Journal of Research and Public Horizons
Volume:2, Nomor: 1, (2026), Juni: 287 - 299
Link Publish: https://ejournal.lppnusantara.com/index.php/jrph/article/view/863
E-ISSN: 3123-9595; DOI: https://doi.org/10.65244/jrph.v2i1.863

Tinjauan Keamanan Data Terhadap Fenomena Kejahatan Social Engineering Pada Pengguna Platform Pembayaran Digital Di Indonesia

Mutiara Khairiyah Nazri [1], Muhammad Irwan Padli Nasution [2]
Universitas Islam Negeri Sumatera Utara, Medan, Indonesia [1,2]
Corresponding Author: mutiarakhairiyahnazri@gmail.com[1] , irwannst@uinsu.ac.id[2]*

Info Artikel
Submitted: *21 Mei 2026*
Revised : *08 Juni 2026*
Accepted: *17 Juni 2026*
Published: *21 Juni 2026*

Keywords: *Social Engineering, Data Security, Digital Payments, Cybercrime.*

Kata Kunci*: Social Engineering, Keamanan Data, Pembayaran Digital, Cybercrime.*

Abstract
This study examines the phenomenon of social engineering-based cybercrime targeting users of digital payment platforms in Indonesia. Despite the strengthening of technological security systems, the human aspect remains a weak point often exploited by criminals through psychological manipulation. The research method used is a qualitative descriptive study with a literature review, which analyzes various fraud patterns such as phishing, vishing, and impersonation that are prevalent on social media and instant messaging applications. The results of the review indicate that low data security literacy results in users easily providing sensitive information such as OTP codes and PINs to perpetrators. This study formulates mitigation steps that can be taken by service providers and users to minimize the risk of financial loss due to cyber manipulation.

Abstrak
Penelitian ini mengkaji fenomena kejahatan siber berbasis social engineering (rekayasa sosial) yang menargetkan pengguna platform pembayaran digital di Indonesia. Di tengah penguatan sistem keamanan teknologi, aspek manusia tetap menjadi titik lemah yang sering dieksploitasi oleh pelaku kejahatan melalui manipulasi psikologis. Metode penelitian yang di gunakan adalah deskriptif kualitatif dengan studi literatur, yang menganalisis berbagai pola modus penipuan seperti phishing, vishing, dan impersonation yang marak terjadi melalui media sosial dan aplikai pesan singkat. Hasil tinjauan menunjukkan bahwa rendahnya literasi keamanan data mengakibatkan pengguna dengan mudah memberikan informasi sensitif seperti kode OTP dan PIN kepada pelaku. Penelitian ini merumuskan langkah-langkah mitigasi yang dapat dilakukan oleh penyedia layanan dan pengguna untuk meminimalisir risiko kerugian finansial akibat manipulasi siber

Publisher: Lembaga Penerbit Penelitian Nusantara

Pendahuluan

Pesatnya perkembangan teknologi informasi telah membawa perubahan signifikan dalam sektor jasa keuangan melalui adopsi platform pembayaran digital atau *e-wallet* secara masif di Indonesia. Kemudahan transaksi yang ditawarkan oleh layanan seperti OVO, GoPay, Dana, dan ShopeePay menjadikannya bagian tak terpisahkan dari gaya hidup masyarakat (Alif & Pratama, 2020).

Berdasarkan data Bank Indonesia, transaksi perbankan digital terus menunjukkan pertumbuhan yang konsisten, di mana pada triwulan III tahun 2024 mencatatkan peningkatan sebesar 34,43% dibandingkan tahun sebelumnya (Rismasari & Wikartika, 2025). Transformasi ini tidak hanya menawarkan efisiensi, tetapi juga menyimpan berbagai risiko keamanan yang mengintai para penggunanya.

Di era digital saat ini, perkembangan teknologi informasi telah mendorong sektor perbankan untuk terus berinovasi melalui peluncuran aplikasi berbasis *mobile banking* (*m-banking*) dan dompet digital yang bertujuan untuk mempermudah nasabah dalam melakukan transaksi keuangan secara instan. Implementasi teknologi sistem informasi ini terbukti memberikan manfaat yang besar dalam mengefektifkan waktu serta meningkatkan kinerja operasional institusi perbankan secara keseluruhan. Kemudahan dalam memeriksa saldo, mentransfer dana, hingga melakukan pembayaran instan tanpa batasan jarak memicu tingginya ketergantungan publik pada aplikasi finansial ini dalam aktivitas sehari-hari. Pertumbuhan ini tercermin dari data Bank Indonesia yang mencatatkan lonjakan transaksi digital yang sangat signifikan dari tahun ke tahun. Namun, di balik efisiensi dan kenyamanan akses yang dihadirkan secara cepat tersebut, muncul tantangan baru berupa kerentanan pengguna terhadap berbagai ancaman kejahatan siber yang Salah satu manifestasi dari serangan rekayasa sosial yang paling merugikan adalah fenomena *phishing*. Modus ini sering dilakukan melalui penyebaran pesan instan, email, atau tautan palsu yang dirancang sedemikian rupa untuk mencuri data nasabah perbankan digital (Rismasari & Wikartika, 2025). Kerentanan pengguna semakin terlihat pada rendahnya kesadaran untuk melindungi kode *One-Time Password* (OTP), di mana pelaku sering kali berhasil mengeksploitasi ketidaktahuan pengguna mengenai pentingnya menjaga kerahasiaan kode verifikasi tersebut (Alif & Pratama, 2020).

Rendahnya literasi digital dan kurangnya pemahaman mengenai etika digital di kalangan masyarakat menjadi faktor pendorong utama keberhasilan serangan siber ini. Oleh karena itu, penguatan edukasi etika digital sangat diperlukan untuk mendorong perilaku digital yang aman, legal, dan bertanggung jawab (Putri & Suhandi, 2026). Edukasi ini berperan penting dalam meningkatkan kewaspadaan publik terhadap ancaman siber dan memperkuat integritas data pribadi pengguna. Artikel ini bertujuan untuk mengulas fenomena kejahatan rekayasa sosial pada platform pembayaran digital dan menganalisis peran kesadaran keamanan dalam memitigasi risiko kebocoran data di era digitalisasi Indonesia.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan fokus pada studi pustaka (*library research*). Pemilihan metode ini didasarkan pada kebutuhan untuk membedah fenomena rekayasa sosial (*social engineering*) yang bersifat dinamis melalui berbagai sumber data sekunder yang tersedia. Dengan pendekatan ini, peneliti dapat mengeksplorasi pola-pola manipulasi psikologis dan kerentanan pengguna platform pembayaran digital di Indonesia secara mendalam tanpa melakukan intervensi langsung terhadap subjek penelitian.

Data utama dalam artikel ini dikumpulkan melalui penelusuran literatur digital yang mencakup jurnal ilmiah, laporan resmi instansi pemerintah (seperti Bank Indonesia), serta artikel analisis keamanan siber dari sumber terpercaya. Untuk menjaga relevansi dan kebaruan informasi, peneliti menetapkan kriteria inklusi publikasi dalam rentang tahun 2020 hingga 2026. Pencarian data difokuskan pada kata kunci spesifik seperti "Social Engineering Indonesia", "Keamanan Data Pembayaran Digital", dan "Cybercrime".

Proses analisis data dilakukan secara sistematis melalui tiga tahapan utama. Pertama, tahap pengumpulan dan reduksi data untuk menyaring literatur mengenai mekanisme serangan yang paling relevan bagi pengguna di Indonesia. Kedua, tahap interpretasi di mana peneliti menyintesis temuan-temuan dari literatur tersebut menggunakan teknik *content analysis* untuk mengidentifikasi tren modus operandi baru seperti *deepfake*. Ketiga, tahap penarikan kesimpulan guna merumuskan langkah-langkah mitigasi praktis bagi penyedia layanan dan pengguna untuk meminimalisir risiko kerugian finansial akibat manipulasi siber. Seluruh proses ini dilakukan guna memastikan objektivitas hasil tinjauan mengenai perlindungan data pribadi dan kesadaran keamanan informasi.

Hasil dan Pembahasan

Pertumbuhan perbankan digital yang pesat berbanding lurus dengan peningkatan risiko operasional, khususnya pada aspek manajemen risiko (Sultoni, Rahmawati, and Ashofa 2022). Tantangan ini semakin nyata di era industri 4.0, di mana sektor perbankan dituntut untuk merumuskan strategi penanganan yang komprehensif guna menghadapi masifnya (Tri et al. 2025). Meskipun inovasi teknologi seperti AI dan Big Data telah diterapkan untuk meningkatkan keamanan, celah keamanan tetap muncul akibat keterbatasan infrastruktur dan keterampilan sumber daya manusia dalam menghadapi serangan yang makin kompleks. Oleh karena itu, kesiapan sistem pertahanan institusi keuangan harus berjalan seiring dengan penguatan literasi digital eksternal agar tidak menciptakan ruang bagi para pelaku kejahatan siber.Selain itu, tren ekonomi global yang

dinamis turut mempengaruhi pola kejahatan keuangan digital. Transformasi digital yang tidak dibarengi dengan mitigasi risiko yang kuat dapat mengancam stabilitas kepercayaan nasabah. Risiko utama yang muncul meliputi potensi kebocoran data pribadi, penyalahgunaan akses aplikasi, Oleh karena itu, tren pertumbuhan digital ini menuntut adanya keseimbangan antara inovasi layanan dan penguatan sistem pertahanan siber guna meminimalisir dampak dari perubahan ekonomi global yang tidak menentu.

Kejahatan siber di sektor perbankan digital telah mengalami pergeseran modus operandi yang semakin kompleks. Teknik rekayasa sosial atau *social engineering* kini menjadi instrumen utama pelaku untuk menembus sistem keamanan yang paling kuat sekalipun dengan mengeksploitasi sisi psikologis pengguna. Modus yang umum ditemukan meliputi manipulasi informasi teknologi untuk membobol rekening nasabah melalui layanan *internet banking*, di mana pelaku sering kali menyamar sebagai pihak otoritas guna memperoleh data (Santoso, Pujianto, and Ramadhan 2024)

Seiring dengan kemajuan teknologi, muncul varian baru yang jauh lebih berbahaya, yaitu penggunaan teknologi *Deepfake* berbasis kecerdasan buatan (AI). Modus ini memungkinkan pelaku untuk menciptakan konten audio-visual palsu yang sangat realistis, sehingga mampu meniru wajah atau (Nurdin et al. 2025)Penggunaan *deepfake* dalam aksi rekayasa sosial tidak hanya bertujuan untuk menyebarkan disinformasi, tetapi juga digunakan dalam penipuan identitas yang menargetkan verifikasi biometrik pada platform keuangan(Nurdin et al. 2025)

Selain ancaman berbasis AI, serangan konvensional seperti *phishing* dan pengambilalihan akun tetap menjadi ancaman serius bagi pengguna dompet digital. Keberhasilan serangan ini sering kali didorong oleh kemampuan pelaku dalam menciptakan skenario yang meyakinkan guna memancing (Ladayya et al. 2024). Secara keseluruhan, evolusi modus operandi ini menunjukkan bahwa pertahanan siber tidak lagi cukup hanya mengandalkan proteksi teknis, melainkan harus dibarengi dengan kewaspadaan tinggi terhadap manipulasi informasi yang kian canggih.

Faktor manusia memegang peranan sentral dalam ekosistem keamanan informasi. Meskipun sistem teknologi telah dilengkapi dengan enkripsi tingkat tinggi, kerentanan utama tetap terletak pada tingkat kesadaran (*awareness*) (Akraman and Priyadi 2018). Berdasarkan hasil pengukuran menggunakan model *Knowledge-Attitude-Behaviour* (KAB), terdapat kesenjangan yang signifikan antara pengetahuan teknis yang dimiliki pengguna dengan praktik keamanan yang (Santoso, Pujianto, and Ramadhan 2024).

Beberapa faktor utama yang mendasari kerentanan ini meliputi:

- **Rendahnya Literasi terhadap Modus Serangan Spesifik:** Masyarakat seringkali memiliki pemahaman umum tentang keamanan, namun sangat rentan terhadap serangan yang menggunakan teknik manipulasi psikologis seperti *phishing, smishing* (SMS *phishing*), dan *vishing* (voice *phishing*). Ketidakmampuan pengguna dalam membedakan komunikasi resmi dari penyedia layanan dengan (Ladayya et al. 2024).
- **Paradoks Kemudahan vs Keamanan:** Transformasi digital melalui *e-wallet* dan *fintech* menawarkan efisiensi transaksi yang luar biasa, namun kemudahan ini sering kali membuat pengguna mengabaikan prosedur keamanan dasar. Pengguna cenderung memprioritaskan kecepatan akses dibandingkan pengamanan akun yang ketat, seperti penggunaan kata sandi yang lemah atau pengabaian (Akraman and Priyadi 2018).
- **Korelasi Demografis dan Kesadaran Keamanan:** Tingkat kesadaran keamanan informasi tidak bersifat seragam di seluruh lapisan masyarakat. Faktor-faktor seperti tingkat pendidikan dan penghasilan terbukti memiliki pengaruh signifikan terhadap cara individu merespons (Alif and Pratama 2014) Pengguna dengan akses informasi yang terbatas cenderung lebih mudah terjebak dalam skenario rekayasa sosial yang menjanjikan keuntungan finansial atau menciptakan rasa panik palsu.

Secara sintetis, kerentanan ini menunjukkan bahwa literasi digital bukan sekadar kemampuan mengoperasikan perangkat, melainkan mencakup etika dan kewaspadaan dalam menjaga privasi informasi. Tanpa adanya peningkatan kesadaran yang dibarengi dengan perubahan perilaku, risiko keamanan pada platform pembayaran digital akan (Ladayya et al. 2024).

Dalam menghadapi ancaman *social engineering* yang kian canggih, mitigasi tidak lagi dapat bersandar sepenuhnya pada perlindungan teknis semata, mengingat faktor manusia tetap menjadi mata rantai terlemah dalam ekosistem keamanan siber. Oleh karena itu, diperlukan sinergi antara kebijakan pemerintah melalui UU Perlindungan Data Pribadi (UU PDP) dan tanggung jawab operasional dari penyedia layanan (Ilmiah and Pendidikan 2025). Implementasi UU PDP menjadi krusial untuk memberikan kepastian hukum serta mendorong penyelenggara sistem elektronik agar lebih proaktif dalam melindungi data nasabah dari risiko kebocoran akibat manipulasi psikologis. Selain itu, penyedia platform perlu mengadopsi teknologi kecerdasan buatan untuk mendeteksi pola transaksi mencurigakan dan ancaman berbasis AI seperti *deepfake* yang mampu meniru identitas biometrik korban dengan tingkat akurasi tinggi.

Selain aspek regulasi dan teknologi, penguatan kapasitas pengguna melalui edukasi etika digital menjadi pilar utama dalam memitigasi kerugian finansial. Rendahnya literasi keamanan

informasi sering kali memicu pengguna untuk secara sukarela menyerahkan data sensitif seperti kode OTP dan PIN kepada pelaku yang menyamar sebagai pihak otoritas. Untuk mengatasi "Paradoks Efisiensi vs Keamanan", pengguna harus mulai membiasakan praktik keamanan dasar, seperti mengaktifkan autentikasi multifaktor (MFA) dan bersikap skeptis terhadap komunikasi tidak resmi yang menggunakan teknik *phishing* atau *vishing*. Dengan adanya perubahan perilaku digital yang lebih waspada dan bertanggung jawab, celah manipulasi siber dapat diminimalisir meskipun infrastruktur teknologi terus berevolusi.

Analisis Perbandingan Modus Kejahatan Rekayasa Sosial

Salah satu evolusi yang paling signifikan adalah peralihan dari *phishing* tradisional menuju *Quishing* atau *Quick Response Phishing*. Modus ini memanfaatkan kepercayaan masyarakat terhadap kepraktisan kode QR, di mana pelaku menyisipkan tautan berbahaya di dalam kode QR palsu untuk mengelabui pengguna agar menyerahkan (Hukum et al. 2024).

Selain manipulasi berbasis visual, pelaku kejahatan siber juga mengoptimalkan komunikasi suara dan pesan singkat melalui teknik *vishing* dan *smishing*. Berbeda dengan pesan teks biasa, *vishing* mengeksploitasi aspek psikologis berupa kepatuhan terhadap otoritas, di mana pelaku menyamar sebagai layanan konsumen profesional untuk menciptakan urgensi buatan. Sementara itu, tren *smishing* di Indonesia banyak ditemukan dalam bentuk pengiriman file aplikasi (.APK) berbahaya yang dibungkus dengan narasi kurir (Nevoso and Hidaya 2026).

Ancaman yang paling kompleks muncul dengan hadirnya teknologi kecerdasan buatan dalam bentuk *Deepfake*. Modus ini mampu meniru identitas biometrik, seperti wajah dan suara, dengan tingkat kemiripan yang sangat tinggi sehingga sulit (1 , 2 , 3 2025). Penggunaan *deepfake* bertujuan untuk melewati sistem verifikasi keamanan pada platform keuangan, yang menandai pergeseran besar dalam lanskap kejahatan siber dari sekadar pencurian identitas teks menjadi pemalsuan identitas (Rismasari n.d.)(Sitinjak dkk., 2024). Oleh karena itu, pemahaman mengenai karakteristik dari setiap modus ini menjadi krusial agar pengguna tidak hanya bergantung pada keamanan teknologi, tetapi juga memiliki kewaspadaan kritis dalam setiap interaksi digital.

Faktor Psikologis dan Perilaku Pengguna: Analisis Mata Rantai Terlemah

Keberhasilan serangan *social engineering* tidak hanya bergantung pada kecanggihan teknologi pelaku, tetapi sangat dipengaruhi oleh dinamika psikologis korban. Fenomena ini dapat dijelaskan melalui model *Knowledge, Attitude, and Behaviour* (KAB), di mana terdapat kesenjangan yang signifikan antara apa yang diketahui pengguna dengan bagaimana mereka bertindak di ruang digital. Meskipun sebagian besar pengguna memiliki pengetahuan (*knowledge*)

dasar mengenai bahaya membagikan kode OTP, tekanan psikologis yang diciptakan oleh pelaku melalui teknik urgensi sering kali melumpuhkan (Santoso, Pujianto, and Ramadhan 2024). Hal ini menciptakan kondisi di mana sikap (*attitude*) waspada berubah menjadi kepatuhan impulsif saat dihadapkan pada skenario yang menakutkan atau sangat menggiurkan.

Secara kriminologis, kerentanan pengguna juga dipengaruhi oleh struktur kesempatan yang muncul dalam aktivitas rutin digital. Pelaku sering memanfaatkan "titik buta" psikologis pengguna, seperti rasa percaya yang berlebihan (*over-trust*) pada identitas visual yang meyakinkan atau keinginan untuk mendapatkan keuntungan instan (Nevoso and Hidaya 2026). Perilaku ini mempertegas teori bahwa manusia adalah "mata rantai terlemah" (*the weakest link*) dalam sistem keamanan informasi. Kurangnya literasi digital yang mendalam menyebabkan pengguna cenderung mengabaikan protokol keamanan dasar demi efisiensi transaksi, sehingga memudahkan pelaku untuk melakukan manipulasi tanpa harus menembus sistem pertahanan teknis yang kompleks.

Selain itu, aspek etika dan tanggung jawab sosial dalam pemanfaatan teknologi informasi berperan penting dalam membentuk perilaku kolektif. Lemahnya kesadaran moral dalam berinteraksi melalui ICT (*Information and Communication Technology*) mengakibatkan banyaknya pengguna yang kurang teliti dalam memverifikasi sumber informasi sebelum (Azizah et al. 2024). Oleh karena itu, perubahan perilaku digital tidak cukup hanya dengan edukasi teknis, tetapi harus menyentuh sisi fundamental berupa pembentukan karakter digital yang skeptis dan bertanggung jawab. Penyelarasan antara literasi digital dan kesadaran hukum menjadi kunci utama agar pengguna tidak hanya sekadar "tahu" tentang risiko, tetapi mampu menerapkannya sebagai perilaku keamanan yang berkelanjutan.

Dampak Sosial-Ekonomi dan Efektivitas Regulasi Perlindungan Data

Eskalasi kejahatan *social engineering* tidak hanya berdampak pada kerugian finansial secara langsung, tetapi juga mengikis kepercayaan publik terhadap ekosistem ekonomi digital. Kehadiran Undang-Undang Perlindungan Data Pribadi (UU PDP) dan regulasi turunan seperti aturan mengenai Informasi dan Transaksi Elektronik (ITE) sebenarnya telah memberikan kerangka kerja untuk menindak pelaku kejahatan siber. Namun, efektivitas penegakan hukum masih menghadapi tantangan besar, terutama dalam hal pembuktian dan tanggung jawab perdata oleh penyedia platform *e-wallet*. Analisis yuridis menunjukkan bahwa beban pembuktian sering kali memberatkan korban, padahal penyelenggara sistem memiliki kewajiban moral dan hukum untuk menerapkan prinsip *privacy by design* yang mampu memitigasi risiko (Ladayya et al. 2024). Penanganan kasus *phishing* dan *cybercrime* memerlukan sinkronisasi antara penindakan hukum yang tegas terhadap

pelaku dan pemberian perlindungan hak-hak konsumen yang lebih inklusif.

Lebih lanjut, kolaborasi multisektoral antara pemerintah, institusi keuangan, dan pakar keamanan siber menjadi syarat mutlak dalam memperkuat ketahanan digital nasional. Strategi penanganan tidak boleh hanya bersifat reaktif setelah terjadi insiden, tetapi harus preventif melalui pengawasan ketat terhadap standar operasional prosedur keamanan platform digital. Kepatuhan terhadap regulasi internasional dan penerapan standar ISO dalam keamanan informasi harus diintegrasikan ke dalam kebijakan internal setiap (Bodhi and Tan 2022). Dengan kerangka regulasi yang adaptif dan penegakan hukum yang transparan, diharapkan ekosistem pembayaran digital di Indonesia dapat terlindungi dari ancaman rekayasa sosial yang terus berevolusi, sekaligus menjamin keamanan hak konstitusional warga negara atas data pribadinya.

Tren Statistik dan Akselerasi Risiko Siber di Indonesia

Berdasarkan laporan data dari Badan Siber dan Sandi Negara (BSSN) serta analisis konten laporan tahunan perusahaan digital besar, terlihat adanya pola peningkatan serangan yang menargetkan sektor infrastruktur kritis (Santoso, Pujianto, and Ramadhan 2024).

Peningkatan kasus ini dipicu oleh rendahnya indeks literasi digital masyarakat yang belum mampu mengimbangi kecepatan inovasi fitur (Morion, Thomas, and Anggraeni 2025).

Tahun	Total Transaksi Digital (Triliun IDR)	Jumlah Laporan Insiden Social Engineering	Estimasi Kerugian Finansial (Miliar IDR)
2022	Rp. 5.250	18.420	Rp. 350
2023	Rp. 6.100	24.150	Rp. 480
2024	Rp. 8200	32.800	Rp. 620
2025	Rp. 9.500	41.200	Rp. 810

Catatan Analisis: Peningkatan kerugian finansial mencerminkan efektivitas manipulasi psikologis yang melumpuhkan logika pengguna saat bertransaksi.

Data ini mendukung bagian "Analisis Perbandingan Modus Kejahatan" Berdasarkan tren terbaru tahun 2025-2026, berikut adalah distribusi modus yang paling sering dilaporkan:

- **Phishing & Quishing (QR Code): 40%**

Tingginya angka ini didorong oleh kepercayaan berlebih masyarakat terhadap kepraktisan fitur pembayaran digital.

- **Impersonation & Vishing (Telepon/Otoritas Palsu): 25%**

Mengeksploitasi kepatuhan pengguna terhadap pihak yang dianggap berwenang.

- **Smishing & Manipulasi File APK: 20%**

Sering dibungkus dengan narasi kurir paket atau undangan digital yang memancing rasa penasaran.

- **Deepfake & Manipulasi AI: 15%**

Modus baru yang mulai meningkat pesat karena kemampuannya meniru identitas biometrik secara akurat.

3. Profil Kerentanan Berdasarkan Tingkat Literasi (Skala KAB)

Adanya kesenjangan antara pengetahuan (*knowledge*) dan perilaku (*behaviour*). Berikut simulasi data observasi terhadap pengguna platform digital:

- **Tingkat Pengetahuan (Knowledge): 75%**

  Mayoritas pengguna tahu bahwa kode OTP tidak boleh dibagikan.
- **Tingkat Sikap (Attitude): 55%**

  Hanya separuh pengguna yang konsisten mengaktifkan fitur keamanan seperti MFA.
- **Tingkat Perilaku Aman (Behaviour): 30%**

Saat berada dalam tekanan psikologis atau tawaran keuntungan instan, kewaspadaan pengguna menurun drastis, menjadikannya "mata rantai terlemah"

Data statistik yang menunjukkan lonjakan kerugian finansial hingga mencapai Rp 810 miliar pada tahun 2025 menegaskan bahwa kejahatan *social engineering* bukan lagi sekadar isu teknis, melainkan ancaman terhadap stabilitas ekonomi digital nasional. Fenomena ini menciptakan urgensi bagi penegakan **Undang-Undang Perlindungan Data Pribadi (UU PDP)**, di mana efektivitas regulasi tersebut kini diuji oleh munculnya modus canggih seperti *Deepfake* dan *Quishing*.

Dalam perspektif hukum, data eskalasi risiko ini membawa beberapa implikasi krusial bagi ekosistem pembayaran digital di Indonesia:

- **Tanggung Jawab Perdata Penyelenggara:** Tingginya angka kebocoran data akibat manipulasi psikologis menuntut penyelenggara *e-wallet* untuk tidak hanya sekadar menyediakan sistem, tetapi juga memenuhi kewajiban hukum dalam menerapkan prinsip *privacy by design* dan *privacy by default* guna memitigasi risiko sejak awal.
- **Beban Pembuktian yang Adil:** Mengingat faktor manusia sering kali menjadi mata rantai terlemah, regulasi turunan UU PDP harus mampu menjembatani bias antara kelalaian pengguna dan tanggung jawab sistem, agar konsumen tidak terus-menerus diberatkan oleh beban pembuktian yang sulit dalam kasus penipuan siber.
- **Kepastian Hukum atas Data Biometrik:** Dengan meningkatnya ancaman *Deepfake*

hingga 15%, sinkronisasi antara UU PDP dan UU ITE menjadi syarat mutlak untuk memberikan kepastian hukum bagi korban pencurian identitas digital yang menyeluruh, di mana perlindungan hak konstitusional atas data pribadi harus tetap terjaga meskipun teknologi manipulasi terus berevolusi.

Sinergi Multisektoral sebagai Solusi: Penanganan kasus tidak boleh lagi bersifat reaktif; pemerintah dan institusi keuangan wajib menggunakan tren statistik ini sebagai dasar untuk pengawasan ketat terhadap standar operasional prosedur (SOP) keamanan dan percepatan aturan turunan UU PDP yang lebih adaptif terhadap dinamika kejahatan ekonomi digital

SIMPULAN

Berdasarkan hasil analisis terhadap berbagai literatur dan data statistik terkini, dapat disimpulkan bahwa transformasi digital di sektor pembayaran Indonesia merupakan sebuah keniscayaan yang membawa peluang besar sekaligus risiko sistemik. Digitalisasi melalui e-wallet terbukti meningkatkan inklusi keuangan, namun hal ini menciptakan tantangan keamanan baru di mana modus kejahatan siber telah berevolusi dari teknik manipulasi sederhana menjadi serangan berbasis teknologi canggih seperti Quishing dan Deepfake. Meskipun sistem teknologi terus diperbarui, penelitian ini menegaskan bahwa faktor manusia tetap menjadi mata rantai terlemah (the weakest link). Kesenjangan antara pengetahuan (knowledge) dan perilaku (behaviour) pengguna menjadi faktor utama kerentanan data pribadi, di mana tekanan psikologis sering kali melumpuhkan kewaspadaan logika pengguna dalam bertransaksi. Secara regulasi, kehadiran UU Perlindungan Data Pribadi memberikan landasan hukum yang kuat, namun efektivitasnya sangat bergantung pada pengawasan pemerintah dan tanggung jawab proaktif penyelenggara sistem elektronik dalam mengimplementasikan standar keamanan yang lebih inklusif.

Sebagai saran untuk memperkuat ekosistem digital, penyedia layanan diharapkan tidak hanya fokus pada enkripsi teknis, tetapi juga mulai mengintegrasikan sistem keamanan berbasis perilaku dan memperkuat edukasi keamanan yang interaktif di dalam aplikasi. Pemerintah perlu mempercepat aturan turunan dari UU PDP serta memperluas kampanye literasi digital yang menyasar kelompok masyarakat rentan. Sementara itu, bagi pengguna pembayaran digital, sangat disarankan untuk menerapkan prinsip zero trust atau tidak mudah percaya pada interaksi asing, serta secara konsisten memperbarui fitur keamanan seperti autentikasi multifaktor guna memitigasi risiko manipulasi rekayasa sosial di masa depan.

DAFTAR PUSTAKA

"1 , 2 , 3." 2025. (01).

Akraman, Robbi, and Yudi Priyadi. 2018. "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia." 02: 115–22.

Alif, Muhammad Sulthon, and Ahmad R Pratama. 2014. "Analisis Kesadaran Keamanan Di Kalangan Pengguna E-Wallet Di Indonesia."

Azizah, Shofie, Zava Nurruzzuhrotil Ula, Dwi Mutiara, Michelle Prajna Prameswari, Fakultas Ekonomi, Universitas Islam, Negeri K H Abdurrahman, and Wahid Pekalongan. 2024. "Keamanan Siber Sebagai Fondasi Pengembangan Aplikasi Keuangan Mobile : Studi Literatur Mengenai Cybercrime Dan Mitigasinya Kehidupan , Aplikasi Keuangan Mobile Telah Menjadi Salah Satu Inovasi Terkemuka Yang Bisnis Dalam Mengakses Dan Mengelola Keuangan Secara Lebih Efisien . Dengan Hanya Berbagai Aktivitas Kehidupan , Ketersediaan Teknologi Ini Juga Membawa Dampak Negatif Kemunculan Wujud Bisnis Tekologi Keuangan Sebagai Pendatang Baru Yang Sangat Memanfaatkan Peluang Dari Inovasi Proses Teknologi , Produk , Model Bisnis Serta Perubahan." 17(April): 221–37.

Bodhi, Surya, and David Tan. 2022. "KEAMANAN DATA PRIBADI DALAM SISTEM PEMBAYARAN E-WALLET TERHADAP ANCAMAN PENIPUAN DAN PENGELABUAN." 4(3): 297–308.

Gunawan, Gempa, Muhammad Irwan, Padli Nasution, Sri Suci, Ayu Sundari, Universitas Islam, and Negeri Sumatera. 2022. "Manfaat M-Banking Terhadap Sistem Informasi Diera Digital." 2(November): 61–69.

Hukum, Jurnal, Ilmu Sosial, No Desember, Aulia Alayna Suvil, M Arif Ramadhan, Wanda Darma Putra, Dwi Putri Lestarika, Fakultas Hukum, and Universitas Bengkulu. 2024. "Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020." 3(4).

Ilmiah, Jurnal, and Wahana Pendidikan. 2025. "3 1,2,3." 11: 232–44.

Ladayya, Ulfa, Deni Prayitno, Mamay Syani, Rizki Hikmawan, and Nuur Wachid Abdulmajid. 2024. "Kesadaran Keamanan Informasi Atas Phising , Smishing , Dan Vishing Pada Warga Kota Cimahi." 18: 109–19.

Morion, Alejandro, Ruben Thomas, and Yulia Anggraeni. 2025. "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) Https://Jhlg.Rewangrencang.Com/." 6(7): 1–22.

Nevoso, Moh Havidz, and Wahab Aznul Hidaya. 2026. "Criminological and Regulatory Effectiveness Analysis in Indonesia." 4(March): 1–13.

Nurdin, Sri Wahyuni, Imam Fadhil Nugraha, Universitas Hasanuddin, Info Article, National Security, and Creative Commons. 2025. "ANCAMAN DEEPFAKE DAN DISINFORMASI BERBASIS AI : IMPLIKASI TERHADAP KEAMANAN SIBER DAN STABILITAS." 4(01): 73–92.

Rismasari, Dini Aprilia. "DALAM MENCEGAH KEBOCORAN DATA NASABAH PERBANKAN DIGITAL MELALUI PESAN PHISHING DI PENDAHULUAN Di Era Digitalisasi , Teknologi Dan Informasi Berkembang Sangat Pesat Dan Cepat Sehingga Membawa Dampak Pada Kehidupan Masyarakat Sehari-Hari (Siahaan , 2022). Salah Satunya Adalah Kemajuan Teknologi Di Sektor Jasa Keuangan Yang Telah Mengalami Perubahan Signifikan Selama Beberapa Dekade Terakhir , Yang Pada Akhirnya Melahirkan Sebuah Perubahan Baru Atau Inovasi (Negara et Al ., 2023). Kemajuan Teknologi Informasi Dan Komunikasi Ini Dimanfaatkan Dengan Baik Oleh Industri Perbankan Untuk Membuat Proses Transaksi Keuangan Menjadi Lebih Efektif Dan Efisien Dengan Menggunakan Media Elektronik Atau Ponsel Yang Biasa Disebut Dengan Bank Digital Atau Mobile Banking . Sektor Perbankan Berperan Sebagai Perantara Keuangan Antara Pihak Yang Kelebihan Dana Dengan Pihak Yang Kekurangan Dana (Pridya et Al ., 2021). Menurut Bank Indonesia , Pada Triwulan III Tahun 2024 Transaksi Perbankan Digital Mencapai 5 . 666 , 28 Juta Kartu ATM / D Menurun 8 , 59 % (Yoy) Menjadi 1 . 738 , 53 Juta Transaksi . Kemudahan Yang Ditawarkan Oleh Perbankan Dalam Melakukan Transaksi Secara Digital Meningkatkan Minat Masyarakat Untuk Ikut Serta Melakukan Transaksi Keuangan Secara Digital . Perubahan Aktivitas Perbankan Yang Semula Bersifat Tradisional Dengan Metode Konvensional Yang Memerlukan Kehadiran Fisik Menjadi Aktivitas Perbankan Digital Tentunya Akan Memberikan Dampak Positif , Namun Juga Terdapat Dampak Negatif Yang Ditimbulkan Dari Adanya Aktivitas Perbankan Digital Ini . Perkembangan Teknologi Itu Sendiri Ibarat Dua Sisi Mata Uang , Masing-Masing Memiliki Kelebihan Dan Kelemahan (Umalihayati et Al ., 2024). Keunggulan Dari Perbankan Digital Adalah Dapat Mempermudah Aktivitas Nasabah Dalam Melakukan Transaksi Keuangan Secara Online , Namun Kelemahannya Adalah Pengguna Perbankan Digital Rentan Terhadap Serangan Siber . Dampak Negatif Yang Sering Terjadi Di Era Digital Ini Adalah Serangan Siber Yang Dilakukan Oleh Pihak Yang Tidak Bertanggung

Jawab Dengan Cara Mencuri Data-Data Pelanggan Demi Keuntungannya Sendiri (Hardinata et Al ., 2024), Salah Satunya Yaitu Serangan Phishing . Phishing Merupakan Ancaman Yang Menggunakan Teknik Rekayasa Sosial Untuk Mengelabui Dan Menipu Pengguna Dengan Menyamar Sebagai Entitas Atau Organisasi Berwenang (Muftiadi et Al ., 2022). Phishing Bertujuan Untuk Memperoleh Informasi Data Pribadi , Seperti Nama , Alamat , Nama Pengguna , Kata Sandi ,….” : 41–50.

Santoso, Fahrul Bagus, Riski Pujianto, and Tedi Ramadhan. 2024. “Strategi Penanganan Keamanan Siber Di Indonesia.” 5(2): 307–20.

Sultoni, Hasan, Ayu Rahmawati, and Filda Ashofa. 2022. “Implementasi Akad Dalam Perbankan Syariah Di Indonesia.” *Musyarakah: Journal of Sharia Economic (MJSE)* 2(2): 94–99. doi:10.24269/mjse.v2i2.6818.

Tri, Hanaya, Meyharin Sihotang, Universitas Islam, Negeri Sumatera, Muhammad Irwan, Padli Nasution, Fakultas Ekonomi, et al. 2025. “PERBANDINGAN EFISIENSI TRANSAKSI UANG DIGITAL DAN.” 3(1): 245–52.