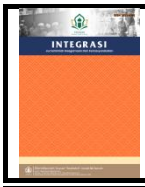

INTEGRASI : Jurnal Ilmiah Keagamaan dan Kemasyarakatan
E-ISSN : 3025-6941
Vol. 3, No. 2, Juli - Desember 2025
https://husin.id/index.php/integrasi/index
DOI : 10.61590/int.v3i02.199

PERLINDUNGAN DATA PRIBADI PENGGUNA APLIKASI DANA DARI KEJAHRAN SIBER BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022

Maharani Bintang[1], Asti Sri Mulyanti[2]

[1,2] Universitas Muhammadiyah Sukabumi
maharanibintang118@ummi.ac.id[1], astisri@ummi.ac.id[2]

ARTICLE INFO

Article History

Published : 30 Sep 2025

Keywords

Perlindungan Data Pribadi, Aplikasi Dana, Kejahatan Siber, UU Nomor 27 Tahun 2022, E-Wallet.

Personal Data Protection, Dana Application, Cybercrime, Law Number 27 Of 2022, E-Wallets.

ABSTRACT

Pesatnya adopsi e-wallet di Indonesia membawa kemudahan transaksi digital, namun belum diimbangi dengan perlindungan data pribadi yang memadai. Kondisi ini menyebabkan meningkatnya risiko kejahatan siber, seperti pencurian identitas dan kebocoran informasi sensitif pengguna. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap data pribadi pengguna aplikasi Dana dari kejahatan siber berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dengan semakin meningkatnya penggunaan dompet digital, risiko kejahatan siber pun turut berkembang. Metode yang digunakan dalam penelitian ini adalah yuridis normatif, dengan pendekatan deskriptif kualitatif. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap data pribadi telah diatur secara komprehensif dalam UU PDP, namun dalam praktiknya masih menghadapi berbagai kendala, seperti rendahnya literasi digital pengguna, sulitnya akses data pelaku, dan belum optimalnya kerja sama antara penyedia layanan dan aparat penegak hukum.

The rapid adoption of e-wallets in Indonesia has brought convenience to digital transactions, but has not been matched by adequate personal data protection. This situation has led to an increased risk of cybercrime, such as identity theft and the leakage of sensitive user information. This study aims to analyze the legal protection of Dana app users' personal data from cybercrime based on Law Number 27 of 2022 concerning Personal Data Protection. With the increasing use of digital wallets, the risk of cybercrime also increases. The method used in this study is normative juridical, with a qualitative descriptive approach. The results show that legal protection of personal data is comprehensively regulated in the Personal Data Protection Law (PDP), but in practice, it still faces various obstacles, such as low user digital literacy, difficult access to perpetrator data, and suboptimal cooperation between service providers and law enforcement officials.

PENDAHULUAN

Transformasi digital di Indonesia telah membawa perubahan signifikan dalam berbagai aspek kehidupan. Salah satu perubahan yang paling mencolok adalah dalam sistem pembayaran. [1] Dengan kemajuan teknologi, masyarakat kini semakin beralih dari transaksi tradisional menggunakan uang tunai ke transaksi digital yang lebih efisien dan praktis. Di antara berbagai inovasi yang muncul, penggunaan dompet digital atau e-wallet menjadi salah satu yang paling menonjol. E-wallet memungkinkan pengguna untuk melakukan berbagai transaksi, termasuk pembayaran, transfer dana, dan pembelian barang, tanpa perlu membawa uang tunai. Salah satu aplikasi e-wallet yang terkemuka di Indonesia adalah Dana, yang telah menjadi pilihan utama bagi jutaan masyarakat untuk memenuhi kebutuhan transaksi sehari-hari.[2]

Namun, pesatnya pertumbuhan e-wallet ini tidak lepas dari tantangan yang signifikan, terutama yang berkaitan dengan keamanan. Di tengah kemudahan yang ditawarkan oleh teknologi ini, meningkatnya kejahatan siber muncul sebagai ancaman serius yang dapat merugikan pengguna secara finansial dan emosional. Kejahatan siber, seperti phishing, pencurian identitas, dan rekayasa sosial, sering kali terjadi akibat kebocoran data pribadi yang dapat terjadi melalui berbagai saluran, baik itu melalui serangan malware, teknik manipulasi psikologis, atau kelalaian pengguna dalam menjaga informasi sensitif mereka.[3]

Data pribadi, yang mencakup informasi seperti nama, alamat, nomor telepon, dan data keuangan, merupakan aset yang sangat penting dalam ekosistem digital saat ini. Ketika data ini jatuh ke tangan yang salah, potensi yang mendasarinya sangat besar, mulai dari penipuan finansial hingga identitas yang dapat merusak reputasi individu. Misalnya, informasi yang diambil oleh penjahat siber dapat digunakan untuk melakukan transaksi ilegal atau membuka akun baru atas nama korban, yang dapat menimbulkan kerugian finansial dan emosional yang signifikan. Perlindungan data pribadi bukan hanya sekedar aspek teknis, tetapi juga sebuah isu etis yang harus diperhatikan oleh semua pihak yang terlibat dalam ekosistem digital. Penyedia layanan perlu menerapkan langkah-langkah keamanan yang kuat dan transparan, sementara pengguna harus diberi pengetahuan yang cukup tentang cara melindungi data mereka sendiri. Regulator juga memiliki peran penting dalam menetapkan kebijakan yang jelas dan tegas untuk melindungi hak-hak individu serta memastikan bahwa pelanggaran terhadap data pribadi mendapatkan konsekuensi

[1] Anwar, R., Gaffar, V., Disman, D., Furqon, C., & Sutisnawati*, Y., 2023. Mobile wallet adoption model among digital immigration generation in Indonesia. Journal of Eastern European and Central Asian Research (JEECAR). https://doi.org/10.15549/jeecar.v10i6.1499.

[2] Langford, B., Chen, J., & Cherry, C., 2015. Risky riding: Naturalistic methods comparing safety behavior from conventional bicycle riders and electric bike riders.. Accident; analysis and prevention, 82, pp. 220-6 . https://doi.org/10.1016/j.aap.2015.05.016.

[3] Arindy and A. Suzianti. "Multi-Generation Perception Towards Digital Wallet in Indonesia." Proceedings of the 3rd Asia Pacific Conference on Research in Industrial and Systems Engineering (2020). https://doi.org/10.1145/3400934.3400940.

yang sesuai. Dengan pendekatan yang holistik dan kolaboratif, perlindungan data pribadi dapat menjadi prioritas utama, menciptakan lingkungan digital yang lebih aman dan bertanggung jawab bagi semua pengguna.[4]

Oleh karena itu, perlindungan data pribadi menjadi isu yang krusial di era digital ini. Masyarakat perlu diberikan edukasi mengenai cara melindungi data pribadi mereka, termasuk mengenali tanda-tanda kejahatan siber dan langkah-langkah yang dapat diambil untuk mengurangi risiko. Selain itu, penyedia layanan e-wallet juga memiliki tanggung jawab untuk menerapkan langkah-langkah keamanan yang ketat, seperti enkripsi data dan autentikasi dua faktor, guna melindungi informasi pengguna. Dengan pendekatan yang komprehensif ini, diharapkan pengguna dapat merasa lebih aman dan terlindungi dalam melakukan transaksi digital, serta kepercayaan terhadap e-wallet dapat terus tumbuh.[5]

Dalam konteks ini, peran negara sangat penting untuk memberikan perlindungan hukum kepada masyarakat, terutama di tengah meningkatnya ancaman kejahatan siber yang dapat membahayakan data pribadi. Negara tidak hanya berfungsi sebagai pengatur, namun juga sebagai pelindung hak individu dalam ekosistem digital yang semakin kompleks. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai respon yang mendesak terhadap kebutuhan regulasi yang komprehensif untuk menjamin keamanan data pribadi di era digital.[6]

Undang-Undang Perlindungan Data Pribadi ini memberikan kerangka hukum yang jelas dalam melindungi hak-hak individu terkait data pribadi, termasuk hak untuk mengetahui, mengakses, dan memperbaiki data pribadi yang dikelola oleh pihak ketiga. Dengan adanya undang-undang ini, individu memiliki landasan hukum yang kuat untuk menuntut pertanggungjawaban jika data mereka disalahgunakan atau dibocorkan. Hak untuk mengetahui memungkinkan individu untuk mendapatkan informasi mengenai bagaimana dan untuk data apa yang mereka gunakan, sehingga meningkatkan transparansi dalam pengelolaan data. Sementara itu, hak untuk mengakses memberikan kesempatan bagi individu untuk memeriksa informasi yang dimiliki oleh penyedia layanan dan memastikan keakuratan data tersebut. Hak untuk memperbaiki data pribadi juga sangat penting, mengingat kesalahan dalam informasi dapat berdampak serius pada reputasi dan keputusan yang diambil berdasarkan data tersebut.[7]

---

[4] Ciptarianto, A., 2022. E-Wallet Application Penetration for Financial Inclusion in Indonesia. International Journal of Current Science Research and Review. https://doi.org/10.47191/ijcsrr/v5-i2-03.

[5] Firdaus, T., & Lubis, M., 2022. Comparative Analysis of Popular Electronic Wallets in Indonesia in Daily Life Selection. Proceedings of the 8th International Conference on Industrial and Business Engineering. https://doi.org/10.1145/3568834.3568865.

[6] Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

[7] Morić, Z., Dakić, V., Djekic, D., & Regvart, D., 2024. Protection of Personal Data in the Context of E-Commerce. J. Cybersecur. Priv., 4, pp. 731-761. https://doi.org/10.3390/jcp4030034.

Lebih jauh lagi, undang-undang ini juga membentuk dasar bagi penegakan hukum yang lebih tegas terhadap pelanggaran, dengan sanksi bagi pihak yang tidak mematuhi ketentuan perlindungan data. Hal ini menciptakan rasa aman bagi individu, yang merasa bahwa hak-hak mereka dilindungi dan bahwa ada saluran hukum yang dapat diakses jika terjadi pelanggaran. Dengan demikian, undang-undang ini tidak hanya berfungsi sebagai proteksi, tetapi juga sebagai pendorong bagi penyedia layanan untuk mengelola data pribadi dengan lebih bertanggung jawab dan etis.

Selain itu, Undang-Undang Perlindungan Data Pribadi juga mengatur tanggung jawab yang jelas bagi penyedia layanan digital dalam mengelola dan melindungi data pengguna. Penyedia layanan diwajibkan untuk menerapkan langkah-langkah keamanan yang memadai, termasuk penggunaan enkripsi, autentikasi multifaktor, dan audit rutin untuk memastikan bahwa data pengguna tetap aman dari ancaman siber. Kewajiban ini tidak hanya melindungi data, tetapi juga membangun kepercayaan pengguna terhadap layanan digital yang mereka gunakan.

Undang-undang ini mewajibkan penyedia layanan untuk melaporkan kejadian kebocoran data kepada otoritas yang berwenang dan pengguna yang terdampak dalam waktu yang ditentukan. Proses pelaporan ini penting untuk memastikan bahwa tindakan cepat dapat diambil untuk meminimalkan dampak pelanggaran data tersebut. Transparansi dalam melaporkan kejadian juga memberikan kesempatan kepada pengguna untuk mengambil langkah-langkah perlindungan tambahan terhadap potensi risiko. Undang-Undang Perlindungan Data Pribadi ini tidak hanya berfungsi sebagai alat perlindungan, tetapi juga sebagai pendorong bagi inovasi dalam praktik keamanan data di sektor swasta. Penyedia layanan didorong untuk terus meningkatkan teknologi dan prosedur mereka guna menanggapi tantangan keamanan yang terus berkembang. Hal ini menciptakan lingkungan yang lebih aman dan mendorong kompetisi sehat di antara penyedia layanan untuk menawarkan solusi yang lebih baik dalam melindungi data pribadi. Inovasi dalam keamanan data dapat membuka peluang baru untuk pengembangan layanan digital yang lebih efisien dan responsif terhadap kebutuhan pengguna.[8]

Implementasi Undang-Undang Perlindungan Data Pribadi diharapkan dapat menciptakan kesadaran kolektif mengenai pentingnya perlindungan data pribadi, baik di kalangan masyarakat maupun penyedia layanan. Kesadaran ini menjadi kunci dalam mendorong perubahan perilaku, sehingga setiap individu dan organisasi menyadari bahwa keamanan data bukan hanya tanggung jawab penyedia layanan, tetapi juga merupakan tanggung jawab bersama.

[8] Rodrigues, G., Serrano, A., Lemos, A., Canedo, E., Mendonça, F., De Oliveira Albuquerque, R., Orozco, A., & Villalba, L., 2024. Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review. Data, 9, pp. 27. https://doi.org/10.3390/data9020027.

Dengan adanya pendidikan dan kampanye informasi tentang hak-hak pengguna dan cara melindungi data pribadi, masyarakat akan lebih memahami tentang risiko yang dihadapi di dunia digital. Hal ini akan mendorong terciptanya budaya privasi yang lebih baik, di mana setiap orang berkomitmen untuk menjaga data mereka sendiri serta menghormati data orang lain. Organisasi, pada pasangan, akan lebih termotivasi untuk menerapkan praktik terbaik dalam pengelolaan data, seperti transparansi dalam penggunaan data dan investasi dalam teknologi keamanan yang lebih canggih. Dengan langkah-langkah ini, diharapkan masyarakat dapat merasa lebih aman dan terlindungi dalam berinteraksi di dunia digital. Lingkungan yang lebih aman akan mendorong partisipasi aktif dalam ekonomi digital, meningkatkan kepercayaan konsumen, dan menciptakan ekosistem digital yang lebih sehat dan berkelanjutan.

Penelitian ini juga akan mendalami peran penyedia layanan, seperti Dana, dalam menjamin keamanan data serta transaksi pengguna. Aspek ini sangat krusial, mengingat penyedia layanan memiliki tanggung jawab untuk menerapkan praktik keamanan yang kuat, termasuk enkripsi data, autentikasi multi-faktor, dan prosedur penanganan kejadian yang cepat. Dengan meneliti bagaimana Dana menjunjung tinggi kewajiban hukum dan menerapkan langkah-langkah keamanan, diharapkan dapat mengungkap seberapa baik mereka melindungi informasi pribadi pengguna.

Melalui analisis ini, diharapkan dapat ditemukan rekomendasi yang tidak hanya meningkatkan efektivitas perlindungan data pribadi, tetapi juga mendorong penyedia layanan untuk berinovasi dalam praktik keamanan mereka. Dengan demikian, pengguna dapat merasa aman dan nyaman dalam melakukan transaksi digital, yang pada gilirannya akan meningkatkan kepercayaan terhadap masyarakat penggunaan e-wallet dan teknologi digital lainnya. Penelitian ini diharapkan dapat memberikan kontribusi yang berarti dalam pengembangan regulasi dan praktik terbaik di bidang perlindungan data, serta menjadi referensi bagi pemangku kepentingan dalam menjaga keamanan data pribadi di era digital.

METODE PENELITIAN

Penelitian Ini Menggunakan Metode Yuridis Normatif, Yang Bertumpu Pada Analisis Terhadap Peraturan Perundang-Undangan Yang Berlaku, Doktrin Hukum, Dan Literatur Terkait. Pendekatan Deskriptif Kualitatif Digunakan Untuk Menggambarkan Dan Menganalisis Secara Sistematis Bagaimana Bentuk Perlindungan Hukum Terhadap Data Pribadi Pengguna E-Wallet, Khususnya Aplikasi Dana.

Sumber Data Terdiri Dari Bahan Hukum Primer Seperti Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik, Serta Regulasi Dari Bank Indonesia Dan Otoritas Jasa Keuangan. Bahan Hukum Sekunder Meliputi Buku, Jurnal Ilmiah, Dan Penelitian Terdahulu,

Sedangkan Data Primer Diperoleh Melalui Wawancara Dengan Pihak Penegak Hukum Di Polres Sukabumi Kota. Analisis Data Dilakukan Secara Kualitatif Dengan Pendekatan Deduktif, Yaitu Mengkaji Fakta Hukum Yang Ada Berdasarkan Peraturan yang Berlaku.

HASIL DAN PEMBAHASAN

Di era digital yang semakin maju, perlindungan data pribadi menjadi salah satu isu yang paling mendesak. Seiring dengan meningkatnya penggunaan aplikasi e-wallet, seperti Dana, muncul kebutuhan yang mendesak untuk memastikan bahwa hak-hak pengguna dilindungi secara efektif. Hasil penelitian ini menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 telah menyediakan kerangka hukum yang cukup komprehensif dalam melindungi data pribadi. UU ini mengatur prinsip-prinsip pemrosesan data, hak-hak subjek data, kewajiban pengontrol data, serta sanksi administratif, perdata, dan pidana bagi pelanggaran. Dalam konteks aplikasi Dana, perusahaan sebagai pengontrol data memiliki tanggung jawab hukum untuk menjaga keamanan data pengguna.

Undang-undang Nomor 27 Tahun 2022 telah menyediakan kerangka hukum yang cukup komprehensif dalam melindungi data pribadi, menjadikannya landasan yang penting di era digital ini. Undang-undang ini mengatur berbagai aspek penting, termasuk prinsip-prinsip pemrosesan data yang harus diikuti oleh semua entitas yang mengelola data pribadi. Prinsip-prinsip ini mencakup keadilan, transparansi, dan akuntabilitas, yang bertujuan untuk memastikan bahwa data diproses dengan cara yang etis dan sesuai dengan hak-hak individu. Selain itu, undang-undang ini menetapkan hak-hak subjek data, yang memberikan pengguna kendali lebih besar atas informasi pribadi mereka. Hak-hak ini meliputi hak untuk mengakses, memperbaiki, dan menghapus data pribadi, serta hak untuk menolak pemrosesan data dalam situasi tertentu. Dengan adanya ketentuan ini, pengguna memiliki kekuatan untuk melindungi informasi yang dianggap sensitif dan pribadi.[9]

Di sisi lain, kewajiban pengontrol data, dalam hal ini perusahaan seperti Dana, juga diatur dengan jelas. Pengendalian data diwajibkan untuk menerapkan langkah-langkah keamanan yang memadai guna melindungi data pengguna dari akses yang tidak sah, transmisi, atau transmisi. Kewajiban ini mencakup penyusunan kebijakan privasi yang transparan, serta pelatihan bagi staf mengenai praktik keamanan data.Selain itu, undang-undang ini juga memberikan sanksi administratif, perdata, dan kejahatan bagi pelanggaran yang terjadi, sehingga memberikan efek jera bagi pelanggar aturan. Dengan adanya kerangka hukum yang tegas ini, diharapkan perusahaan akan lebih bertanggung jawab dalam menjaga kepercayaan pengguna. Dalam konteks aplikasi Dana,

[9] Husainah, N., Paulina, J., Misrofingah, M., Pradipta, I., Maulana, A., & Fahlevi, M., 2023. Determining factors of digital wallet actual usage: A new model to identify changes in consumer behavior. International Journal of Data and Network Science. https://doi.org/10.5267/j.ijdns.2022.12.017.

tanggung jawab hukum perusahaan sebagai pengontrol data menjadi semakin krusial, mengingat banyaknya informasi sensitif yang dikelola. Oleh karena itu, penerapan undang-undang Perlindungan Data Pribadi dalam praktik sehari-hari menjadi penting untuk menciptakan lingkungan digital yang aman dan terpercaya bagi semua pengguna.[10]

Aplikasi Dana telah menerapkan berbagai langkah teknis untuk melindungi data pengguna, termasuk enkripsi data, autentikasi dua faktor, sertifikasi ISO 27001, dan kebijakan zero data sharing. Langkah-langkah ini dirancang untuk menciptakan lapisan keamanan yang kuat, sehingga data pribadi pengguna tetap aman dari ancaman kejahatan siber. Namun, meskipun upaya-upaya tersebut telah dilakukan, kejahatan siber tetap terjadi dengan frekuensi yang diinduksi.[11]

Studi kasus yang dijelaskan menunjukkan bahwa sebagian besar kejadian kejahatan siber disebabkan oleh kelalaian pengguna, seperti memberikan kode OTP kepada pihak yang tidak bertanggung jawab. Hal ini menyoroti betapa pentingnya kesadaran dan literasi digital dalam perlindungan data pribadi. Pengguna sering kali menjadi titik lemah dalam sistem keamanan, dan pemahaman yang baik tentang cara melindungi informasi pribadi mereka sangat diperlukan untuk mencegah.

Peningkatan literasi digital ini mencakup edukasi tentang bagaimana mengenali tanda-tanda penipuan, pentingnya menjaga kerahasiaan informasi sensitif, dan cara menggunakan fitur keamanan yang disediakan oleh aplikasi. Dengan meningkatnya pemahaman pengguna tentang risiko yang ada dan cara menghindarinya, diharapkan tingkat kejahatan siber dapat diminimalkan. Oleh karena itu, selain langkah-langkah teknis yang telah diterapkan oleh Dana, kolaborasi antara penyedia layanan dan pengguna dalam meningkatkan kesadaran akan keamanan data menjadi kunci untuk menciptakan lingkungan digital yang lebih aman dan terlindungi.

Wawancara dengan aparat kepolisian mengungkap bahwa penegakan hukum terhadap kejahatan siber masih menghadapi kendala serius yang menghambat efektivitas investigasi. Salah satu hambatan utama adalah sulitnya akses terhadap data pelaku, yang sering kali dilindungi oleh regulasi perlindungan data yang ketat. Meskipun perlindungan data pribadi sangat penting, terkadang hal ini dapat menjadi penghalang bagi aparat penegak hukum dalam mengumpulkan bukti yang diperlukan untuk menyelidiki dan menuntut pelaku kejahatan siber. Disamping itu, pelaku anonimitas juga menjadi tantangan signifikan. Banyak pelaku kejahatan siber yang menggunakan teknologi untuk menyembunyikan identitas mereka, sehingga menyulitkan pihak yang berwenang dalam melacak dan menangkap mereka. Tak kalah penting, tidak adanya kerja

[10] Hartanto, H., Rosadi, V., & Yosmar, E., 2023. Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana. PATTIMURA Legal Journal. https://doi.org/10.47268/pela.v2i3.10582.

[11] Nawi, N., Husin, H., Al-Jahwari, N., Zainuddin, S., Khan, N., Hassan, A., Ibrahim, W., Mohamed, A., Nasir, N., & Hasan, M., 2024. The path to sustainability begins with going paperless: Antecedents of intention to use electronic wallet using serial mediation approach. Heliyon, 10. https://doi.org/10.1016/j.heliyon.2024.e24127.

sama formal antara penyedia layanan e-wallet dan aparat penegak hukum menambah kompleksitas situasi ini. Banyak penyedia layanan, termasuk e-wallet, cenderung lebih fokus pada kepatuhan terhadap regulasi perlindungan data tanpa memberikan saluran yang jelas untuk berbagi informasi yang relevan dengan penegakan hukum.[12]

Kondisi ini memperlambat proses investigasi dan memperbesar peluang bagi pelaku untuk melarikan diri atau mengulangi tindak kejahatan. Oleh karena itu, perlu dibentuk protokol kerja sama antar lembaga yang lebih efektif dan kebijakan teknis yang lebih jelas dalam memberikan akses bagi penegak hukum secara terbatas dan bertanggung jawab. Protokol ini harus memastikan bahwa perlindungan data tetap terjaga sambil memberikan aparat penegak hukum kemampuan untuk mengakses informasi yang diperlukan dalam kasus-kasus kejahatan siber. Dengan langkah-langkah ini, diharapkan penegakan hukum akan menjadi lebih responsif dan efektif dalam menghadapi tantangan yang ditimbulkan oleh kejahatan siber di era digital.

Undang-undang No. 27 Tahun 2022 Secara Normatif Telah Memberikan Kerangka Perlindungan Hukum Yang Kuat Terhadap Data Pribadi. Namun, Efektivitas Penerapannya Terhadap Pengguna Aplikasi Dana Masih Menghadapi Tantangan, Antara Lain:[13]

1. Rendahnya literasi digital masyarakat menjadi salah satu tantangan utama dalam penggunaan aplikasi Dana dan platform digital lainnya. Banyak pengguna yang tidak sepenuhnya memahami risiko yang terkait dengan membagikan informasi sensitif seperti kode OTP, PIN, atau data pribadi. Meskipun penyedia aplikasi telah melakukan upaya untuk memberikan edukasi digital, seperti panduan penggunaan dan penjelasan mengenai keamanan, penetrasi informasi ini masih belum merata di seluruh lapisan masyarakat.Kondisi ini menunjukkan betapa pentingnya penyelenggaraan program edukasi berkelanjutan yang melibatkan berbagai pihak, termasuk Kementerian Komunikasi dan Informatika (Kominfo), penyedia aplikasi, dan lembaga pendidikan.[14] Program edukasi ini perlu dirancang untuk menjangkau semua kalangan, mulai dari anak-anak hingga orang dewasa, dengan materi yang mudah dipahami dan relevan dengan pengalaman sehari-hari. [15] Melalui pendekatan yang terintegrasi, diharapkan masyarakat dapat lebih sadar akan risiko yang ada dan bagaimana cara melindungi data pribadi mereka. Pendidikan yang berkelanjutan juga dapat membantu membangun budaya keamanan siber yang kuat, di mana setiap individu merasa bertanggung jawab untuk menjaga informasi pribadi mereka.

[12] Husainah, N., Paulina, J., Misrofingah, M., Pradipta, I., Maulana, A., & Fahlevi, M., 2023. Determining factors of digital wallet actual usage: A new model to identify changes in consumer behavior. International Journal of Data and Network Science. https://doi.org/10.5267/j.ijdns.2022.12.017

[13] Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Ite).

[14] Kominfo. (2023). *Pedoman Perlindungan Data Pribadi*. Diakses Dari https://Kominfo.Go.Id

[15] Otoritas Jasa Keuangan (Ojk). (2022). *Perlindungan Konsumen Jasa Keuangan Digital*.

Dengan meningkatkan literasi digital, masyarakat tidak hanya akan lebih aman dalam menggunakan aplikasi, tetapi juga akan berkontribusi pada terciptanya lingkungan digital yang lebih aman secara keseluruhan.

2. Kendala prosedural dalam penegakan hukum menjadi salah satu faktor utama yang menghambat efektivitas proses investigasi kasus kejahatan siber. Berdasarkan hasil wawancara dengan aparat Polres Sukabumi, mereka mengungkapkan bahwa proses penyidikan sering kali terkendala oleh terbatasnya akses terhadap data pelaku. Lembaga seperti Dana, sebagai penyedia layanan e-wallet, terikat dengan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang mewajibkan mereka untuk menjaga kerahasiaan data pengguna. Meskipun langkah ini penting untuk melindungi privasi individu, hal ini juga menyebabkan tantangan bagi penyidik yang memerlukan informasi untuk menyelesaikan kasus. Proses birokrasi dan legal formal yang kompleks menjadi penghalang tambahan, di mana penyelidikan harus melalui sejumlah prosedur sebelum dapat memperoleh data yang diperlukan. Proses ini sering kali melibatkan persetujuan dari berbagai pihak dan memerlukan waktu yang tidak sedikit, yang pada akhirnya dapat memperlambat investigasi dan memungkinkan pelaku kejahatan untuk melarikan diri atau menghapus jejak mereka. Dengan kondisi ini, penting untuk membuka dan menetapkan kebijakan yang dapat memfasilitasi akses informasi bagi aparat penegak hukum tanpa memberikan perlindungan data pribadi. Pembentukan protokol kerja yang sama yang lebih efisien antara penyedia layanan dan aparat penegak hukum dapat membantu meminimalkan hambatan ini. Melalui pendekatan yang lebih responsif dan kolaboratif, diharapkan proses penyidikan dapat berjalan lebih cepat dan efektif, sehingga pelaku kejahatan siber dapat ditangkap dan diadili secara adil.[16]
3. Belum optimalnya koordinasi antar lembaga menjadi salah satu penghambat signifikan dalam proses penegakan hukum terhadap kejahatan siber. Salah satu isu yang mencolok adalah tidak adanya nota kesepahaman (MoU) antara aparat penegak hukum dan penyedia e-wallet seperti Dana. Ketidakhadiran kerja sama formal ini sangat merugikan, terutama dalam konteks penyidikan yang memerlukan respon cepat. Dalam kasus kejahatan siber, terutama yang berkaitan dengan pencucian uang melalui rekening e-wallet, waktu sangatlah krusial. Proses mengungkap kejahatan yang lambat dapat memberikan peluang bagi pelaku untuk menghilangkan jejak mereka atau bahkan melarikan diri. Kerja sama formal antara aparat penegak hukum dan penyedia layanan digital akan memungkinkan akses yang lebih

[16] Wahyuni, S. (2022). *Cybercrime Dan Perlindungan Konsumen E-Wallet*. Yogyakarta: Deepublish.

cepat dan efisien terhadap data yang diperlukan untuk investigasi, sehingga mempercepat proses pengumpulan bukti dan transmisian.

Dengan adanya MoU, kedua pihak dapat menetapkan prosedur yang jelas dan efektif untuk berbagi informasi, serta memahami tanggung jawab masing-masing dalam menjaga keamanan data pribadi sambil mendukung penegakan hukum. Oleh karena itu, perlu adanya dorongan untuk membangun sinergi antar lembaga, agar pencegahan kejahatan siber dapat dilakukan secara lebih efektif dan efisien, demi menciptakan lingkungan digital yang lebih aman bagi masyarakat.

Lebih lanjut, Undang-Undang Perlindungan Data Pribadi (UU PDP) belum sepenuhnya mengatur perlindungan terhadap pihak ketiga yang menjadi korban identitas. Hal ini berarti bahwa banyak individu yang dirugikan oleh tindakan kejahatan siber tidak mendapatkan perlindungan yang memadai dalam hal pemulihan identitas dan hak-hak mereka. Di sisi lain, belum tersedianya teknologi identifikasi secara real-time di lembaga hukum juga menjadi kendala. Tanpa teknologi yang memadai, aparat penegak hukum kesulitan untuk segera melakukan tindakan yang diperlukan untuk menghentikan kejahatan dan menangkap pelaku. Oleh karena itu, perlu adanya upaya untuk memperkuat regulasi yang melindungi korban mencakup identitas, serta pengembangan teknologi yang dapat mendukung identifikasi pelaku secara lebih efektif. Dengan langkah-langkah ini, diharapkan penegakan hukum akan lebih responsif terhadap kejahatan siber dan memberikan perlindungan yang lebih baik bagi masyarakat.

4. Sebagai penyelenggara data, Dana telah mengklaim menerapkan kebijakan zero data sharing dan memperoleh sertifikasi keamanan yang menunjukkan komitmennya terhadap perlindungan data pengguna. Namun, meskipun langkah-langkah teknis ini diambil, tetap ditemukan celah dari sisi pengguna yang dapat dimanfaatkan oleh pelaku kejahatan siber. Hal ini mengindikasikan bahwa sistem perlindungan data tidak hanya perlu kuat secara teknis, tetapi juga harus disertai dengan tanggung jawab sosial yang lebih besar dari pihak Dana. Tanggung jawab sosial ini mencakup upaya untuk secara aktif mengedukasi pengguna mengenai risiko yang terkait dengan penggunaan aplikasi, seperti pentingnya menjaga kerahasiaan informasi pribadi, mengenali potensi penipuan, dan memahami cara menggunakan fitur keamanan yang ada. Dana harus berperan sebagai fasilitator dalam membangun kesadaran dan pengetahuan pengguna, sehingga mereka dapat melindungi diri mereka sendiri dari ancaman yang ada.

   Selain itu, menyediakan proteksi ganda juga menjadi hal yang penting. Ini bisa mencakup pengembangan fitur keamanan tambahan yang mudah diakses oleh pengguna, serta mekanisme untuk melaporkan dan menangani kasus-kasus yang mencakup data dengan

cepat dan efisien. Dengan menggabungkan pendekatan teknis yang kuat dengan edukasi dan perlindungan yang komprehensif, Dana dapat menciptakan lingkungan yang lebih aman bagi penggunanya, serta meningkatkan kepercayaan masyarakat terhadap layanan yang mereka tawarkan.

5. Minimnya penggunaan prinsip "Privacy By Design" dalam sistem keamanan e-wallet menjadi perhatian serius dalam konteks perlindungan data pribadi. Prinsip ini mengharuskan penyedia layanan untuk mengintegrasikan perlindungan data sejak perancangan aplikasi, sehingga privasi pengguna menjadi bagian integral dalam setiap aspek pengembangan. Namun, hingga saat ini, prinsip ini belum sepenuhnya diadopsi oleh penyedia layanan seperti Dana. Tanpa penerapan prinsip ini, banyak fitur dan fungsi aplikasi dapat dirancang tanpa mempertimbangkan privasi privasi, membuat pengguna lebih rentan terhadap risiko tercakup data. Misalnya, jika fitur keamanan tidak diaktifkan dari awal, pengguna mungkin tidak memiliki kontrol yang memadai atas informasi pribadi mereka. Hal ini dapat mengakibatkan bocornya data atau menyembunyikan informasi yang merugikan.

   Oleh karena itu, sangat penting bagi penyedia layanan untuk menerapkan prinsip "Privacy By Design" dalam setiap langkah pengembangan produk.[17] Dengan melakukan hal ini, mereka tidak hanya memenuhi kewajiban hukum, tetapi juga menunjukkan komitmen terhadap perlindungan privasi pengguna. Prinsip integrasi ini dapat menciptakan kepercayaan yang lebih besar dari masyarakat, serta membangun reputasi yang kuat sebagai penyedia layanan yang bertanggung jawab dan peduli terhadap keamanan data penggunanya.[18]
6. Keterbukaan posisi hukum antara penyedia dan pengguna dalam kontrak digital, seperti Terms of Service, menjadi masalah yang signifikan dalam konteks perlindungan data. Dalam banyak kasus, pengguna hanya diberikan pilihan untuk menerima syarat-syarat yang ditetapkan secara sepihak oleh penyedia tanpa adanya kesempatan untuk melakukan negosiasi. Hal ini menciptakan ketidakadilan, di mana pengguna terpaksa menerima ketentuan yang mungkin tidak mereka pahami sepenuhnya atau setujui. Lebih lanjutnya, banyak penyedia layanan yang tidak transparan mengenai mekanisme penanganan pelanggaran data, sehingga pengguna tidak mengetahui langkah-langkah yang akan diambil jika terjadi transmisi atau transmisi data. Ketidakjelasan ini dapat menyebabkan ketidakpercayaan di kalangan pengguna, yang merasa bahwa hak-hak mereka tidak

[17] Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2021). *Information Security Management Systems: Understanding Iso 27001 Standards*. Crc Press.

[18] Riawati, P., Kurnia, J., Penta, P., & , S., 2023. Digital Wallet Users in Indonesia: Factors Affecting Consumer Satisfaction and Consumer Loyalty.

dilindungi secara memadai. Oleh karena itu, penting bagi penyedia layanan untuk meningkatkan transparansi dan akuntabilitas dalam kontrak digital mereka. Hal ini dapat dilakukan dengan menyediakan informasi yang jelas dan mudah dipahami mengenai hak dan kewajiban pengguna, serta langkah-langkah yang akan diambil dalam situasi pelanggaran data. Dengan demikian, diharapkan muncul keseimbangan yang lebih baik dalam hubungan hukum antara penyedia dan pengguna, serta menciptakan lingkungan yang lebih adil dan aman bagi semua pihak yang terlibat.[19]

KESIMPULAN

Undang-Undang Nomor 27 Tahun 2022 telah memberikan dasar hukum yang kuat untuk melindungi data pribadi pengguna e-wallet, seperti aplikasi Dana. Meskipun regulasi ini dirancang untuk meningkatkan perlindungan data, efektivitasnya masih menghadapi sejumlah tantangan dalam implementasinya. Beberapa kendala utama, seperti rendahnya literasi digital di kalangan masyarakat, lemahnya kerja sama antar lembaga, dan kompleksitas kejahatan siber informasi, mengakibatkan perlindungan yang tidak optimal terhadap pribadi pengguna.

Literasi digital yang rendah membuat banyak pengguna tidak memahami risiko yang terkait dengan penggunaan aplikasi, seperti pentingnya menjaga kerahasiaan informasi pribadi. Hal ini memberi peluang bagi kejahatan siber untuk mengeksploitasi ketidaktahuan pengguna. Selain itu, lemahnya kerja sama antar lembaga, baik antara penyedia layanan e-wallet dengan aparat penegak hukum maupun antar lembaga pemerintah, memperlambat proses penegakan hukum dan penyebaran kejahatan siber. Ketidakjelasan dan kompleksitas dalam prosedur pengumpulan data juga menyulitkan penyidik dalam melakukan investigasi.

Untuk mengatasi tantangan ini, sangat penting untuk menciptakan sinergi antara penyedia layanan, pengguna, dan aparat penegak hukum. Peningkatan edukasi pengguna tentang keamanan siber, hak-hak mereka, dan cara melindungi data pribadi menjadi langkah awal yang krusial. Penyedia layanan, seperti Dana, juga perlu memperkuat sistem keamanan mereka dengan menerapkan teknologi terbaru dan prinsip "Privacy By Design" dalam pengembangan aplikasi.

Selain itu, kebijakan yang memfasilitasi koordinasi antar lembaga perlu dirumuskan. Nota kesepahaman (MoU) antara penyedia layanan dan aparat penegak hukum dapat membantu mempercepat akses data yang diperlukan dalam penyelidikan, serta memastikan bahwa hak-hak pengguna tetap terlindungi. Dengan langkah-langkah komprehensif ini, diharapkan perlindungan terhadap data pribadi di era digital dapat berjalan lebih efektif dan efisien, menciptakan lingkungan yang lebih aman bagi semua pengguna.

[19] Hughes, G., 2020. Enforceability of Contract Terms Displayed on Social Media. , pp. 1-22. https://doi.org/10.4018/978-1-7998-3130-3.ch001.

DAFTAR PUSTAKA

Andriyani, L. (2023). Hukum Perlindungan Data Pribadi Di Era Digital. Jakarta: Sinar Grafika.

Anwar, R., Gaffar, V., Disman, D., Furqon, C., & Sutisnawati, Y., 2023. Mobile wallet adoption model among digital immigration generation in Indonesia. Journal of Eastern European and Central Asian Research (JEECAR). https://doi.org/10.15549/jeecar.v10i6.1499.

Arindy and A. Suzianti. "Multi-Generation Perception Towards Digital Wallet in Indonesia." Proceedings of the 3rd Asia Pacific Conference on Research in Industrial and Systems Engineering (2020). https://doi.org/10.1145/3400934.3400940.

Ciptarianto, A., 2022. E-Wallet Application Penetration for Financial Inclusion in Indonesia. International Journal of Current Science Research and Review. https://doi.org/10.47191/ijcsrr/v5-i2-03.

Firdaus, T., & Lubis, M., 2022. Comparative Analysis of Popular Electronic Wallets in Indonesia in Daily Life Selection. Proceedings of the 8th International Conference on Industrial and Business Engineering. https://doi.org/10.1145/3568834.3568865.

Hartanto, H., Rosadi, V., & Yosmar, E., 2023. Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana. PATTIMURA Legal Journal. https://doi.org/10.47268/pela.v2i3.10582.

Husainah, N., Paulina, J., Misrofingah, M., Pradipta, I., Maulana, A., & Fahlevi, M., 2023. Determining factors of digital wallet actual usage: A new model to identify changes in consumer behavior. International Journal of Data and Network Science. https://doi.org/10.5267/j.ijdns.2022.12.017.

Hughes, G., 2020. Enforceability of Contract Terms Displayed on Social Media. , pp. 1-22. https://doi.org/10.4018/978-1-7998-3130-3.ch001.

Kominfo. (2023). Pedoman Perlindungan Data Pribadi. Diakses Dari https://Kominfo.Go.Id

Langford, B., Chen, J., & Cherry, C., 2015. Risky riding: Naturalistic methods comparing safety behavior from conventional bicycle riders and electric bike riders.. Accident; analysis and prevention, 82, pp. 220-6 . https://doi.org/10.1016/j.aap.2015.05.016.

Morić, Z., Dakić, V., Djekic, D., & Regvart, D., 2024. Protection of Personal Data in the Context of E-Commerce. J. Cybersecur. Priv., 4, pp. 731-761. https://doi.org/10.3390/jcp4030034.

Nawi, N., Husin, H., Al-Jahwari, N., Zainuddin, S., Khan, N., Hassan, A., Ibrahim, W., Mohamed, A., Nasir, N., & Hasan, M., 2024. The path to sustainability begins with going paperless: Antecedents of intention to use electronic wallet using serial mediation approach. Heliyon, 10. https://doi.org/10.1016/j.heliyon.2024.e24127.

Otoritas Jasa Keuangan (Ojk). (2022). Perlindungan Konsumen Jasa Keuangan Digital.

Riawati, P., Kurnia, J., Penta, P., & , S., 2023. Digital Wallet Users in Indonesia: Factors Affecting Consumer Satisfaction and Consumer Loyalty.

Rodrigues, G., Serrano, A., Lemos, A., Canedo, E., Mendonça, F., De Oliveira Albuquerque, R., Orozco, A., & Villalba, L., 2024. Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review. Data, 9, pp. 27. https://doi.org/10.3390/data9020027.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2021). Information Security Management Systems: Understanding Iso 27001 Standards. Crc Press.

Wahyuni, S. (2022). Cybercrime Dan Perlindungan Konsumen E-Wallet. Yogyakarta: Deepublish.

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Ite).

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.