Nusantara Education and Innovation Journal
NOVARA
P-ISSN: xxxx-xxxx E-ISSN: xxxx-xxx

Serangan dan Perlindungan Data Pribadi di Media Sosial: Apa yang Harus Diketahui Pengguna di Indonesia

Akhmad Maulana[1*], Ahmad Fadhel Syakir Hidayat[2]
[1,2] Universitas Islam Sultan Aji Muhammad Idris Samarinda

Article History:
Received: 10 December 2024
Accepted: 27 January 2025
Published: 27 February 2025

Kata Kunci:
data pribadi, media sosial, keamanan digital, privasi pengguna, perlindungan data, Indonesia

Keywords:
personal data, social media, digital security, user privacy, data protection, Indonesia.

A B S T R A K

Perkembangan pesat media sosial di Indonesia meningkatkan kenyamanan interaksi digital, tetapi sekaligus menajamkan risiko serangan terhadap data pribadi pengguna. Penelitian ini bertujuan mengidentifikasi pola serangan siber yang umum terjadi di media sosial, menganalisis tingkat kesadaran dan perilaku perlindungan pengguna, serta merumuskan strategi pengamanan data pribadi yang dapat diterapkan secara praktis. Penelitian menggunakan metode kualitatif deskriptif melalui kajian literatur terkini mengenai phishing, social engineering, account hijacking, serta serangan berbasis kecerdasan buatan seperti deepfake dan zero-click malware. Hasil kajian menunjukkan masih adanya kesenjangan signifikan antara pengetahuan risiko dan praktik keamanan sehari-hari, terutama dalam pengelolaan kata sandi, pengaturan privasi, dan pengendalian akses aplikasi pihak ketiga. Studi ini merekomendasikan penguatan literasi keamanan siber, pemanfaatan fitur keamanan seperti autentikasi dua faktor, serta kolaborasi antara pemerintah, platform digital, dan masyarakat untuk membangun ekosistem media sosial yang lebih aman dan bertanggung jawab.

A B S T R A C T

The rapid growth of social media in Indonesia enhances digital interaction convenience but simultaneously heightens risks to users' personal data security. This study aims to identify prevalent cyberattack patterns on social media, analyze users' awareness levels and protective behaviors, and formulate practical personal data protection strategies. Employing a descriptive qualitative method through a literature review, the research examines common threats including phishing, social engineering, account hijacking, and AI-based attacks such as deepfake and zero-click malware. Findings reveal a significant gap between users' knowledge of risks and actual security practices, particularly in password management, privacy settings, and third-party app access control. The study recommends strengthening cybersecurity literacy, utilizing security features like two-factor authentication, and fostering collaboration among government, digital platforms, and society to create a safer, more responsible social media ecosystem.

Citation: Maulana, A. & Hidayat, A.F.S, (2025). Serangan dan Perlindungan Data Pribadi di Media Sosial: Apa yang Harus Diketahui Pengguna di Indonesia. *Nusantara Education and Innovation Journal*, 2*(1),* 39-48. https://doi.org/10.64093/novara.v2i1.444

**** Corresponding Author:***
Akhmad Maulana: akhmadmaulana@gmail.com

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang sangat pesat telah mengubah cara manusia berinteraksi, berkomunikasi, dan membangun identitas diri di ruang digital, salah satunya melalui media sosial. Platform seperti Facebook, Instagram, X (Twitter), dan TikTok tidak hanya menjadi sarana berbagi informasi, tetapi juga ruang utama pembentukan jejaring sosial, ekspresi diri, hingga aktivitas ekonomi. Di balik berbagai kemudahan tersebut, media sosial menyimpan risiko serius terhadap keamanan dan privasi data pribadi pengguna karena banyaknya informasi sensitif yang dibagikan secara terbuka maupun semi-terbuka kepada pihak lain. Data yang terpapar di media sosial berpotensi dimanfaatkan untuk pencurian identitas, penipuan, maupun berbagai bentuk serangan siber yang menimbulkan kerugian materiil maupun immateriil bagi pengguna(Dewangan et al., 2024).

Secara global, jumlah pengguna media sosial terus meningkat dari tahun ke tahun dan diikuti oleh naiknya intensitas aktivitas daring individu. Laporan terkini menunjukkan bahwa pengguna aktif media sosial telah mencapai miliaran orang di seluruh dunia, dan Indonesia termasuk dalam kelompok negara dengan tingkat penetrasi media sosial yang tinggi. Kondisi ini menjadikan pengguna Indonesia sangat terekspos pada berbagai ancaman keamanan digital, terutama ketika praktik pengelolaan data pribadi belum dilakukan secara bijak. Sejumlah insiden kebocoran data dan penyalahgunaan informasi pribadi yang melibatkan platform besar menunjukkan bahwa pengelolaan keamanan data tidak hanya menjadi masalah teknis, tetapi juga menyangkut kesadaran, perilaku, serta tata kelola data di tingkat individu, institusi, dan negara(Harakan et al., 2024).

Ancaman terhadap data pribadi di media sosial tidak hanya berasal dari kelemahan teknis sistem, tetapi juga dari pola serangan siber yang semakin kompleks. Berbagai penelitian mencatat maraknya serangan seperti phishing, social engineering, dan pengambilalihan akun (account hijacking) yang memanfaatkan kelengahan pengguna dalam mengelola kredensial dan pengaturan privasi. Perkembangan kecerdasan buatan turut melahirkan bentuk ancaman baru, antara lain deepfake dan zero-click malware yang mampu mengeksploitasi celah keamanan tanpa interaksi langsung dari korban. Di sisi lain, perilaku oversharing informasi pribadi, penggunaan kata sandi yang lemah dan berulang, serta ketidakhati-hatian dalam memberikan izin aplikasi pihak ketiga memperbesar peluang terjadinya kebocoran data.(*Ath-Thariq ; Jurnal Dakwah Dan Komunikasi, Vol. 06, No. 02, Juli-Desember 2022 220*, 2022)

Di Indonesia, isu perlindungan data pribadi mendapatkan perhatian khusus melalui lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menegaskan hak subjek data dan kewajiban pengendali data dalam menjaga keamanan informasi pribadi. Namun, implementasi regulasi ini masih menghadapi berbagai tantangan, antara lain rendahnya literasi keamanan siber, keterbatasan pengawasan, serta belum meratanya pemahaman mengenai konsekuensi hukum pelanggaran perlindungan data. Banyak pengguna media sosial yang menyadari adanya risiko siber, tetapi belum mengubah perilaku sehari-hari dalam mengelola akun dan data pribadi secara konsisten.(Firdaus & Wardhani, 2024)

Berdasarkan kondisi tersebut, terdapat kesenjangan antara meningkatnya kompleksitas serangan siber di media sosial dan tingkat kesiapan pengguna dalam melindungi data pribadi mereka. Banyak kajian sebelumnya fokus pada aspek teknis serangan atau aspek regulasi, namun relatif sedikit yang secara komprehensif menggabungkan pembahasan tentang pola serangan, tingkat kesadaran pengguna, dan strategi perlindungan praktis dalam konteks pengguna media sosial di Indonesia. Oleh karena itu, penelitian ini bertujuan untuk: (1) mengidentifikasi pola dan jenis serangan terhadap data pribadi di media sosial, (2) menganalisis tingkat kesadaran dan perilaku perlindungan pengguna, dan (3) merumuskan strategi perlindungan data pribadi yang dapat diterapkan oleh pengguna agar mampu memanfaatkan media sosial secara lebih aman dan bertanggung jawab(Al et al., 2023).

B. Tinjauan Pustaka

Konsep data pribadi dan privasi, jenis serangan siber di media sosial, serta literasi digital dan perilaku perlindungan pengguna (Dewangan et al., 2024). Data pribadi di media sosial mencakup informasi yang dapat mengidentifikasi individu, mulai dari identitas dasar hingga jejak aktivitas digital, yang menjadi sangat rentan karena pola berbagi informasi yang masif dan sering kali terbuka (Harakan et al., 2024). Dalam konteks Indonesia, perlindungan data pribadi telah memperoleh landasan hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), namun efektivitasnya masih bergantung pada tingkat pemahaman dan kepatuhan para pemangku kepentingan, termasuk pengguna media sosial sendiri (Firdaus & Wardhani, 2024).

Berbagai studi yang dikaji menunjukkan bahwa media sosial menjadi target utama serangan seperti phishing, social engineering, dan pengambilalihan akun (account hijacking), dengan phishing yang kerap memanfaatkan tautan atau halaman palsu untuk mencuri kredensial (Ansyafa et al., 2024). Teknik *social engineering* umumnya menggunakan manipulasi psikologis melalui *pretexting* dan *impersonation* sehingga korban bersedia memberikan informasi sensitif (Souhoka et al., 2025). Pengambilalihan akun sering berkaitan dengan penggunaan ulang kata sandi (*credential reuse*) dan credential stuffing yang memanfaatkan data kebocoran dari platform lain (Sujiwana et al., 2024). Perkembangan teknologi juga memunculkan ancaman baru berbasis kecerdasan buatan seperti deepfake, yang mampu memalsukan konten audio-visual untuk menipu korban, serta serangan *zero-click malware* yang dapat mengeksploitasi celah tanpa interaksi pengguna dan menyebabkan kebocoran data secara diam-diam (Marpaung, 2025).

Di sisi lain, literasi digital berperan penting dalam menentukan bagaimana pengguna memahami risiko dan menerapkan praktik perlindungan data pribadi di media sosial; penelitian menunjukkan hubungan positif antara tingkat literasi digital dan adopsi praktik keamanan seperti autentikasi dua faktor (Saputra et al., 2023). Hasil-hasil penelitian yang dirangkum dalam naskahmu menunjukkan adanya kesenjangan antara pengetahuan dan praktik: banyak pengguna menyadari risiko serangan siber namun masih melakukan oversharing (Pudjiarti et al., 2023), menggunakan kata sandi lemah, serta jarang meninjau pengaturan privasi dan izin aplikasi pihak ketiga (Farooqi et al., 2020). Kajian tersebut juga menegaskan bahwa pengguna dengan literasi digital lebih baik cenderung mengaktifkan autentikasi dua faktor, lebih selektif terhadap permintaan pertemanan dan tautan mencurigakan, serta lebih peka terhadap indikasi *social engineering* (Noviyanti et al., 2025). Di tingkat struktural, literatur yang dikaji menekankan pentingnya kombinasi edukasi keamanan siber, pemanfaatan fitur keamanan digital, regulasi perlindungan data yang kuat, dan kolaborasi antara pemerintah, penyedia platform, serta masyarakat untuk membangun ekosistem media sosial yang aman dan bertanggung jawab.

C. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif berbasis kajian literatur untuk menggambarkan pola serangan terhadap data pribadi di media sosial, menilai tingkat kesadaran pengguna, serta merumuskan strategi perlindungan yang relevan bagi konteks Indonesia (Dewangan et al., 2024). Pendekatan ini dipilih karena masalah yang dikaji bersifat konseptual dan kontekstual, sehingga memerlukan pengintegrasian temuan dari berbagai studi empiris dan kajian teoretis untuk memperoleh pemahaman komprehensif.

Sumber data dalam penelitian ini terdiri atas artikel jurnal, prosiding konferensi, laporan institusi, serta dokumen kebijakan yang relevan dengan topik perlindungan data pribadi, serangan siber pada media sosial, dan literasi digital. Sumber-sumber utama diperoleh dari daftar pustaka awal artikel ini dan dilengkapi dengan publikasi lain yang

terbit dalam rentang waktu terbaru, guna menggambarkan perkembangan mutakhir terkait ancaman siber dan kebijakan perlindungan data yang berlaku.

Kriteria inklusi dalam kajian ini mencakup publikasi yang membahas serangan siber pada platform media sosial atau perlindungan data pribadi, baik dalam bentuk kajian empiris maupun tinjauan literatur, dengan fokus pada konteks Indonesia atau memiliki relevansi praktis bagi pengguna di Indonesia, serta diterbitkan dalam rentang waktu yang dianggap mutakhir. Sementara itu, kriteria eksklusi meliputi sumber non-ilmiah yang tidak memiliki metodologi yang jelas, referensi populer yang tidak dapat diverifikasi, serta dokumen yang tidak membahas aspek teknis, perilaku, atau regulasi yang relevan dengan topik kajian.

Proses pengumpulan dan seleksi literatur dilakukan melalui penelusuran pada basis data akademik serta sumber-sumber yang tercantum dalam pustaka awal naskah. Tahap awal seleksi dilakukan dengan menelaah judul dan abstrak untuk menentukan tingkat relevansi, kemudian dilanjutkan dengan pembacaan teks penuh terhadap artikel yang memenuhi kriteria. Tahapan utama dalam proses ini meliputi identifikasi literatur, penyaringan awal, seleksi berdasarkan judul dan abstrak, penilaian full-text, ekstraksi tema, serta sintesis tematik.

Untuk meningkatkan validitas dan keandalan temuan, penelitian ini menerapkan triangulasi sumber dengan membandingkan hasil dari berbagai jenis publikasi, seperti artikel jurnal, laporan institusi, dan dokumen kebijakan. Keandalan data diperkuat melalui dokumentasi yang sistematis terhadap proses seleksi dan ekstraksi data, serta interpretasi temuan yang dilakukan secara hati-hati dengan merujuk langsung pada bukti yang terdapat dalam literatur primer. Keterbatasan metode ini terletak pada ketergantungannya terhadap kualitas dan ketersediaan literatur yang ada, sehingga penelitian lanjutan disarankan untuk menggunakan pendekatan empiris, seperti survei atau studi kasus, guna menguji temuan secara kuantitatif.

D. Hasil Penelitian

Kajian literatur sistematis mengidentifikasi tiga pola serangan siber dominan terhadap data pribadi di media sosial yang paling sering dilaporkan dalam studi terkini. Phishing menjadi ancaman utama melalui pembuatan halaman login palsu yang identik dengan tampilan resmi platform, pesan otomatis berisi tautan berbahaya, serta iklan palsu yang mengarahkan korban ke situs penipuan; teknik ini semakin efektif karena memanfaatkan rasa urgensi dan kepercayaan pengguna terhadap notifikasi resmi (Ansyafa et al., 2024). Social engineering melibatkan manipulasi psikologis melalui pretexting (skenario palsu), impersonasi figur terpercaya atau kerabat, serta pesan pribadi yang dibuat sangat personal untuk membujuk korban memberikan kredensial secara sukarela. Account hijacking paling sering terjadi melalui credential stuffing, di mana kata sandi yang bocor dari kebocoran data platform lain dimanfaatkan untuk meretas akun media sosial, terutama karena kebiasaan pengguna memakai password serupa di berbagai layanan.

Analisis terhadap perilaku pengguna mengungkap kesenjangan signifikan antara pemahaman risiko dan implementasi praktik keamanan sehari-hari. Sebanyak 70% responden dalam survei literatur menyatakan mengetahui bahaya phishing dan peretasan akun, namun hanya 30% secara konsisten menerapkan pengaturan privasi ketat atau memverifikasi tautan sebelum diklik; perilaku oversharing informasi seperti lokasi real-time, tanggal lahir, dan hubungan keluarga menjadi pintu masuk utama bagi rekayasa sosial dan reset password otomatis (Pudjiarti et al., 2023). Kelompok usia muda (18-25 tahun) dengan intensitas penggunaan media sosial rata-rata 4 jam per hari menunjukkan kerentanan tertinggi, sementara pengguna dengan literasi digital rendah kesulitan membedakan akun asli dan tiruan, sehingga lebih rentan terhadap impersonasi dan pesan manipulatif.

Strategi perlindungan yang terbukti efektif mencakup pendekatan berlapis mulai dari tingkat individu hingga struktural. Autentikasi dua faktor (2FA) terbukti menurunkan

risiko hijacking hingga 90% ketika dikombinasikan dengan password manager untuk menghasilkan kata sandi unik per platform; pembatasan izin aplikasi pihak ketiga dan pemantauan aktivasi login secara berkala juga direkomendasikan sebagai praktik wajib (Farooqi et al., 2020). Di tingkat sistemik, penguatan regulasi seperti UU PDP No. 27/2022 memerlukan dukungan edukasi literasi digital masif melalui sekolah dan kampanye publik, serta kolaborasi pemerintah-platform-masyarakat untuk menerapkan enkripsi end-to-end dan transparansi algoritma, sehingga membentuk ekosistem media sosial yang lebih aman bagi pengguna Indonesia.

E. Pembahasan

Pola dan Jenis Serangan Siber di Media Sosial

Serangan siber pada media sosial menunjukkan pola yang semakin kompleks dan terstruktur seiring meningkatnya aktivitas digital masyarakat. Serangan yang paling dominan phishing, social engineering, dan pengambilalihan akun tidak lagi berdiri sendiri, tetapi saling berkelindan dengan teknik manipulasi psikologis serta eksploitasi data pribadi yang dipublikasikan pengguna. phishing modern memanfaatkan halaman palsu yang dirancang menggunakan teknik *pixel-perfect cloning*, sehingga tampak identik dengan tampilan resmi platform seperti Instagram dan Facebook. Kemiripan ini semakin diperkuat dengan penggunaan *automated notification*, yaitu pesan yang seolah dikirim oleh sistem untuk menciptakan kesan urgensi misalnya ancaman penangguhan akun, verifikasi login mencurigakan, atau peringatan pelanggaran kebijakan. Strategi ini efektif karena memicu reaksi emosional, membuat korban bertindak cepat tanpa sempat memeriksa URL atau sumber pesan (Ansyafa et al., 2024).

Selain phishing, serangan social engineering berkembang menjadi ancaman yang lebih sulit dideteksi. (Richardo, 2025) menekankan bahwa pelaku memanfaatkan identitas palsu yang disesuaikan dengan karakteristik target berdasarkan riwayat interaksi publik di media sosial. Pola komentar, daftar pertemanan, hingga kebiasaan unggahan digunakan untuk membangun narasi kepercayaan (*trust-building attack*). Teknik seperti impersonasi, *pretexting*, serta manipulasi pesan pribadi semakin mudah dilakukan karena pengguna cenderung membagikan informasi pribadi secara terbuka. Temuan (Dewangan et al., 2024) menyoroti bahwa oversharing mulai dari lokasi terkini, rutinitas harian, hingga informasi keluarga memberi pelaku *contextual clues* yang memudahkan penyusunan skenario penipuan yang tampak realistis. Akibatnya, korban tidak hanya memberikan data pribadi secara sukarela tetapi juga kerap menyerahkan akses akun tanpa sadar.

Di sisi lain, serangan account hijacking meningkat drastis akibat lemahnya manajemen kata sandi. (Sujiwana et al., 2024) menemukan bahwa lebih dari separuh korban menggunakan ulang password yang sama pada berbagai platform, sehingga ketika satu layanan mengalami kebocoran data, pelaku dapat dengan mudah menjalankan *credential stuffing* untuk mengambil alih akun lain. Fenomena ini sejalan dengan temuan (Fitriyani, 2025) yang menunjukkan bahwa pembajakan akun WhatsApp sering dipicu oleh penggunaan kata sandi sederhana, tidak diperkuat dengan autentikasi dua faktor, serta minimnya kebiasaan melakukan monitoring login. Bentuk serangan ini lebih berbahaya karena memungkinkan pelaku mengakses pesan pribadi, daftar kontak, hingga memulai percakapan penipuan yang memanfaatkan identitas korban.

Selain serangan tradisional, ancaman berbasis kecerdasan buatan mulai meramaikan lanskap kejahatan digital di media sosial. Teknologi seperti deepfake, bot infiltrasi, dan *zero-click malware* memungkinkan pelaku mengotomatisasi serangan dan meningkatkan tingkat keberhasilan. (Harakan et al., 2024) memperingatkan bahwa bot otomatis kini digunakan untuk menyebarkan tautan berbahaya, menyerang kotak masuk pengguna secara masif, dan memindai kerentanan akun. Sementara itu, *zero-click malware* memungkinkan infiltrasi perangkat tanpa interaksi pengguna sama sekali, menjadikannya salah satu ancaman paling sulit dideteksi. (Marpaung, 2025) menegaskan

bahwa teknologi deepfake mempermudah pelaku memproduksi suara atau wajah yang mirip individu asli, sehingga pesan manipulatif seperti permintaan uang, file sensitif, atau kode verifikasi tampak benar-benar berasal dari orang terdekat.

Secara keseluruhan, pola serangan siber di media sosial tidak lagi bersifat linear, tetapi membentuk *multi-vector threat model* yang menggabungkan rekayasa teknis, rekayasa psikologis, dan eksploitasi data publik. Hal ini menjadikan pengguna sebagai titik lemah utama sekaligus pintu masuk serangan, terutama apabila praktik keamanan digital masih rendah dan informasi pribadi dibagikan secara tidak terkendali.

Faktor Kerentanan dan Tingkat Kesadaran Pengguna

Kerentanan Kerentanan pengguna terhadap serangan siber dipengaruhi oleh berbagai faktor individual dan sistemik seperti literasi digital, kebiasaan berbagi informasi, serta persepsi risiko yang rendah terhadap ancaman dunia maya (Pudjiarti et al., 2023). Meskipun sebagian besar pengguna sudah mengenal istilah phishing, hanya sedikit yang mampu mengidentifikasi tautan palsu atau membedakan pesan berbahaya dari pesan resmi platform secara konsisten (Noviyanti et al., 2025). Kondisi ini menunjukkan adanya kesenjangan antara pengetahuan teoretis dan praktik keamanan digital di kehidupan sehari-hari.

Fenomena oversharing informasi pribadi di media sosial juga menjadi pemicu utama meningkatnya kerentanan pengguna karena unggahan foto, lokasi, identitas keluarga, dan aktivitas harian dapat digunakan pelaku untuk membangun skenario rekayasa sosial yang meyakinkan (Pengguna et al., 2025). Banyak pengguna masih menganggap bahwa informasi seperti check-in lokasi atau foto rumah bukanlah data sensitif sehingga mereka membagikannya secara publik, padahal data tersebut dapat dijadikan konteks tambahan oleh pelaku untuk memperkuat teknik impersonasi atau pretexting (Sari & Fitri, 2025).

Selain itu, persepsi risiko yang rendah menyebabkan sebagian besar pengguna merasa dirinya bukan target serangan, sehingga mereka tidak melakukan tindakan pencegahan seperti mengaktifkan autentikasi dua faktor atau memeriksa izin aplikasi pihak ketiga (Fitriyani, 2025). Faktor pendidikan dan pengalaman digital juga berperan besar dalam menentukan tingkat kewaspadaan, di mana pengguna dengan literasi rendah cenderung mengabaikan peringatan keamanan dan menerima permintaan akses data tanpa membaca ketentuan secara utuh (*Ath-Thariq ; Jurnal Dakwah Dan Komunikasi, Vol. 06, No. 02, Juli-Desember 2022 220*, 2022).

Faktor sistemik pun tidak kalah penting karena banyak kasus kebocoran data terjadi akibat kelemahan keamanan internal platform, seperti enkripsi yang tidak memadai, lemahnya kontrol akses, atau kurangnya audit keamanan berkala yang seharusnya melindungi data pengguna (Lesmana & Nasution, 2025). Selain itu, penyedia platform sering kali tidak memberikan edukasi keamanan yang jelas dan mudah dipahami, sehingga pengguna tidak dibekali pemahaman yang memadai mengenai cara mengelola risiko atau mengenali tanda-tanda serangan (Sitorus et al., 2025).

Secara keseluruhan, kerentanan pengguna berasal dari kombinasi antara kurangnya pengetahuan praktis, perilaku berbagi informasi yang tidak terkontrol, persepsi ancaman yang rendah, serta lemahnya dukungan sistem keamanan dari platform digital itu sendiri. Kondisi ini menunjukkan bahwa upaya mitigasi harus dilakukan secara menyeluruh, bukan hanya berfokus pada edukasi pengguna, tetapi juga pada peningkatan transparansi dan tanggung jawab keamanan di tingkat platform dan regulator nasional.

Dampak Serangan terhadap Keamanan Data Pribadi

Serangan Serangan siber yang menargetkan akun media sosial memiliki dampak yang luas terhadap keamanan data pribadi, stabilitas identitas digital, dan kepercayaan publik terhadap platform digital. Salah satu ancaman terbesar muncul ketika aplikasi pihak ketiga memperoleh akses berlebihan terhadap data pengguna, sering kali melalui persetujuan otomatis tanpa pemahaman yang memadai. Hal ini memungkinkan data

sensitif seperti kontak, lokasi, pola aktivitas, hingga pesan pribadi diproses, disimpan, atau diperjualbelikan tanpa kontrol pengguna yang memadai (Farooqi et al., 2020). Kondisi ini memperlihatkan bahwa pengguna sering kali tidak menyadari bahwa otorisasi sederhana dapat membuka celah besar bagi penyalahgunaan data.

Kebocoran data pribadi membawa konsekuensi lebih lanjut berupa pencurian identitas, pengambilalihan akun finansial, dan manipulasi sosial dalam skala besar. Big data yang tersedia di media sosial dapat dimanfaatkan oleh pelaku untuk melakukan *profiling* yang sangat detail, sehingga memudahkan personalisasi pesan penipuan atau rekayasa sosial yang sulit dibedakan dari aktivitas asli. Lemahnya pola kata sandi memperburuk situasi karena kombinasi password yang sederhana atau digunakan ulang memungkinkan pelaku mengakses akun inti korban, termasuk akun perbankan atau layanan pembayaran digital, yang dapat menyebabkan kerugian finansial langsung (Ramadhani et al., 2024).

Dampak serangan juga terlihat pada aspek sosial dan psikologis pengguna. Serangan yang menyasar akun media sosial sering kali tidak berhenti pada pencurian data, tetapi berlanjut pada penyebaran konten palsu, penipuan terhadap keluarga korban, dan manipulasi identitas digital yang dapat merusak reputasi individu. Banyak kasus menunjukkan bahwa pembajakan akun WhatsApp digunakan pelaku untuk menghubungi kerabat korban dengan alasan darurat atau permintaan transfer uang, sehingga menimbulkan kerugian sosial dan ekonomi secara bersamaan. Peristiwa semacam ini menunjukkan bahwa dampak serangan siber tidak hanya dirasakan oleh korban langsung, tetapi juga oleh jaringan sosial terdekatnya.

Selain merugikan individu, serangan siber berkontribusi pada menurunnya kepercayaan publik terhadap platform digital. Ketika terjadi pelanggaran data dalam skala besar, publik cenderung meragukan komitmen platform dalam menjaga keamanan dan privasi penggunan (Firdaus & Wardhani, 2024). Kurangnya transparansi mengenai bagaimana data disimpan, diproses, dan diamankan menambah kecemasan pengguna, terutama jika penyedia layanan tidak menunjukkan langkah pemulihan yang jelas. Penelitian lain mengungkapkan bahwa banyak platform digital masih memiliki celah kepatuhan terkait regulasi perlindungan data, sehingga penerapan kebijakan keamanan sering tidak konsisten dengan standar yang ditetapkan pemerintah (Kurniasandi et al., 2022).

Secara keseluruhan, dampak serangan siber terhadap keamanan data pribadi bersifat multidimensional, mencakup kerugian finansial, gangguan emosional, kerusakan reputasi, serta hilangnya kepercayaan terhadap platform digital. Situasi ini menunjukkan perlunya kombinasi pendekatan teknis, edukatif, dan regulatif untuk melindungi integritas identitas digital pengguna secara menyeluruh.

Strategi Perlindungan dan Penguatan Regulasi

Perlindungan data pribadi di media sosial memerlukan strategi berlapis yang mencakup edukasi pengguna, teknologi keamanan, serta kebijakan regulatif yang kuat. Edukasi literasi digital menjadi fondasi utama karena pengguna merupakan garda terdepan dalam mencegah serangan. Peningkatan pemahaman mengenai pola ancaman, tipe serangan, dan tanda-tanda phishing terbukti dapat menurunkan risiko secara signifikan (Saputra et al., 2023).

Langkah pengamanan teknis seperti autentikasi dua faktor (2FA), pembatasan izin aplikasi pihak ketiga, pengaturan privasi ketat, serta penggunaan password manager menjadi sangat penting dalam menjaga keamanan identitas digital. Penerapan prinsip kombinatorik dalam pembuatan kata sandi kompleks membuat password lebih sulit diprediksi oleh teknik brute force maupun credential stuffing (Ritonga et al., 2025). Selain itu, aktivasi autentikasi dua faktor secara konsisten telah terbukti mampu menurunkan potensi pembajakan akun lebih dari 90 persen karena pelaku memerlukan bukti kepemilikan tambahan selain kata sandi biasa (Fitriyani, 2025).

Dari sisi regulasi, Undang-Undang Perlindungan Data Pribadi (UU PDP) menjadi dasar hukum nasional dalam mengatur mekanisme pemrosesan data, kewajiban pengendali data, dan hak subjek data. Namun implementasinya masih menghadapi sejumlah hambatan, terutama terkait standar teknis keamanan, praktik enkripsi, pembatasan pengumpulan data, dan transparansi algoritma yang digunakan platform digital. Tantangan lain muncul karena masih ditemukannya celah kepatuhan dalam sektor e-commerce dan media sosial yang menyebabkan penerapan regulasi bersifat administratif dan belum sepenuhnya efektif (Kurniasandi et al., 2022).

Di tingkat kolaboratif, perlindungan data pribadi memerlukan keterlibatan banyak pihak, termasuk pemerintah, penyedia platform, akademisi, dan masyarakat luas. Kolaborasi lintas sektor dibutuhkan untuk membangun ekosistem digital yang aman dan berkelanjutan melalui edukasi, literasi keamanan, serta transparansi kebijakan data (Jering, 2025). Selain itu, sinergi dengan penyedia platform penting dilakukan untuk memperkuat metode verifikasi, mengurangi penyalahgunaan data pihak ketiga, serta meningkatkan kualitas sistem deteksi dini terhadap aktivitas mencurigakan.

Upaya mitigasi yang berlapis mulai dari edukasi pengguna, penerapan teknologi keamanan yang mudah digunakan, hingga regulasi yang efektif menjadi kunci utama dalam membangun budaya keamanan digital yang kuat. Dengan pendekatan komprehensif ini, risiko serangan siber dapat ditekan, sementara kepercayaan publik terhadap platform digital dapat meningkat secara signifikan.

F. Simpulan

Serangan siber pada media sosial menunjukkan pola yang semakin kompleks karena menggabungkan eksploitasi teknis dengan manipulasi psikologis. Phishing, social engineering, dan account hijacking menjadi bentuk serangan paling dominan karena memanfaatkan celah keamanan platform sekaligus perilaku pengguna yang cenderung abai terhadap risiko. Ancaman modern berbasis kecerdasan buatan seperti deepfake, bot otomatis, dan zero-click malware semakin memperburuk kondisi keamanan digital dengan meningkatkan tingkat keberhasilan serangan tanpa memerlukan interaksi korban.

Kerentanan pengguna sangat dipengaruhi oleh tingkat literasi digital, perilaku oversharing, dan persepsi risiko yang rendah. Meskipun sebagian pengguna memahami istilah dasar seperti phishing, banyak yang tidak mampu mengidentifikasi ancaman secara praktis, sehingga celah antara pengetahuan dan perilaku protektif tetap tinggi. Faktor pendidikan, pengalaman digital, serta minimnya edukasi dari platform turut memperbesar risiko tersebut.

Dampak serangan tidak hanya dirasakan dalam bentuk kebocoran data pribadi, tetapi juga mencakup pencurian identitas, kerugian finansial, kerusakan reputasi digital, dan menurunnya kepercayaan publik terhadap platform digital. Kasus penyalahgunaan data oleh aplikasi pihak ketiga, pemanfaatan big data untuk profiling, serta pengambilalihan akun yang berujung pada penipuan kepada keluarga korban menunjukkan bahwa ancaman siber memiliki konsekuensi sosial yang luas.

Upaya perlindungan data pribadi membutuhkan pendekatan berlapis yang melibatkan edukasi literasi digital, penguatan teknologi keamanan, dan regulasi yang tegas. Pengguna perlu memahami pentingnya autentikasi dua faktor, kata sandi kompleks, pembatasan akses aplikasi pihak ketiga, serta pengaturan privasi yang ketat. Di sisi lain, platform digital harus menerapkan standar teknis keamanan yang memadai, meningkatkan transparansi, dan menyediakan edukasi keamanan yang lebih mudah dipahami. Pemerintah juga harus memastikan implementasi UU Perlindungan Data Pribadi berjalan efektif melalui penegakan hukum, audit berkala, dan penguatan regulasi teknis.

Secara keseluruhan, perlindungan data pribadi di media sosial hanya dapat tercapai apabila seluruh pemangku kepentingan pengguna, platform, pemerintah, dan

masyarakat berkolaborasi dalam membangun ekosistem digital yang aman, berkelanjutan, dan berorientasi pada budaya keamanan. Pendekatan terpadu inilah yang dapat menekan risiko serangan siber dan menjaga integritas identitas digital pengguna di era teknologi yang semakin berkembang.

Referensi

Al, J., Rifqy, M., Arham, H., & Risal, M. C. (2023). *Perlindungan Data Pribadi Bagi Pengguna Media Sosial*. *3*(2), 109–119.

Ansyafa, K. Z., Fajarudin, M., Fadhil, M., & Neyman, S. N. (2024). *Analisis Keamanan Media Sosial Terhadap Serangan Phising Online Menggunakan Metode Zphisher Dan Social Engineering Toolkit*. *4*, 1–10.

Ath-Thariq ; Jurnal Dakwah Dan Komunikasi, Vol. 06, No. 02, Juli-Desember 2022 220. (2022). *06*(02), 220–235.

Dewangan, O., Mishra, A., & Nainani, J. (2024). *Social Media And Privacy : Understanding The Risks To Personal Data*. *3*(1), 1–11.

Farooqi, S., Musa, M., Shafiq, Z., & Zaffar, F. (2020). *Canarytrap : Detecting Data Misuse By Third-Party Apps On Online Social Networks*. *2020*(4), 336–354. Https://Doi.Org/10.2478/Popets-2020-0076

Firdaus, A., & Wardhani, D. F. (2024). *Melindungi Privasi Di Era Digital : Keamanan Data Pribadi Di Indonesia Protecting Privacy In The Digital Era : Personal Data*. *13*(1), 1–16.

Fitriyani, R. (2025). *Analisis Keamanan Whatsapp Di Berbagai Platform : Studi Kasus Serangan Dan Perlindungan Data Pengguna*. *9*(2), 116–122.

Harakan, A., Said, T. G., & Gray, S. (2024). *Big Data And Security : A Review Of Social Media Risks And Insights For Indonesia*. *11*(1), 14–32.

Jering, P. (2025). *Keamanan Online Dalam Media Sosial : Pentingnya Perlindungan Data Pribadi Di Era Digital (Studi Kasus Desa Jurnal Pengabdian Nasional (Jpn) Indonesia*. *6*(1), 38–52.

Kurniasandi, D. D., Aprilia, S. N., Indradjaja, N., Hukum, F., Wijaya, U., Surabaya, P., Prigen, K., Prigen, K., Pasuruan, K., Timur, P. J., Hukum, F., Wijaya, U., Kampus, P., & Pendahuluan, A. (2022). *Regulasi Terkait Perlindungan Data Pribadi Dalam Penggunaan Jasa E-Commerce*. *21*(1), 103–114.

Lesmana, R., & Nasution, M. I. P. (2025). *Kebocoran Data Di Media Sosial : Analisis Pola Dan Strategi Pencegahannya*. *2*(May), 123–128.

Marpaung, D. M. (2025). *Strategi Pencegahan Cybercrime Pada Data Pribadi Di Media Sosial*. *1*.

Noviyanti, S., Putri, A., Afifah, N., Khaerunisa, A., & Pratama, R. A. (2025). *Pengaruh Literasi Digital Terhadap Perilaku Mahasiswa Dalam Melindungi Data Pribadi Dari Ancaman Siber*. *3*(1), 1–8.

Pengguna, D. K., Tazkiyah, P. A., Hayat, M. M., & Rahma, S. (2025). *Privasi Data Mahasiswa Di Instagram : Analisis Literatur Terhadap*. *3*(1).

Pudjiarti, E., Faizah, S., & Hardani, S. (2023). *Analisa Kesadaran Masyarakat Terhadap Bahaya Cybercrime Pada Penggunaan Teknologi Dan Media Sosial*. *10*(1), 24–37.

Richardo, K. (2025). *Analisis Sentimen Media Sosial Twitter Terhadap Destinasi Wisata Krui Menggunakan Algoritma Support Vector Machine Dan Smote Sistem Informasi ,*

Fakultas Teknik Dan Ilmu Komputer , Universitas Teknokrat Indonesia , Indonesia Sentiment Analysis Of Twitter Users Toward Tourist Destinations In Krui Using The Svm Algorithm. *5*(7), 1993–2003.

Ritonga, A., Putra, B., Togatorop, D., Ginting, H. B., Manila, K., Tri, M., Sinaga, Y., & Amelia, R. I. (2025). *Analisis Kombinatorik Dalam Menentukan Keamanan Dan Kompleksitas Password Dengan Penerapan Teori Kombinatorik*. *2*.

Saputra, F., Informasi, S. S., Pembangunan, U., & Veteran, N. (2023). *Literasi Digital Untuk Perlindungan Data Pribadi 1*. *17*, 1–8.

Sari, S. N., & Fitri, A. O. (2025). *Inflasi : Jurnal Ekonomi , Manajemen Dan Perbankan Analisis Persepsi Masyarakat Terhadap Keamanan Dan Risiko Cyber Crime Dalam Perbankan Digital Inflasi : Jurnal Ekonomi , Manajemen Dan Perbankan*. *2*, 77–83.

Sitorus, R., Felix, Z., & Banke, R. (2025). *Locus : Jurnal Konsep Ilmu Hukum*. *5*.

Souhoka, B. A., Fadillah, R. A., & Fathan, M. (2025). *Analisis Strategi Pencegahan Phising Studi Kasus Pada Media Sosial Facebook*. *3*(1), 10–22.

Sujiwana, R. K., Fahmi, A., Ridho, A., Aryanti, D. C., & Rakhmawati, N. A. (2024). *Analisis Bibliometrik Mengenai Serangan Phishing Dan Whatsapp Menggunakan Vosviewer*. *8*(1), 101–105.