak pengguna dompet digital (e-wallet) yang mengalami kerugian, seperti DANA yang diretas atau dibajak oleh pihak yang tidak bertanggung jawab. Akibatnya, pengguna tidak hanya kehilangan saldo, tetapi juga data pribadi mereka yang telah tersebar.

Akibat kejadian ini, banyak pengguna merasa kecewa karena pelayanan customer care DANA yang sangat lambat, atau meskipun ada tanggapan dari pihak DANA, tidak ada tindakan nyata untuk menyelesaikan masalah yang dihadapi oleh pengguna. Akibat hal tersebut, pengguna yang awalnya merasa bahwa aplikasi DANA memudahkan mereka untuk melakukan transaksi dengan aman dan nyaman, kini menjadi kehilangan kepercayaan, dan

[11] Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono, "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia," *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (2019): 145–60.

[12] Hartanto Hartanto, Vincent Rosadi, and Ervin Alvaro Yosmar, "Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana," *PATTIMURA Legal Journal* 2, no. 3 (2023): 267–79.

minat untuk menggunakan aplikasi e-wallet DANA pun berkurang.

Pengesahan Undang-Undang Perlindungan Konsumen ini didorong oleh kesadaran akan posisi konsumen yang cenderung lemah dalam transaksi jual beli barang atau jasa. Undang-Undang Perlindungan Konsumen berfungsi sebagai dasar hukum yang mengintegrasikan dan memperkuat penegakan hukum di bidang perlindungan konsumen. Di samping itu, masih ada kemungkinan untuk terbentuknya undang-undang baru yang mengatur ketentuan-ketentuan yang bertujuan melindungi konsumen. Perlindungan konsumen sangat penting untuk memastikan pemenuhan hak-hak yang diterima oleh seluruh masyarakat Indonesia, khususnya sebagai konsumen pengguna e-wallet.

Dalam konteks perlindungan hukum, terdapat dua jenis perlindungan yang diberikan kepada konsumen, yaitu perlindungan preventif dan perlindungan represif. Perlindungan hukum preventif adalah langkah-langkah yang diambil untuk mencegah terjadinya peristiwa yang memiliki akibat hukum, sementara perlindungan hukum represif adalah tindakan yang dilakukan setelah peristiwa yang memiliki akibat hukum tersebut terjadi. Bentuk perlindungan hukum preventif dalam Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen dapat ditemukan dalam beberapa pasal.[13]

Pertama, penyelenggara e-wallet diwajibkan untuk memberikan informasi yang akurat, jelas, dan jujur mengenai layanan sistem pembayaran, termasuk risiko kehilangan saldo dan pencurian data, sebagaimana diatur dalam Pasal 7 UUPK. Kedua, penyelenggara e-wallet dan pihak terkait harus memberikan edukasi kepada konsumen mengenai cara penggunaan dompet digital (e-wallet) yang aman, tips untuk menghindari penipuan, serta pentingnya menjaga kerahasiaan data pribadi, sebagaimana diatur dalam Pasal 4 UUPK. Sementara itu, bentuk perlindungan hukum represif dapat ditemukan dalam Pasal 45 dan Pasal 19 UUPK. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen juga mengatur hak-hak konsumen, termasuk hak untuk memperoleh kenyamanan dan keamanan dalam menggunakan barang dan/atau jasa, serta hak untuk menerima kompensasi, sebagaimana diatur dalam Pasal 4 Huruf (a). Selain itu, Pasal 4 Huruf (d) juga mengatur "hak untuk menyampaikan pendapat dan mengajukan keluhan terkait barang dan/atau jasa yang digunakan".[14]

Peraturan ini memberikan kesempatan kepada pengguna e-

[13] Amadea G. G. Watupongoh, Dientje Rumimpunu and Sarah D.L. Roeroe, "TINJAUAN HUKUM TERHADAP PERLINDUNGAN KONSUMEN BAGI PENGGUNA E-WALLET DI INDONESIA" *Lex Privatum Jurnal Fakultas Hukum Unsrat* , Vol. 15, no. 3 (2025): 1–23.

[14] Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, *Peraturan Pemerintah Republik Indonesia*, no. 1 (1999): 1–46.

wallet untuk mengajukan keluhan atau menyampaikan kekurangan terkait layanan yang diberikan oleh dompet digitall. Sebagai timbal balik, para pelaku usaha, dalam hal ini penyelenggara e-wallet, memiliki kewajiban untuk menanggapi pendapat atau keluhan dari konsumen mereka.[15]

Seperti e-wallet lainnya, e-wallet DANA bertanggung jawab secara hukum untuk menjaga keamanan transaksi, menjaga data pengguna, dan mematuhi undang-undang perlindungan konsumen dan perbankan. Pengguna dapat menempuh jalur hukum untuk mendapatkan ganti rugi jika kesalahan atau kelalaian DANA mengakibatkan kerugian.

1) Persyaratan Perlindungan Data: Sesuai dengan Undang-Undang Perlindungan Data Pribadi (UU PDP), DANA secara hukum diwajibkan untuk melindungi privasi dan informasi pribadi pengguna. Ini mencakup kewajiban untuk memastikan bahwa informasi pengguna disimpan dengan aman dan hanya digunakan dengan persetujuan yang sah.
2) Kewajiban Keamanan Transaksi: DANA bertanggung jawab untuk menjamin bahwa setiap transaksi yang dilakukan melalui aplikasinya aman. Ini termasuk menerapkan fitur keamanan teknis termasuk deteksi penipuan, enkripsi data, dan verifikasi transaksi yang tepat.
3) Kewajiban untuk Mematuhi Peraturan: Karena DANA merupakan e-wallet, maka DANA wajib mematuhi seluruh undang-undang perbankan dan keuangan yang berlaku, seperti yang berkaitan dengan perlindungan konsumen, pencegahan penipuan, anti pencucian uang, dan identifikasi pelanggan.
4) Tanggung Jawab atas Kerugian: Pengguna dapat mengajukan ganti rugi melalui sistem hukum sesuai dengan Undang-Undang Perlindungan Konsumen yang berlaku jika pengguna mengalami kerugian akibat menerima layanan yang tidak sesuai atau kesalahan yang dilakukan oleh DANA.
5) Tanggung Jawab atas Wanprestasi: Pengguna berhak atas penggantian kerugian mereka jika DANA dianggap wanprestasi, yang berarti tidak memenuhi tanggung jawabnya.
6) Kompensasi: Mereka harus segera mengganti rugi kepada pengguna jika terjadi kehilangan saldo sebagai akibat dari kesalahan DANA atau sistem.

Sebagai e-wallet, DANA tunduk pada sejumlah kewajiban hukum, termasuk menjaga keamanan informasi pengguna, memastikan

[15] Zahra Kamila and Rahmad Efendi, "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, no. 2 (2023): 7187–88.

keamanan transaksi, dan mematuhi undang-undang perbankan. Pengguna yang menderita kerugian akibat kesalahan DANA dapat mengajukan tuntutan ganti rugi ke pengadilan.

Produsen atau yang disebut juga dengan pelaku usaha tunduk pada ketentuan dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Berikut ini adalah ketentuannya. Menurut Pasal 19, pelaku usaha secara umum mempunyai kewajiban sebagai berikut;

1) Pelaku usaha wajib mengganti kerugian konsumen, pencemaran, dan kerugian yang ditimbulkan akibat pemanfaatan barang dan/atau jasa yang diproduksi atau diperjualbelikan.
2) Pelaku usaha wajib memberikan kompensasi sebagaimana diatur dalam ayat (1), yang dapat berupa penggantian atau penukaran barang atau jasa dengan yang sejenis atau identik.
3) Setelah tanggal transaksi, ganti rugi diberikan dalam jangka waktu paling lama 7 (tujuh) hari.
4) Pemberian ganti rugi sebagaimana diatur dalam ayat (1) dan ayat (2) tidak menghalangi kemungkinan adanya tuntutan pidana jika terdapat bukti tambahan yang menunjukkan unsur kesalahan.
5) Jika pelaku usaha dapat membuktikan bahwa kesalahan tersebut disebabkan oleh konsumen, maka ketentuan yang tercantum dalam ayat (1) dan ayat (2) tidak berlaku. "Pelaku usaha yang menolak atau tidak memenuhi tuntutan ganti rugi dari konsumen sebagaimana diatur dalam Pasal 19 ayat (1), ayat (2), ayat (3), dan ayat (4) dapat digugat melalui Badan Penyelesaian Sengketa Konsumen atau dibawa ke badan peradilan di tempat tinggal konsumen",[16] apabila pelaku usaha tidak bersedia bertanggung jawab sebagaimana dimaksud dalam Pasal 23. Dalam Pasal 23 tersebut jelas disebutkan bahwa konsumen dapat menggunakan perlindungan konsumen untuk menggugat produsen atau badan usaha.[17]

Menurut Pasal 1 angka 2 UU ITE No. 19 Tahun 2016, transaksi elektronik adalah tindakan hukum yang dilakukan dengan memanfaatkan komputer, jaringan komputer, atau media elektronik lainnya. Hubungan antara UU ITE dan dompet elektronik diatur dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Berdasarkan definisi pasal tersebut, transaksi elektronik adalah setiap pertukaran informasi yang terjadi melalui jaringan elektronik. Dompet elektronik, atau e-wallet, adalah konsep yang berbeda dari uang elektronik jika dibandingkan dengan

[16] *ibid*

[17] Watupongoh, Amadea GG, Dientje Rumimpunu, and Sarah DL Roeroe. "TINJAUAN HUKUM TERHADAP PERLINDUNGAN KONSUMEN BAGI PENGGUNA E-WALLET DI INDONESIA." LEX PRIVATUM 15.3 (2025).

konsep tradisional.[18] Dengan kata lain, jika uang berupa elektronik, maka dompetnya pun berbentuk digital. Berdasarkan pengertian tradisional, e-wallet memiliki konsekuensi hukum dan tanggung jawab yang berbeda yang harus dipahami. UU ITE No. 11 Tahun 2008 Pasal 21 Ayat 4 menyatakan bahwa pengguna jasa bertanggung jawab atas segala akibat hukum jika terjadi kegagalan fungsi agen elektronik sebagai akibat dari kecerobohan pengguna jasa. Akibatnya, penyelenggara wajib mengganti kerugian yang dialami pengguna jasa.

E. Kesimpulan

1. Kejahatan siber merupakan bentuk tindak kriminal modern yang dilakukan melalui jaringan internet, seperti pencurian data, perusakan sistem, hingga penipuan digital. Kejahatan ini bersifat lintas batas, tidak terikat lokasi maupun waktu, dan dapat menimpa siapa saja. Jenis-jenis umum *cybercrime* mencakup akses tanpa izin, penyebaran virus, konten ilegal, pemalsuan data, spionase siber, penguntitan daring, serta pencurian data kartu (*carding*). Dengan pesatnya perkembangan teknologi digital dan meningkatnya penggunaan platform seperti dompet digital DANA, pelaku kejahatan juga makin canggih dalam mencari celah keamanan dan menipu pengguna. Modus yang sering terjadi antara lain phishing, peretasan akun, penyamaran sebagai pihak resmi DANA, penyebaran tautan palsu seperti DANA Kaget, link pemulihan akun yang menyesatkan, dan informasi palsu terkait kartu fisik DANA. Oleh karena itu, penting bagi setiap pengguna untuk meningkatkan kewaspadaan, mengenali berbagai modus penipuan digital, serta selalu memverifikasi informasi dari sumber resmi demi menjaga keamanan data dan kenyamanan transaksi.
2. Perlindungan hukum bagi konsumen dompet digital seperti DANA bertujuan untuk menjamin keamanan, kenyamanan, dan hak-hak pengguna dalam transaksi elektronik. Perlindungan ini mencakup upaya preventif seperti penyediaan informasi, edukasi, dan sistem keamanan serta upaya represif melalui pengaduan, ganti rugi, dan proses hukum jika terjadi pelanggaran. Meski DANA memudahkan transaksi dan menawarkan berbagai promo, risiko tetap ada, seperti kehilangan saldo atau kebocoran data. Oleh karena itu, DANA wajib mematuhi regulasi seperti UU Perlindungan Konsumen, UU ITE, dan UU Perlindungan Data Pribadi, termasuk memberikan kompensasi dan

[18] Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 perubahan atas Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

menjaga kerahasiaan data. Jika kewajiban ini dilanggar, konsumen berhak menuntut melalui BPSK atau pengadilan. Penting bagi penyedia layanan untuk menaati hukum dan bagi konsumen untuk memahami haknya demi transaksi digital yang aman dan adil.

F. Saran

Saran penulis, perusahaan dompet digital seperti DANA sebaiknya membuka kantor cabang fisik di berbagai daerah untuk memudahkan masyarakat mengajukan pengaduan secara langsung atas kasus kejahatan siber yang mereka alami, mengingat layanan digital seperti *chatbot* masih sering terkendala. Di sisi lain, penulis merekomendasikan agar pemerintah memperkuat regulasi dan pengawasan terhadap penyedia layanan keuangan digital, termasuk memastikan adanya perlindungan hukum yang jelas bagi konsumen, membentuk mekanisme pengaduan yang cepat dan terpadu, serta mendorong program edukasi dan literasi digital guna meningkatkan kesadaran masyarakat mengenai risiko dan upaya pencegahan kejahatan siber.

Daftar Pustaka

A. Undang-Undang

Indonesia. *Undang-Undang tentang Perlindungan Konsumen*. UU Nomor 8 Tahun 2009. LN No. 42 Tahun 1999. TLN No. 3821.

Indonesia. *Undang-Undang tentang Informasi dan Transaksi Elektronik*. UU Nomor 1 Tahun 2024 perubahan atas UU Nomor 11 Tahun 2008. LN No.1 Tahun 2024. TLN No. 6905.

B. Buku

Yurizal. *Penegakan Hukum Tindak Pidana Cyber Crime*. Malang: Media Nusa Creative, 2018.

C. Jurnal

Benuf, Kornelius; Siti Mahmudah; dan Ery Agus Priyono. "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia". *Refleksi Hukum: Jurnal Ilmu Hukum*. Vol. 3 No.2 Tahun 2019.

Amadea G. G. Watupongoh; Dientje Rumimpunu; dan Sarah D.L. Roeroe. "Tinjauan Hukum Terhadap Perlindungan Konsumen Bagi Pengguna E-Wallet Di Indonesia". *Lex Privatum Jurnal Fakultas Hukum Unsrat* . Vol. 15 No.3 Tahun 2025.

Chaerani, Elvi. "Penerapan Peraturan Perlindungan Konsumen Terhadap Kasus Cyber Crime Dalam Transaksi Non-Tunai Menggunakan Dompet Digital". *Jurnal Universitas Pelita Harapan*. Tahun 2024.

Hartanto, Hartanto; Vincent Rosadi; dan Ervin Alvaro Yosmar. "Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana". *PATTIMURA Legal Journal* Vol. 2 No.3 Tahun 2023.

Kamila, Zahra; dan Rahmad Efendi. "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*. Vol. 6 No.2 Tahun 2023.

Kelrey, Ahmad Ridha; dan Aan Muzaki. "Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan". *Cyber Security Dan Forensik Digital*. Vol. 2 No.2 Tahun 2019.

Naomi, Fiona Pappano; dan I Made Dedy Priyanto. "Perlindungan Hukum Pengguna E-Wallet Dana Ditinjau Dari Undang-Undang Perlindungan Konsumen". *Kertha Semaya : Journal Ilmu Hukum*. Vol. 9 No.1 Tahun 2020.

Rahayu, Siti Kurnia et al. "Cybercrime Dan Dampaknya Pada Teknologi E-Commerce". *Journal of Information System, Applied, Management, Accounting and Research*. Vol. 5 No.3 2021.

Ratulangi, Christian Henry; Anna S. Wahongan; dan Franky R. Mewengkang. "Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan". *Lex Privatum* Vol. 9 No.5 Tahun 2021.

Sari, Azani Cempaka. "PengenalanTeknologi Informasi : Mengenal Apa Itu Phising Penyebab, Dan Mengatasinya". *Binus University School of Computer Science*. Tahun 2018.

D. Internet

DANA. "Awas Jebakan Badman! Yuk, Cek Berbagai Modus Penipuan" tersedia di : https: www.dana.id. diakses tanggal 6 Mei 2025.

Fikrie, Muhammad. "Serangan Siber Ke RI Naik 6 Kali Lipat Pada H1 2024, Mayoritas Dari Dalam Negeri". tersedia di : https: www.kumparan.com. diakses tanggal 6 Mei 2025.