Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 4 (2026) pp: 8985-8991
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Keamanan Sistem Pembayaran Digital terhadap Perlindungan Data Pengguna

Nabilla Ivana Nova[1], Sela Nabila[2], Parid Rehan Paiza[3], Norita Sinaga[4]
[1234] Fakultas Ilmu Komputer Universitas Pamulang
[1]nabillaivananova@gmail.com , [2]selanabila0311@gmail.com, [3]paridrehanpaiza17@gmail.com , [4]dosen03146@unpam.ac.id

Abstract

The increasing adoption of digital payment systems has significantly transformed transaction patterns by offering faster, more practical, and efficient payment processes. These systems also play an important role in promoting financial inclusion and supporting economic recovery. Nevertheless, the growing reliance on digital payments presents various data security risks that may harm both users and service providers, including personal data breaches, identity theft, social engineering–based fraud, and account takeover incidents. This study aims to analyze the security mechanisms implemented in digital payment systems and to examine user data protection practices adopted by service providers in Indonesia. The research uses a qualitative approach through literature review and descriptive analysis of scientific journals, digital financial industry reports, technology whitepapers, and national data protection regulations. This method enables the identification of existing technical practices, governance policies, and security gaps. The findings show that most service providers have implemented essential security measures, such as end-to-end encryption, Transport Layer Security (TLS) protocols, server-side data encryption, tokenization of card data, multi-factor authentication, and one-time password (OTP) verification. Many platforms also integrate machine learning–based systems to detect suspicious activities and prevent fraud proactively. However, human factors and governance weaknesses remain key vulnerabilities. Limited digital security literacy among users increases exposure to phishing and credential misuse, while weak internal controls, inadequate incident management, and low transparency regarding data handling heighten risks. Therefore, strengthening technology, governance, and user education is crucial to ensuring a secure and sustainable digital payment ecosystem.

Keywords*: Cybersecurity, Multi-Factor Authentication, Tokenization, Fraud Detection, Data Protection Regulations, Data Governance*

1. Introduction

Inovasi teknologi finansial telah membawa perubahan yang sangat signifikan dalam pola transaksi keuangan masyarakat modern. Kehadiran berbagai instrumen pembayaran digital, seperti dompet digital, mobile banking, dan sistem pembayaran berbasis QRIS, telah menggeser kebiasaan masyarakat dari penggunaan uang tunai menuju transaksi non-tunai yang lebih cepat, praktis, dan efisien. Layanan-layanan ini dimanfaatkan secara luas dalam berbagai aktivitas ekonomi sehari-hari, mulai dari transaksi ritel, pembayaran tagihan rutin, hingga transfer dana antarindividu tanpa batasan waktu dan lokasi. Transformasi ini tidak hanya meningkatkan kenyamanan dan efisiensi waktu bagi pengguna, tetapi juga mengurangi ketergantungan pada uang fisik serta memperluas akses layanan keuangan bagi masyarakat yang sebelumnya belum terjangkau oleh sistem perbankan konvensional. Namun, di balik kemudahan tersebut, penggunaan pembayaran digital juga menuntut adanya kepercayaan pengguna terhadap keamanan sistem dan perlindungan data pribadi yang dikelola oleh penyedia layanan, karena seluruh proses transaksi bergantung pada pemrosesan data secara elektronik. Hal ini sejalan dengan temuan Utomo dan Rahman yang menyatakan bahwa tingkat adopsi dan keberlanjutan penggunaan layanan e-wallet sangat dipengaruhi oleh persepsi pengguna terhadap keamanan dan perlindungan data pribadi yang mereka miliki dalam ekosistem pembayaran digital [1].

Seiring dengan meningkatnya adopsi sistem pembayaran digital, eskalasi pengumpulan, pemrosesan, dan penyimpanan data pribadi pengguna di dalam ekosistem digital menjadi semakin signifikan dan kompleks. Penyedia layanan pembayaran digital mengelola beragam jenis data, mulai dari informasi identitas, nomor telepon, detail akun, riwayat transaksi, hingga metadata lokasi dan preferensi penggunaan, yang secara keseluruhan membentuk profil digital pengguna. Akumulasi data tersebut memiliki nilai ekonomi dan strategis yang tinggi, baik bagi pengembangan layanan maupun bagi pihak-pihak yang berniat menyalahgunakannya. Kondisi ini menjadikan data pribadi sebagai target utama kejahatan siber, terutama ketika pengelolaannya tidak diimbangi

dengan sistem keamanan dan tata kelola data yang memadai. Dampak dari lemahnya perlindungan data tidak hanya terbatas pada kerugian finansial, seperti penipuan dan pencurian identitas, tetapi juga mencakup pelanggaran hak privasi pengguna melalui pemanfaatan data untuk kepentingan komersial tanpa persetujuan yang sah [2].

Ancaman terhadap keamanan pembayaran digital tidak selalu bersumber dari kelemahan teknis sistem semata, melainkan dalam banyak kasus justru dipicu oleh faktor non-teknis yang berkaitan erat dengan perilaku pengguna dan rendahnya tingkat literasi keamanan digital. Berbagai praktik berisiko masih sering ditemukan dalam penggunaan layanan pembayaran digital, seperti membagikan kode OTP atau PIN kepada pihak lain, mengklik tautan phishing yang menyerupai layanan resmi, menggunakan kata sandi yang lemah atau sama di berbagai platform, serta mengakses layanan keuangan melalui jaringan Wi-Fi publik yang tidak aman. Pola perilaku tersebut membuka celah yang signifikan bagi pelaku kejahatan siber untuk melakukan pengambilalihan akun, pencurian identitas, dan akses tidak sah terhadap data sensitif pengguna. Temuan ini sejalan dengan kajian Pradana dan Nasution yang menegaskan bahwa ancaman kejahatan siber pada penggunaan e-wallet tidak hanya disebabkan oleh aspek teknologi, tetapi juga sangat dipengaruhi oleh tingkat kesadaran dan kehati-hatian pengguna dalam menjaga data pribadi dan kredensial akses mereka [3].

Dalam konteks tersebut, keamanan pembayaran digital perlu dipahami sebagai suatu sistem terpadu yang melibatkan peran dan tanggung jawab berbagai aktor utama yang saling berinteraksi, yaitu penyedia layanan, regulator, dan pengguna. Penyedia layanan memiliki kewajiban utama untuk merancang dan mengimplementasikan mekanisme keamanan teknis yang andal, seperti enkripsi data, autentikasi berlapis, tokenisasi, serta sistem deteksi dan respons terhadap aktivitas mencurigakan guna meminimalkan risiko kebocoran data dan penyalahgunaan transaksi. Di sisi lain, regulator memegang peranan strategis dalam menetapkan kerangka kebijakan yang komprehensif terkait perlindungan data pribadi, kewajiban pelaporan insiden keamanan, serta standar kepatuhan yang dapat diawasi dan ditegakkan secara efektif. Namun demikian, keberhasilan perlindungan keamanan transaksi digital tidak semata-mata ditentukan oleh aspek teknologi dan regulasi, melainkan juga sangat bergantung pada peran aktif pengguna sebagai lapisan pertahanan pertama. Kesadaran dan literasi digital pengguna dalam menjaga kerahasiaan data, memahami risiko privasi, serta menerapkan praktik penggunaan layanan yang aman terbukti berpengaruh signifikan terhadap tingkat keamanan transaksi, sebagaimana ditunjukkan oleh temuan Sahlan dan Nasution yang menyatakan bahwa tingkat kesadaran privasi data pribadi memiliki hubungan erat dengan perilaku pengguna dalam memanfaatkan layanan keuangan digital, termasuk dalam pengambilan keputusan dan pengelolaan risiko penggunaan layanan pembayaran berbasis teknologi [4].

Meskipun berbagai mekanisme keamanan telah diterapkan oleh penyedia layanan pembayaran digital, efektivitas penerapannya dalam praktik masih memerlukan kajian yang lebih mendalam dan komprehensif. Pesatnya perkembangan teknologi, integrasi sistem dengan pihak ketiga, serta pemanfaatan infrastruktur berbasis cloud dan Application Programming Interface (API) telah meningkatkan kompleksitas arsitektur sistem pembayaran digital secara signifikan. Kompleksitas ini tidak hanya membuka potensi munculnya celah teknis, seperti kerentanan sistem dan kesalahan konfigurasi, tetapi juga menimbulkan tantangan pada aspek tata kelola data, transparansi pengelolaan informasi, dan kepatuhan terhadap regulasi perlindungan data pribadi. Dalam konteks tersebut, keamanan transaksi digital tidak dapat dipandang semata-mata sebagai persoalan teknis, melainkan juga sebagai isu regulasi dan manajemen risiko yang saling terkait. Perlindungan data pribadi dalam transaksi digital harus memperhatikan keseimbangan antara aspek keamanan, efisiensi layanan, dan kepatuhan terhadap regulasi, karena lemahnya salah satu aspek tersebut dapat menurunkan tingkat kepercayaan pengguna dan meningkatkan risiko penyalahgunaan data [5].

Berdasarkan kondisi tersebut, diperlukan pendekatan yang holistik dan berkelanjutan dalam memperkuat keamanan pembayaran digital. Pendekatan ini mencakup penguatan teknologi keamanan, peningkatan tata kelola dan transparansi pengelolaan data, serta penyelenggaraan program edukasi dan literasi digital yang konsisten bagi pengguna. Sinergi yang efektif antara penyedia layanan, regulator, dan pengguna diharapkan mampu menciptakan ekosistem pembayaran digital yang lebih aman, andal, dan terpercaya, sehingga dapat mendukung pertumbuhan ekonomi digital sekaligus melindungi kepentingan masyarakat secara luas.

2. Research Methods

Penelitian ini menggunakan metode studi literatur yang dipadukan dengan analisis deskriptif untuk memperoleh pemahaman komprehensif mengenai keamanan sistem pembayaran digital dan perlindungan data pengguna. Pendekatan ini dipilih karena mampu menggambarkan secara sistematis perkembangan konsep, kebijakan, serta praktik keamanan yang diterapkan dalam ekosistem pembayaran digital. Melalui studi literatur, peneliti mengkaji

DOI: https://doi.org/ 10.31004/riggs.v4i4.5119

berbagai sumber tertulis yang relevan guna membangun landasan teoretis dan konseptual yang kuat sebagai dasar analisis.

Data penelitian diperoleh dari beragam sumber sekunder yang kredibel, meliputi jurnal ilmiah nasional dan internasional, laporan resmi regulator sistem pembayaran, publikasi industri fintech, serta dokumen kebijakan terkait perlindungan data pribadi. Pemilihan sumber literatur dilakukan secara selektif dengan mempertimbangkan tingkat relevansi terhadap topik penelitian, keterbaruan publikasi, serta kesesuaiannya dengan konteks penerapan keamanan pembayaran digital di Indonesia. Proses seleksi ini bertujuan untuk memastikan bahwa data yang digunakan mencerminkan kondisi terkini dan dapat dipertanggungjawabkan secara akademik.

Tahap awal penelitian difokuskan pada pengumpulan dan penelaahan referensi yang membahas konsep dasar pembayaran digital, prinsip keamanan informasi, serta kerangka perlindungan data pengguna. Referensi yang terkumpul kemudian dianalisis untuk mengidentifikasi berbagai teknologi keamanan yang umum digunakan oleh penyedia layanan pembayaran digital, seperti enkripsi data, autentikasi berlapis, tokenisasi, dan sistem deteksi aktivitas berisiko. Klasifikasi teknologi ini dilakukan untuk memudahkan pemetaan mekanisme keamanan yang diterapkan dalam praktik.

Tahap selanjutnya mencakup identifikasi jenis risiko dan pola ancaman terhadap data pengguna, baik yang bersumber dari celah teknis sistem maupun dari faktor non-teknis seperti perilaku pengguna. Analisis ini juga mencakup kajian terhadap penerapan perlindungan data oleh penyedia layanan, yang ditinjau melalui kebijakan privasi, pengendalian akses, serta mekanisme keamanan transaksi yang diberlakukan. Dengan demikian, penelitian ini tidak hanya menyoroti aspek teknologi, tetapi juga memperhatikan tata kelola dan kebijakan yang mendasari perlindungan data.

Hasil dari seluruh tahapan analisis selanjutnya disintesis untuk menyusun temuan penelitian, memetakan isu-isu utama yang muncul, serta merumuskan rekomendasi penguatan keamanan sistem pembayaran digital dan peningkatan literasi digital pengguna. Metode studi literatur dan analisis deskriptif ini dinilai sesuai untuk kajian konseptual pada tahap awal penelitian, khususnya dalam memahami fenomena, memetakan permasalahan, dan menganalisis kecenderungan risiko keamanan digital tanpa melibatkan pengujian empiris secara langsung. Pendekatan ini memungkinkan peneliti membangun gambaran umum mengenai kondisi keamanan dan praktik perlindungan data yang berjalan dalam ekosistem pembayaran digital.

3. Results and Discussions

Hasil analisis menunjukkan bahwa tingkat keamanan dalam sistem pembayaran digital tidak semata-mata ditentukan oleh kecanggihan teknologi, melainkan oleh keselarasan antara desain sistem, tata kelola data, serta kebiasaan pengguna dalam memanfaatkan layanan. Dalam banyak kasus, insiden keamanan terjadi bukan karena kegagalan sistem inti, tetapi akibat rekayasa sosial yang memanfaatkan kelengahan pengguna, seperti penipuan berbasis phishing atau permintaan OTP oleh pihak yang mengaku sebagai layanan resmi. Kondisi ini menegaskan bahwa keamanan pembayaran digital bersifat multidimensi, di mana teknologi, regulasi, dan literasi pengguna harus berjalan secara simultan. Tanpa dukungan perilaku pengguna yang aman, mekanisme teknis yang kuat sekalipun tidak mampu memberikan perlindungan optimal.

Dari sisi penyedia layanan, penerapan teknologi keamanan seperti enkripsi, autentikasi berlapis, tokenisasi, dan pemantauan transaksi secara real time telah membentuk fondasi perlindungan data yang cukup kuat. Namun demikian, terdapat variasi kualitas implementasi antar platform, yang berdampak pada perbedaan tingkat perlindungan yang diterima pengguna. Beberapa penyedia telah menerapkan standar keamanan yang ketat dan konsisten, sementara sebagian lainnya masih berada pada tahap penyesuaian. Selain itu, kebijakan privasi sebagai instrumen formal perlindungan data belum sepenuhnya efektif karena rendahnya tingkat pemahaman pengguna. Banyak pengguna memberikan persetujuan tanpa membaca isi kebijakan, sehingga tidak memahami jenis data yang dikumpulkan, tujuan pemrosesan, maupun kemungkinan distribusi data ke pihak ketiga. Ketidaktahuan ini sering memicu persepsi kerugian ketika terjadi isu kebocoran data atau penyalahgunaan informasi pribadi.

Temuan penelitian menegaskan bahwa titik paling rentan dalam ekosistem pembayaran digital berada pada interaksi manusia dengan sistem. Pola kepercayaan berlebih terhadap pesan atau pihak yang mengaku resmi menunjukkan bahwa ancaman digital berkembang melalui manipulasi psikologis, bukan semata-mata eksploitasi teknis. Regulasi telah berperan sebagai penopang tata kelola keamanan dengan mendorong transparansi, kewajiban pelaporan insiden, dan perlindungan data pribadi, namun pengawasan dan mekanisme pengaduan masih menghadapi keterbatasan. Oleh karena itu, peran pengguna menjadi faktor penentu terakhir, di mana kedisiplinan dalam mengaktifkan fitur keamanan, memperbarui aplikasi, serta memverifikasi sumber komunikasi terbukti menurunkan risiko penyalahgunaan. Secara keseluruhan, penguatan keamanan pembayaran digital perlu diarahkan

DOI: https://doi.org/ 10.31004/riggs.v4i4.5119

pada peningkatan standar teknologi, penyederhanaan kebijakan privasi agar mudah dipahami, serta pengembangan literasi keamanan digital yang aplikatif, sehingga perlindungan data tidak hanya bergantung pada sistem, tetapi menjadi bagian dari budaya penggunaan layanan digital.

3.1. Penerapan Teknologi Keamanan pada Layanan Pembayaran Digital

Hasil analisis menunjukkan bahwa sebagian besar penyedia layanan pembayaran digital telah mengintegrasikan berbagai teknologi keamanan sebagai bagian dari standar operasional sistem mereka guna melindungi data dan transaksi pengguna. Teknologi yang paling umum diterapkan meliputi enkripsi data transaksi dan identitas pengguna untuk menjaga kerahasiaan informasi, penerapan autentikasi multi faktor melalui kombinasi PIN, OTP, atau biometrik untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses akun, serta tokenisasi dalam penyimpanan informasi kartu guna meminimalkan risiko kebocoran data sensitif. Selain itu, penyedia layanan juga memanfaatkan sistem monitoring dan pelacakan transaksi mencurigakan secara real time serta pencatatan log aktivitas sebagai dasar evaluasi dan audit keamanan sistem. Penerapan langkah-langkah teknis tersebut sejalan dengan temuan Khoiriah et al. yang menyatakan bahwa enkripsi, autentikasi berlapis, dan pemantauan transaksi merupakan fondasi utama dalam menjaga keamanan dan privasi pada ekosistem keuangan digital yang semakin kompleks [6].

Penerapan teknologi keamanan tersebut secara umum terbukti mampu menurunkan risiko akses tidak sah, penyalahgunaan akun, dan kebocoran data pengguna. Enkripsi dan tokenisasi berperan penting dalam melindungi data baik pada saat penyimpanan maupun transmisi, sehingga meskipun terjadi intersepsi, informasi yang diperoleh tidak dapat digunakan secara langsung. Autentikasi multi faktor juga meningkatkan lapisan keamanan dengan memperkecil peluang keberhasilan pengambilalihan akun oleh pihak yang tidak berwenang. Di sisi lain, keberadaan sistem monitoring transaksi mencurigakan memungkinkan penyedia layanan mendeteksi pola anomali secara dini dan melakukan tindakan pencegahan sebelum kerugian yang lebih besar terjadi. Temuan ini sejalan dengan hasil *systematic literature review* yang dilakukan oleh Dewi et al., yang menegaskan bahwa kombinasi antara teknologi proteksi data dan sistem deteksi ancaman secara proaktif merupakan strategi efektif dalam mengurangi risiko keamanan pada sistem pembayaran elektronik [7].

Namun demikian, efektivitas penerapan teknologi keamanan tersebut tidak sepenuhnya terlepas dari faktor non-teknis, khususnya perilaku pengguna serta kualitas implementasi dan tata kelola keamanan oleh penyedia layanan. Praktik pengguna seperti penggunaan kata sandi yang lemah, kelalaian dalam menjaga kerahasiaan OTP, serta rendahnya kewaspadaan terhadap serangan phishing dapat secara signifikan menurunkan efektivitas sistem keamanan yang telah dirancang. Di sisi lain, perbedaan kualitas implementasi antar penyedia layanan, termasuk keandalan sistem monitoring, konsistensi pembaruan keamanan, dan kecepatan respons terhadap insiden, turut memengaruhi tingkat perlindungan data yang dirasakan pengguna. Hal ini sejalan dengan pandangan Alvionita yang menekankan bahwa tanggung jawab keamanan data digital oleh penyelenggara sistem elektronik tidak hanya bersifat teknis, tetapi juga mencakup aspek tata kelola, kepatuhan, dan edukasi pengguna agar perlindungan data dapat berjalan secara optimal [8].

3.2. Bentuk Perlindungan Data Pengguna

Berdasarkan hasil kajian literatur dan analisis kebijakan, perlindungan data pengguna pada layanan pembayaran digital umumnya diterapkan melalui kebijakan dan prosedur organisasi yang dirancang untuk membatasi risiko akses tidak sah terhadap data sensitif. Penyedia layanan menerapkan pembatasan akses internal dengan prinsip *least privilege*, sehingga hanya pihak atau unit tertentu yang memiliki kewenangan dalam pengelolaan data pengguna. Pendekatan ini bertujuan meminimalkan potensi kebocoran data yang disebabkan oleh kesalahan manusia maupun penyalahgunaan wewenang di lingkungan internal organisasi. Selain itu, penerapan persetujuan pengguna (*user consent*) sebelum pemrosesan data pribadi menjadi fondasi legal dan etis dalam pengelolaan data di ekosistem pembayaran digital. Hal ini sejalan dengan temuan Ramon, Iriansyah, dan Triana yang menegaskan bahwa persetujuan pengguna merupakan elemen utama dalam perlindungan hak privasi dan keamanan data pribadi pada layanan berbasis aplikasi online, karena menjadi dasar legitimasi hukum atas pengumpulan dan penggunaan data oleh penyedia layanan [9].

Hasil analisis juga menunjukkan bahwa penyedia layanan pembayaran digital secara umum telah menyediakan kebijakan privasi yang dapat diakses oleh pengguna melalui aplikasi maupun situs resmi. Kebijakan privasi tersebut menjelaskan jenis data yang dikumpulkan, tujuan pengumpulan, mekanisme penyimpanan, serta hak-hak pengguna atas data pribadinya. Namun demikian, tingkat pemahaman pengguna terhadap isi kebijakan privasi masih bervariasi, terutama karena penggunaan istilah hukum dan teknis yang relatif kompleks. Kondisi ini menunjukkan adanya kesenjangan antara ketersediaan informasi dan pemahaman aktual pengguna. Akbar, Sitorus, dan Putra Nasution menyatakan bahwa meskipun kebijakan perlindungan data telah disediakan oleh pelaku usaha

DOI: https://doi.org/ 10.31004/riggs.v4i4.5119

digital, efektivitasnya akan terbatas apabila konsumen tidak memahami substansi hak dan kewajibannya dalam transaksi digital [10]. Di sisi lain, sebagian penyedia layanan telah melengkapi sistemnya dengan fitur notifikasi aktivitas akun, seperti pemberitahuan login, transaksi, dan perubahan pengaturan keamanan, yang berfungsi sebagai mekanisme peringatan dini terhadap aktivitas mencurigakan serta sebagai bentuk transparansi kepada pengguna.

Selain kebijakan dan fitur teknis, beberapa platform pembayaran digital juga menyediakan pusat bantuan keamanan dan materi edukasi literasi digital bagi pengguna. Fasilitas ini mencakup panduan praktik keamanan dasar, cara mengenali serangan *phishing* dan *social engineering*, serta prosedur pelaporan apabila terindikasi terjadi kebocoran data atau penyalahgunaan akun. Keberadaan pusat bantuan dan materi edukatif tersebut mencerminkan upaya penyedia layanan untuk mendorong peran aktif pengguna dalam menjaga keamanan data pribadi. Monica, Yulianti, dan Nurintiara menegaskan bahwa penguatan perlindungan data pribadi dalam transaksi dompet elektronik tidak hanya bergantung pada regulasi dan teknologi, tetapi juga pada peningkatan kesadaran serta literasi digital pengguna sebagai bagian dari sistem keamanan secara keseluruhan [11]. Meskipun demikian, efektivitas perlindungan data tetap sangat bergantung pada konsistensi implementasi kebijakan oleh penyedia layanan serta kemampuan pengguna dalam memahami dan memanfaatkan fitur keamanan yang tersedia secara optimal.

3.3. Risiko Keamanan yang Masih Muncul

Hasil penelitian menunjukkan bahwa risiko keamanan yang masih sering muncul dalam ekosistem pembayaran digital pada dasarnya bersumber dari interaksi pengguna dengan sistem digital itu sendiri. Berbagai praktik berisiko, seperti membagikan kode OTP kepada pihak yang tidak dikenal, mengklik tautan palsu yang menyerupai layanan resmi, serta penggunaan kata sandi yang lemah atau digunakan secara berulang pada berbagai platform, masih banyak ditemukan dalam aktivitas transaksi digital sehari-hari. Selain itu, kebiasaan pengguna melakukan login melalui jaringan publik tanpa proteksi keamanan yang memadai serta menginstal aplikasi modifikasi atau tidak resmi semakin memperbesar peluang terjadinya akses tidak sah terhadap akun dan data pribadi. Temuan ini mengindikasikan bahwa meskipun penyedia layanan telah menerapkan beragam mekanisme pengamanan teknis, faktor manusia tetap menjadi titik lemah utama yang dapat dimanfaatkan oleh pelaku kejahatan siber, aspek perilaku pengguna masih menjadi salah satu penyebab dominan insiden keamanan dan privasi dalam sistem pembayaran digital meskipun teknologi keamanan terus berkembang [12].

Pembahasan lebih lanjut mengungkap bahwa rendahnya tingkat literasi digital dan kesadaran pengguna terhadap pentingnya perlindungan data pribadi menjadi tantangan signifikan dalam menjaga keamanan transaksi digital. Banyak pengguna belum sepenuhnya memahami konsekuensi dari penyalahgunaan data pribadi serta risiko jangka panjang yang dapat timbul akibat kelalaian dalam menjaga informasi sensitif. Hal ini tercermin dari kebiasaan pengguna yang cenderung mengabaikan syarat dan ketentuan penggunaan layanan, sehingga tidak menyadari hak, kewajiban, serta potensi risiko yang melekat pada penggunaan sistem pembayaran digital. Kondisi tersebut berimplikasi pada meningkatnya potensi pelanggaran privasi dan berkurangnya efektivitas kebijakan perlindungan data yang telah dirancang oleh penyedia layanan. Perlindungan data pribadi di dunia maya tidak hanya bergantung pada regulasi dan sistem keamanan, tetapi juga sangat dipengaruhi oleh tingkat pemahaman dan kesadaran pengguna dalam mengelola data pribadinya secara bertanggung jawab [13].

Selain faktor perilaku dan literasi pengguna, hasil penelitian juga menunjukkan adanya tantangan dalam aspek pelaporan dan penanganan insiden keamanan. Banyak kasus kebocoran data atau penipuan digital yang tidak dilaporkan secara formal oleh pengguna, baik karena kurangnya pemahaman mengenai prosedur pelaporan maupun anggapan bahwa kerugian yang dialami bersifat kecil dan dapat diabaikan. Akibatnya, penyedia layanan dan regulator tidak memperoleh gambaran yang utuh mengenai skala, pola, serta tren ancaman keamanan yang terjadi di lapangan, sehingga menyulitkan upaya mitigasi risiko secara sistematis. Kondisi ini menegaskan bahwa keamanan sistem pembayaran digital tidak hanya ditentukan oleh kecanggihan teknologi yang digunakan, tetapi juga oleh efektivitas komunikasi, kejelasan mekanisme pelaporan insiden, serta tingkat kepercayaan pengguna terhadap penyedia layanan. Faktor keamanan dan kepercayaan memiliki peran penting dalam keberlanjutan adopsi pembayaran digital, di mana respons yang transparan dan efektif terhadap insiden keamanan dapat memperkuat kepercayaan pengguna terhadap sistem yang digunakan [14].

3.4. Peran Regulasi dan Pengawasan

Hasil analisis menunjukkan bahwa regulasi perlindungan data pribadi memiliki peran yang sangat penting dalam mendorong penyedia layanan pembayaran digital untuk meningkatkan standar keamanan dalam pemrosesan dan penyimpanan data pengguna. Keberadaan regulasi tersebut menempatkan kewajiban hukum yang jelas bagi penyedia layanan untuk menerapkan langkah-langkah teknis dan organisatoris yang memadai, seperti pengamanan

DOI: https://doi.org/ 10.31004/riggs.v4i4.5119

sistem, pembatasan akses, serta pengelolaan data secara bertanggung jawab guna mencegah akses tidak sah, kehilangan data, maupun penyalahgunaan informasi pribadi. Selain itu, regulasi juga mengharuskan penyedia layanan untuk menyampaikan informasi yang transparan mengenai tujuan pengumpulan data, ruang lingkup pemrosesan, serta hak-hak pengguna atas data pribadinya. Kondisi ini menegaskan bahwa kepatuhan terhadap regulasi tidak hanya bersifat administratif, tetapi juga mencerminkan tanggung jawab etis penyedia layanan dalam menjaga kepercayaan pengguna, sebagaimana ditegaskan oleh Alvionita bahwa penyelenggara sistem elektronik memiliki tanggung jawab hukum dan moral dalam menjamin keamanan data digital yang dikelolanya sebagai bagian dari perlindungan hak privasi pengguna [8].

Meskipun regulasi telah memberikan kerangka hukum yang relatif jelas, temuan penelitian menunjukkan bahwa efektivitas perlindungan data sangat bergantung pada kekuatan pengawasan dan penegakan hukum oleh otoritas terkait. Tanpa pengawasan yang konsisten dan sanksi yang tegas, kepatuhan penyedia layanan berpotensi hanya bersifat formalitas, misalnya dengan menyediakan kebijakan privasi yang panjang namun sulit dipahami oleh pengguna awam. Dalam praktiknya, masih ditemukan kebijakan privasi yang menggunakan istilah teknis dan bahasa hukum yang kompleks, sehingga tujuan transparansi belum sepenuhnya tercapai. Hal ini menunjukkan adanya kesenjangan antara norma hukum dan implementasinya di lapangan. Harahap menegaskan bahwa regulasi perlindungan data pribadi akan kehilangan efektivitasnya apabila tidak diiringi dengan mekanisme penegakan yang kuat, termasuk audit berkala, kewajiban pelaporan insiden kebocoran data, serta koordinasi antarlembaga pengawas untuk memastikan kepatuhan penyedia layanan secara substansial, bukan sekadar normatif [5].

Selain peran regulator dan penyedia layanan, hasil pembahasan juga menekankan pentingnya peningkatan literasi hukum dan digital di kalangan pengguna sebagai bagian dari ekosistem perlindungan data. Edukasi mengenai hak-hak atas data pribadi, seperti hak untuk memperoleh informasi, hak atas keamanan data, serta hak untuk mengajukan keberatan atau pengaduan ketika terjadi pelanggaran, menjadi faktor kunci dalam memperkuat posisi pengguna. Dengan tingkat literasi yang memadai, pengguna tidak hanya bersikap pasif sebagai penerima layanan, tetapi mampu menjadi aktor aktif yang lebih kritis terhadap praktik pengelolaan data oleh penyedia layanan. Hal ini sejalan dengan temuan Utomo dan Rahman yang menunjukkan bahwa tingkat kesadaran keamanan data pribadi pada pengguna e-wallet berpengaruh langsung terhadap perilaku penggunaan layanan digital yang lebih aman dan berhati-hati. Oleh karena itu, sinergi antara regulasi yang kuat, pengawasan yang efektif, dan peningkatan kesadaran pengguna menjadi prasyarat utama dalam mewujudkan ekosistem pembayaran digital yang aman, transparan, dan berkeadilan [1].

3.5. Peran Pengguna dalam Menjaga Keamanan Data

Hasil analisis menunjukkan bahwa pengguna memiliki peran yang sangat signifikan dalam menjaga keamanan data dan transaksi pada sistem pembayaran digital, karena perilaku individu sering kali menjadi faktor penentu keberhasilan atau kegagalan mekanisme perlindungan yang telah dirancang secara teknis oleh penyedia layanan. Meskipun sistem pembayaran digital umumnya telah dilengkapi dengan berbagai lapisan keamanan, efektivitas perlindungan data tetap sangat dipengaruhi oleh cara pengguna mengelola akun dan informasi pribadinya. Praktik dasar seperti tidak membagikan kode OTP atau PIN kepada pihak lain merupakan langkah krusial dalam mencegah pengambilalihan akun oleh pihak yang tidak berwenang. Berbagai kasus penipuan digital menunjukkan bahwa kebocoran data lebih sering terjadi akibat kelalaian pengguna dibandingkan kegagalan sistem, terutama ketika pengguna secara tidak sadar memberikan akses kepada pelaku kejahatan siber melalui manipulasi atau rekayasa sosial. Temuan ini sejalan dengan penelitian Sahlan dan Nasution yang menyatakan bahwa tingkat kesadaran privasi data memiliki hubungan yang erat dengan perilaku penggunaan layanan keuangan digital, di mana rendahnya kesadaran privasi meningkatkan kerentanan pengguna terhadap penyalahgunaan data pribadi [15].

Selain perilaku dasar tersebut, pemanfaatan fitur keamanan yang disediakan oleh aplikasi pembayaran digital juga terbukti berkontribusi signifikan dalam meningkatkan perlindungan data pengguna. Aktivasi autentikasi biometrik, penggunaan verifikasi dua faktor, serta pembaruan aplikasi secara berkala berperan penting dalam menutup celah keamanan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab. Pembaruan sistem umumnya mencakup perbaikan kerentanan dan peningkatan mekanisme proteksi terhadap pola serangan terbaru, sehingga pengguna yang mengabaikan pembaruan aplikasi berada pada tingkat risiko keamanan yang lebih tinggi. Di samping itu, penggunaan kata sandi yang unik dan kuat untuk setiap layanan digital dapat meminimalkan dampak kebocoran kredensial lintas platform. Hal ini sejalan dengan temuan Pradana dan Nasution yang menegaskan bahwa keamanan data pribadi dalam penggunaan e-wallet sangat dipengaruhi oleh kombinasi antara teknologi pengamanan yang diterapkan dan kepatuhan pengguna dalam memanfaatkan fitur keamanan yang tersedia [12].

Kesadaran pengguna terhadap ancaman social engineering, seperti phishing dan berbagai bentuk penipuan berbasis rekayasa sosial, berperan besar dalam menjaga keamanan data pribadi di lingkungan transaksi digital. Sikap

DOI: https://doi.org/ 10.31004/riggs.v4i4.5119

waspada dengan menghindari klik pada tautan mencurigakan, memverifikasi identitas pihak yang menghubungi, serta bersikap kritis terhadap permintaan informasi sensitif menjadi bentuk perlindungan non-teknis yang sangat efektif. Temuan ini menegaskan bahwa literasi dan kesadaran keamanan digital merupakan faktor kunci dalam menentukan tingkat perlindungan data pengguna. Oleh karena itu, upaya penguatan keamanan tidak dapat hanya bergantung pada teknologi dan kebijakan penyedia layanan, tetapi juga harus diiringi dengan peningkatan literasi digital pengguna secara berkelanjutan. Hal ini sejalan dengan pandangan Baqis dan Nasution yang menekankan bahwa perlindungan dan keamanan data privasi di era digital membutuhkan keterlibatan aktif pengguna sebagai bagian dari sistem keamanan itu sendiri, bukan sekadar sebagai objek perlindungan [11].

4. Conclusion

Sistem pembayaran digital telah berperan sebagai infrastruktur penting dalam mendukung aktivitas transaksi masyarakat. Layanan ini tidak hanya meningkatkan efisiensi, tetapi juga memperluas akses keuangan melalui proses transaksi yang cepat dan praktis. Penyedia layanan telah mengembangkan berbagai teknologi keamanan seperti enkripsi, autentikasi berlapis, tokenisasi, serta monitoring aktivitas untuk melindungi data dan mencegah penyalahgunaan akun. Upaya tersebut menunjukkan bahwa keamanan telah menjadi komponen utama dalam pengelolaan sistem pembayaran digital. Hasil analisis menunjukkan bahwa risiko kebocoran data tetap berpotensi muncul, terutama pada titik interaksi pengguna dengan sistem. Ancaman banyak berkembang melalui rekayasa sosial, kelalaian dalam menjaga informasi pribadi, dan rendahnya literasi keamanan digital. Hal ini menegaskan bahwa keamanan tidak hanya bergantung pada kekuatan teknologi, tetapi juga pada kedisiplinan penggunaan layanan serta pemahaman pengguna terhadap praktik perlindungan data. Keamanan pembayaran digital perlu dipahami sebagai tanggung jawab bersama. Penyedia layanan perlu terus meningkatkan kualitas implementasi teknologi, memperkuat tata kelola data, serta menyajikan kebijakan privasi yang jelas dan mudah dipahami. Regulator perlu memperkuat pengawasan, memastikan kepatuhan terhadap standar keamanan, dan mendorong transparansi pengelolaan data. Pengguna perlu meningkatkan kesadaran keamanan dengan menjaga kerahasiaan informasi sensitif, memanfaatkan fitur proteksi aplikasi, dan lebih berhati-hati dalam berinteraksi di ruang digital. Secara keseluruhan, penelitian ini menunjukkan bahwa penguatan keamanan sistem pembayaran digital membutuhkan sinergi antara teknologi, regulasi, dan literasi pengguna. Ketiganya saling melengkapi dan menentukan tingkat perlindungan data yang diterima masyarakat. Dengan kolaborasi yang konsisten dan berkelanjutan, sistem pembayaran digital tidak hanya menghadirkan kemudahan transaksi, tetapi juga membangun kepercayaan melalui pengelolaan data yang aman, bertanggung jawab, dan berpihak pada kepentingan pengguna.

Reference

[1] Utomo, B. C., Rahman, A. A. *Analisis Kesadaran Keamanan Data Pribadi pada Pengguna E-Wallet DANA*. JRST. Jurnal Nasional UMP
Pradana, W. Y., Nasution, M. I. P. *Keamanan Data Pribadi dalam Penggunaan E-Wallet Terhadap Ancaman Cyber Crime*. Surplus. YPTB
Monica, A., Yulianti, C., Nurintiara, A. *Upaya Penguatan Hukum Pelindungan Data Pribadi Dalam Keamanan Transaksi Menggunakan Dompet Elektronik*. Padjadjaran Law Review. Jurnal Fakultas Hukum Unpad
[4] Sahlan, M., Nasution, M. I. P. *Hubungan Antara Kesadaran Privasi Data Pribadi dan Penggunaan Layanan PayLater di Kalangan Pengguna E-commerce di Indonesia*. Journal Sains Student Research. E-Jurnal Kampus Akademik
[5] Harahap, P. H. *Perlindungan Data Pribadi dalam Transaksi Digital: Implikasi Regulasi, Keamanan, dan Efisiensi*. Yurisprudentia. Jurnal UIN Syahada
[6] Khoiriah, S., Salsabila, A., Camberra, D. D., dkk. *Keamanan dan Privasi dalam Keuangan Digital*. Jurnal Publikasi Sistem Informasi dan Manajemen Bisnis. Journal Center
[7] Dewi, A. C., Ujianto, E. I. H., Rianto, R. *Electronic Payment Threats and Security: A Systematic Literature Review*. JANAPATI. Jurnal Undiksha
[8] Alvionita, P. A. *Tanggung Jawab Keamanan Data Digital oleh Penyelenggara Sistem Elektronik*. Lex Privatum. Jurnal UNSRAT
[9] Ramon, F., Iriansyah, H., Triana, Y. *Perlindungan Hukum Terhadap Hak Privasi dan Keamanan Data Pribadi dalam E-commerce melalui Aplikasi Online*. Yustisi. Ejournal UIKA Bogor
[10] Akbar, N., Sitorus, H. K., Putra Nasution, M. Y. *Perlindungan Hukum Terhadap Data Diri Konsumen Dalam Transaksi Digital*. Indonesian Journal of Law. Jurnal INTEKOM
[11] Baqis, A. M., Nasution, M. I. P. *Pentingnya Perlindungan dan Keamanan Data Privasi di Era Digital*. Jurnal Manajemen dan Pendidikan Agama Islam. Aripafi Journal
[12] Hashim, A., dkk. *The Research Trend of Security and Privacy in Digital Payment*. Informatics (MDPI). MDPI
[13] Hasibuan, E. S., Putri, E. A. *Perlindungan Keamanan Atas Data Pribadi di Dunia Maya*. Jurnal Hukum Sasana. Ejurnal Ubhara Jaya
[14] Gunung Jati, R. A. F., Alfhito, M. D., Mardiyani. *What Drives Digital Payment Adoption? Examining the Role of Ease of Use, Security, and Trust*. Journal of Enterprise and Development. Berugak Jurnal
[15] Rahmahdhani, D. N., Nasution, M. I. P., Sundari, S. A. *Perlindungan Data Privasi yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking*. JUEB. Jurnal Jomparnd

DOI: https://doi.org/ 10.31004/riggs.v4i4.5119