

Kebocoran Data di Media Sosial: Analisis Pola dan Strategi Pencegahannya

Rendy Lesmana¹, Muhammad Irwan Padli Nasution²

^{1,2}Universitas Islam Negeri Sumatera Utara

ARTICLE INFO

Article history:

Received April 25, 2025

Revised April 30, 2025

Accepted May 06, 2025

Available online May 10, 2025

Keywords:

Kebocoran data, media sosial, privasi digital, keamanan informasi, literasi digital, strategi pencegahan

Kata Kunci:

Data breach, social media, digital privacy, information security, digital literacy, prevention strategies.



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.
Copyright © 2025 by Author. Published by Yayasan Daarul Huda

ABSTRAK

Media sosial telah berkembang menjadi ruang utama interaksi digital yang digunakan oleh miliaran orang di seluruh dunia. Di balik manfaatnya dalam mempercepat komunikasi dan penyebaran informasi, terdapat ancaman serius terhadap keamanan data pribadi pengguna. Kebocoran data di media sosial telah menjadi fenomena yang semakin sering terjadi dan membawa dampak negatif, seperti pencurian identitas, penipuan daring, dan pelanggaran privasi. Penelitian ini bertujuan untuk menganalisis pola-pola umum kebocoran data yang muncul di berbagai platform media sosial serta menyusun strategi pencegahan yang dapat diterapkan untuk meminimalkan risiko tersebut. Melalui pendekatan kualitatif dengan studi literatur dan analisis kasus, ditemukan bahwa kebocoran data sering kali disebabkan oleh kombinasi antara lemahnya sistem keamanan platform, rendahnya kesadaran pengguna terhadap pentingnya privasi, serta praktik pengumpulan dan pemrosesan data oleh pihak ketiga tanpa transparansi. Penelitian ini menyarankan beberapa strategi mitigasi, di antaranya peningkatan literasi digital bagi pengguna, perbaikan kebijakan privasi yang lebih akuntabel,

penerapan teknologi keamanan canggih seperti enkripsi dan otentikasi ganda, serta penguatan regulasi perlindungan data oleh otoritas yang berwenang. Dengan demikian, hasil kajian ini diharapkan dapat memberikan kontribusi nyata dalam menciptakan ekosistem digital yang lebih aman, transparan, dan bertanggung jawab bagi seluruh pemangku kepentingan, termasuk pengguna, pengembang platform, dan pemerintah.

ABSTRACT

Social media has become the main space for digital interaction used by billions of people around the world. Behind its benefits in accelerating communication and dissemination of information, there are serious threats to the security of users' personal data. Data leaks on social media have become an increasingly frequent phenomenon and have negative impacts, such as identity theft, online fraud, and privacy violations. This study aims to analyze common patterns of data leaks that appear on various social media platforms and to develop preventive strategies that can be applied to minimize these risks. Through a qualitative approach with literature studies and case analysis, it was found that data leaks are often caused by a combination of weak platform security systems, low user awareness of the importance of privacy, and data collection and processing practices by third parties without transparency. This study suggests several mitigation strategies, including increasing digital literacy for users, improving more accountable privacy policies, implementing advanced security technologies such as encryption and double authentication, and strengthening data protection regulations by authorized authorities. Thus, the results of this study are expected to provide a real contribution in creating a safer, more transparent, and more responsible digital ecosystem for all stakeholders, including users, platform developers, and the government.

PENDAHULUAN

Dalam beberapa tahun terakhir, penggunaan media sosial telah mengalami peningkatan yang sangat signifikan. Menurut laporan Digital 2024 Global Overview Report oleh We Are Social dan Meltwater, lebih dari 5 miliar orang di dunia menggunakan internet, dan sekitar 62% di antaranya aktif menggunakan media sosial. Di Indonesia sendiri, pengguna media sosial mencapai lebih dari 170 juta orang pada awal tahun 2024, yang setara dengan lebih dari 60% populasi nasional. Pertumbuhan pesat ini menunjukkan bahwa media sosial telah menjadi bagian integral dari kehidupan sehari-hari, tidak hanya untuk

*Corresponding author

E-mail addresses: Rendylesmana1295@gmail.com, irwannst@uinsu.ac.id

komunikasi pribadi, tetapi juga sebagai sarana bisnis, pendidikan, dan bahkan pelayanan publik. Namun, tingginya aktivitas digital ini sebanding dengan meningkatnya ancaman terhadap data pribadi pengguna.

Seiring dengan meningkatnya ketergantungan masyarakat pada platform digital, isu keamanan siber—terutama kebocoran data—menjadi semakin kompleks. Media sosial, dengan karakteristiknya yang terbuka dan cepat dalam penyebaran informasi, sangat rentan terhadap eksploitasi data oleh pihak yang tidak bertanggung jawab. Banyak kasus kebocoran data yang melibatkan platform besar seperti Facebook, Instagram, dan Twitter, di mana informasi pribadi pengguna seperti nama, lokasi, alamat email, bahkan data biometrik dapat diakses secara ilegal oleh pihak ketiga. Kejadian-kejadian ini bukan hanya melanggar hak privasi, tetapi juga berisiko menimbulkan kerugian sosial dan ekonomi yang besar bagi individu maupun institusi.

Kebocoran data pada media sosial tidak terjadi begitu saja, melainkan melalui pola-pola tertentu yang dapat dianalisis. Pola tersebut antara lain mencakup celah keamanan dalam sistem, manipulasi pengguna melalui rekayasa sosial (*social engineering*), serta kebijakan privasi yang tidak transparan. Dalam banyak kasus, pengguna tidak sepenuhnya menyadari informasi apa saja yang mereka bagikan, bagaimana informasi tersebut digunakan, dan oleh siapa. Hal ini menjadikan mereka sebagai target empuk bagi pelaku kejahatan siber. Oleh karena itu, penting untuk memetakan pola-pola ini guna memahami akar permasalahannya secara lebih komprehensif.

Selain itu, fenomena data harvesting atau pengumpulan data masif oleh pihak ketiga tanpa persetujuan yang jelas dari pengguna turut menjadi faktor penyumbang terjadinya kebocoran data. Praktik ini sering kali dilakukan oleh pengiklan, pengembang aplikasi pihak ketiga, atau bahkan platform media sosial itu sendiri untuk kepentingan komersial. Data yang dikumpulkan tersebut bisa dijual kepada broker data atau digunakan untuk menyusun profil pengguna guna menyasar mereka secara psikologis, politik, maupun ekonomi. Praktik-praktik semacam ini menciptakan ekosistem digital yang eksploitatif dan jauh dari prinsip perlindungan privasi.

Literasi digital yang rendah juga menjadi penyebab utama kerentanan terhadap kebocoran data. Banyak pengguna media sosial yang belum memahami pentingnya pengaturan privasi, penggunaan kata sandi yang kuat, atau dampak dari membagikan informasi pribadi secara terbuka. Hal ini diperparah dengan kurangnya edukasi yang sistematis dari pihak berwenang dan penyedia platform digital. Ketidaktahuan ini membuat pengguna sulit mengenali risiko dan menghindari praktik-praktik digital yang berbahaya. Maka dari itu, peningkatan literasi digital menjadi salah satu strategi pencegahan yang krusial.

Di sisi lain, peran pemerintah dalam melindungi data masyarakat di ruang digital masih menghadapi banyak tantangan. Meskipun beberapa negara, termasuk Indonesia, telah memiliki regulasi perlindungan data seperti UU Perlindungan Data Pribadi (UU PDP), penerapannya masih terbatas dan belum sepenuhnya mampu mengimbangi kecepatan perkembangan teknologi. Diperlukan sinergi antara kebijakan publik, penguatan institusi pengawasan, serta komitmen penyedia platform untuk menjamin keamanan dan transparansi dalam pengelolaan data pengguna.

Melihat besarnya risiko yang ditimbulkan oleh kebocoran data di media sosial, maka penelitian ini menjadi sangat penting untuk dilakukan. Analisis terhadap pola-pola kebocoran data dan perumusan strategi pencegahannya tidak hanya berguna secara akademik, tetapi juga memberikan kontribusi praktis dalam pengambilan kebijakan dan edukasi masyarakat. Dengan memahami sumber permasalahan dan cara-cara penanggulangannya, kita dapat menciptakan lingkungan digital yang lebih aman, beretika, dan berkelanjutan. Urgensi penelitian ini terletak pada kebutuhan mendesak untuk melindungi hak-hak privasi warga negara di tengah derasnya arus transformasi digital.

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan kualitatif dengan desain penelitian deskriptif, yang bertujuan untuk menganalisis dan menggali pola kebocoran data yang terjadi pada media sosial serta merumuskan langkah-langkah pencegahan yang dapat diterapkan. Pendekatan ini dipilih karena cocok untuk mengeksplorasi fenomena sosial yang kompleks, di mana faktor teknis, perilaku pengguna, dan kebijakan platform saling berinteraksi dan mempengaruhi kejadian kebocoran data.

Sumber data dalam penelitian ini adalah data sekunder yang diambil dari berbagai sumber literatur, laporan riset, artikel berita, serta dokumentasi yang relevan. Peneliti mempelajari beberapa kajian terdahulu, kebijakan perlindungan data pribadi, serta studi kasus terkait kebocoran data yang terjadi pada platform media sosial utama. Kasus-kasus kebocoran yang terjadi pada platform besar seperti Facebook, Twitter, dan Instagram menjadi bahan utama untuk menganalisis pola kejadian serta dampak yang ditimbulkannya.

Pengumpulan data dilakukan dengan menggunakan teknik studi pustaka, yang mencakup seleksi dan identifikasi sumber-sumber yang memiliki relevansi dengan topik penelitian. Data dikumpulkan dari artikel-artikel, laporan yang diterbitkan oleh pemerintah, dan penelitian akademis yang memberikan

informasi terkini serta valid mengenai kebocoran data di media sosial. Pemilihan sumber didasarkan pada kredibilitas dan kaitannya dengan topik yang sedang diteliti.

Dalam analisis data, peneliti menerapkan teknik analisis isi (content analysis) untuk mengidentifikasi tema, pola, serta hubungan yang muncul dari berbagai sumber yang telah dikumpulkan. Teknik ini memungkinkan peneliti untuk mengklasifikasikan berbagai penyebab kebocoran data, tren kebocoran yang terjadi, serta strategi pencegahan yang dapat diterapkan untuk mengurangi risiko kebocoran data.

Agar temuan penelitian memiliki keakuratan yang tinggi, peneliti menggunakan triangulasi data, yang melibatkan perbandingan dan pengecekan silang antara berbagai sumber untuk memastikan konsistensi temuan yang diperoleh. Triangulasi ini dilakukan untuk memperkuat kredibilitas hasil penelitian dan memastikan bahwa analisis yang dilakukan berbasis pada data yang sah dan dapat dipertanggungjawabkan.

Dengan pendekatan ini, penelitian bertujuan untuk memberikan pemahaman yang lebih komprehensif mengenai pola kebocoran data di media sosial dan mengidentifikasi langkah-langkah preventif yang dapat diambil guna memitigasi risiko kebocoran data di masa depan.

HASIL DAN PEMBAHASAN

Kebocoran Data di Media Sosial

Kebocoran data pribadi di media sosial merupakan tantangan serius dalam era digital yang serba terhubung. Berdasarkan temuan dari studi pustaka, insiden kebocoran data biasanya melibatkan penyalahgunaan informasi oleh pihak ketiga, kelalaian platform dalam menjaga keamanan, serta kurangnya kesadaran pengguna dalam mengelola privasi akun mereka. Contohnya, dalam kasus kebocoran data Facebook tahun 2019, lebih dari 530 juta data pengguna tersebar di internet, termasuk nomor telepon dan identitas pengguna. Ini menunjukkan bahwa infrastruktur digital yang ada belum sepenuhnya mampu memberikan perlindungan optimal bagi penggunanya.

Fenomena ini diperparah oleh tingginya intensitas pengguna dalam membagikan informasi pribadi di media sosial, seperti tanggal lahir, lokasi, hingga data biometrik seperti foto wajah. Informasi ini, apabila jatuh ke tangan yang salah, dapat disalahgunakan untuk kejahatan digital seperti penipuan identitas, pencurian akun, dan eksploitasi ekonomi. Celah keamanan pun tidak hanya berasal dari sisi pengguna, tetapi juga dari arsitektur sistem digital yang rentan.

Selain itu, aplikasi pihak ketiga yang terintegrasi dengan media sosial juga menjadi salah satu pintu masuk kebocoran data. Aplikasi ini sering meminta akses terhadap informasi pribadi pengguna, dan dalam banyak kasus, pengguna menyetujuinya tanpa memahami risiko yang melekat. Kondisi ini diperburuk oleh kurangnya transparansi platform mengenai bagaimana data digunakan dan siapa saja yang memiliki akses terhadap informasi tersebut.

Tingkat literasi digital masyarakat yang masih rendah juga menjadi faktor penting yang memperbesar risiko kebocoran data. Banyak pengguna yang belum memahami pentingnya menjaga privasi digital, menggunakan kata sandi lemah, serta tidak mengaktifkan fitur keamanan tambahan seperti autentikasi dua faktor. Hal ini memperlihatkan bahwa aspek teknis dan perilaku pengguna sama-sama memainkan peran besar dalam menyebabkan kerentanan data.

Secara keseluruhan, kebocoran data di media sosial tidak dapat dipandang sebagai masalah teknis semata, tetapi juga berkaitan erat dengan pola konsumsi informasi, budaya berbagi berlebihan (oversharing), dan lemahnya kesadaran kritis pengguna dalam menjaga data pribadinya.

Pola Kebocoran Data di Media Sosial

Dari hasil analisis yang dilakukan, ditemukan sejumlah pola utama yang menjadi penyebab terjadinya kebocoran data di media sosial. Salah satu pola yang paling sering muncul adalah adanya celah atau kerentanan dalam sistem keamanan yang dimiliki oleh platform media sosial itu sendiri. Celah ini dapat berupa penggunaan protokol keamanan yang usang, sistem enkripsi yang tidak memadai, hingga lemahnya pengawasan terhadap aktivitas mencurigakan di jaringan mereka. Dalam banyak kasus, peretas mampu menembus sistem dan mendapatkan akses terhadap data pengguna melalui kelemahan-kelemahan teknis ini.

Selain itu, praktik penggunaan kata sandi yang tidak kuat oleh pengguna turut menjadi faktor penyumbang signifikan terhadap kerentanan data. Banyak pengguna masih menggunakan kombinasi sandi yang mudah ditebak, seperti tanggal lahir atau urutan angka sederhana, yang dengan mudah dapat dibobol oleh pihak yang tidak bertanggung jawab menggunakan teknik brute force atau kamus sandi. Tidak hanya itu, pengguna yang sama seringkali memakai sandi yang sama di berbagai platform, sehingga apabila satu akun berhasil diretas, maka akun lainnya pun ikut terancam.

Pola berikutnya yang cukup mengkhawatirkan adalah maraknya penggunaan teknik rekayasa sosial atau social engineering dalam upaya pencurian data. Teknik ini memanfaatkan manipulasi psikologis, seperti menyamar sebagai pihak terpercaya untuk mengelabui korban agar secara sukarela memberikan informasi sensitif. Salah satu bentuk paling umum dari pola ini adalah phishing, di mana pengguna diarahkan ke situs palsu yang menyerupai halaman login asli, dan kemudian informasi yang dimasukkan seperti email dan kata sandi dikumpulkan oleh pelaku.

Faktor lainnya yang tidak kalah penting adalah rendahnya tingkat pemahaman pengguna terhadap fitur-fitur pengaturan privasi di platform media sosial. Banyak pengguna tidak menyadari bahwa pengaturan default akun mereka memungkinkan informasi pribadi mereka terlihat oleh publik. Ketika pengguna mengunggah data pribadi seperti lokasi, nomor telepon, atau informasi keluarga tanpa mengatur tingkat kerahasiaannya, maka data tersebut dapat dengan mudah diakses dan dimanfaatkan oleh pihak yang tidak berwenang.

Kurangnya edukasi digital turut memperparah keadaan ini. Sebagian besar pengguna masih belum memahami risiko dari membagikan data pribadi secara terbuka di internet. Mereka menganggap media sosial sebagai ruang aman untuk berbagi, padahal setiap informasi yang diunggah bisa saja disimpan, dicatat, atau bahkan diperjualbelikan oleh pihak-pihak tertentu. Ketidaktahuan ini membuka peluang besar bagi pelaku kejahatan siber untuk mengeksploitasi data demi keuntungan pribadi, seperti penipuan, pencurian identitas, atau pemerasan.

Lebih jauh lagi, terdapat pola sistemik di mana platform media sosial sendiri tidak selalu memberikan transparansi atau kemudahan dalam mengatur privasi pengguna. Beberapa pengaturan tersembunyi di balik menu yang rumit, atau tidak dijelaskan secara jelas dalam bahasa yang mudah dipahami. Akibatnya, meskipun fitur pengamanan tersedia, banyak pengguna yang tidak pernah menggunakannya secara optimal.

Dengan demikian, pola-pola kebocoran data di media sosial bukan hanya disebabkan oleh serangan eksternal, tetapi juga berkaitan erat dengan perilaku pengguna yang belum sadar risiko, serta kebijakan platform yang belum sepenuhnya melindungi hak privasi pengguna. Kombinasi dari kelemahan sistem, praktik pengguna, dan minimnya edukasi menciptakan ekosistem digital yang sangat rentan terhadap insiden kebocoran data.

Pola dan Strategi Pencegahannya

Dari berbagai sumber yang dianalisis, pola-pola kebocoran data di media sosial dapat dikategorikan ke dalam tiga kelompok utama: celah sistem, manipulasi sosial, dan perilaku pengguna. Pertama, celah sistem terjadi karena kurangnya sistem enkripsi, penggunaan protokol keamanan lama, dan lemahnya kontrol akses internal. Kedua, manipulasi sosial mencakup teknik rekayasa seperti phishing dan baiting, di mana pengguna diarahkan untuk memberikan informasi pribadi secara sukarela. Ketiga, perilaku pengguna yang cenderung abai terhadap pengaturan privasi dan tidak menyadari risiko digital menjadi pemicu utama kebocoran data.

Sebagai respons terhadap persoalan ini, sejumlah strategi pencegahan telah dikembangkan oleh berbagai pihak. Di tingkat individu, penting untuk mendorong literasi keamanan digital, termasuk kesadaran dalam menggunakan kata sandi yang kompleks, memahami cara kerja pelacakan data, serta bijak dalam membagikan informasi pribadi di ruang publik digital. Edukasi ini dapat dilakukan melalui program sosialisasi oleh pemerintah maupun inisiatif komunitas digital.

Dari sisi penyedia platform, mereka perlu memperkuat sistem keamanan dengan menerapkan teknologi enkripsi mutakhir, audit keamanan berkala, serta memberikan kontrol yang lebih luas kepada pengguna terhadap data mereka. Salah satu contohnya adalah penyediaan dashboard privasi yang transparan dan mudah diakses, agar pengguna bisa memantau dan mengatur informasi apa saja yang dibagikan serta kepada siapa informasi tersebut tersedia.

Sementara itu, di tingkat kebijakan, pemerintah memiliki peran strategis dalam melindungi data warganya. Penerapan regulasi perlindungan data pribadi yang tegas dan komprehensif sangat diperlukan. Regulasi semacam ini tidak hanya berfungsi sebagai alat hukum, tetapi juga sebagai pengarah etika bagi platform digital agar bertanggung jawab dalam pengelolaan data. Di beberapa negara, seperti Uni Eropa, penerapan General Data Protection Regulation (GDPR) telah menjadi contoh sukses yang bisa diadopsi dan disesuaikan oleh negara lain, termasuk Indonesia.

Lebih jauh, strategi pencegahan harus bersifat holistik dan melibatkan semua pemangku kepentingan. Tanpa keterlibatan pengguna yang bijak, platform yang transparan, dan pemerintah yang responsif, maka risiko kebocoran data akan tetap tinggi. Oleh karena itu, sinergi tiga elemen utama ini—masyarakat, perusahaan teknologi, dan otoritas negara—menjadi kunci dalam membangun ekosistem digital yang aman dan bertanggung jawab.

SIMPULAN

Berdasarkan hasil analisis, dapat disimpulkan bahwa kebocoran data di media sosial merupakan fenomena kompleks yang dipengaruhi oleh berbagai faktor, baik dari sisi teknis maupun non-teknis. Pola kebocoran umumnya disebabkan oleh kelemahan dalam sistem keamanan platform, seperti kurangnya enkripsi dan sistem autentikasi yang memadai, serta meningkatnya praktik manipulasi psikologis seperti phishing yang memanfaatkan kelengahan pengguna. Di sisi lain, perilaku pengguna yang kurang memahami pentingnya pengaturan privasi turut memperbesar potensi risiko kebocoran data, terutama ketika informasi pribadi dibagikan secara terbuka tanpa pertimbangan keamanan.

Untuk menjawab tantangan tersebut, strategi pencegahan yang efektif harus bersifat multidimensional, melibatkan peran aktif dari pengguna, penyedia platform, dan pemerintah. Penguatan literasi digital masyarakat menjadi langkah awal yang penting untuk meningkatkan kesadaran terhadap risiko kebocoran data. Di samping itu, pengembangan teknologi keamanan yang lebih canggih serta penerapan regulasi perlindungan data pribadi yang ketat sangat diperlukan untuk memastikan keamanan dan privasi pengguna tetap terlindungi. Dengan sinergi antar pihak, ekosistem media sosial yang aman dan bertanggung jawab dapat diwujudkan.

REFERENSI

- Rahmawati, D., Aksana, A. D. M., dan Mukaromah, S. (2023). Privasi Dan Keamanan Data Di Media Sosial: Dampak Negatif Dan Strategi Pencegahan. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, 3(1), 571-580.
- Nugroho, P. N. F., Listanto, F. M., Amelia, N., dan Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen, dan Keuangan*. 1(2).
- Huda, N. U., Astaruddin, T. H., dkk. (2024). *Data Pribadi, Hak Warga, dan Negara Hukum: Menjaga Privasi Di Tengah Ancaman Digital*. Bandung: Widina Media Utama.
- Raharjo, S., dan Utami, E. (2022). *Keamanan Basis Data Relasional*. Yogyakarta: Andi (Anggota IKAPI).
- Prastyanti, A. R. (2025). *Monograf Perlindungan Data Pribadi Konsumen Pengguna Transaksi Elektronik*. Surakarta: Penerbit NEM.
- Ardhana, P. Y. V., Sari, N. M. dkk. (2025). *Strategi dan Teknologi Media Sosial*. Jawa Barat: CV. Mega Press Nusantara.
- Nugroho, T. M., Istiqomah, L. dkk. (2025). *Generasi Digital Jiwa Berkarakter: Pendidikan Masa Kini "Membentuk Generasi Cerdas Teknologi Dengan Nilai-Nilai Kemanusiaan"*. Yogyakarta: Karya Bakti Makmur (KBM) Indonesia.
- Wibowo., B. dan Hidayat, T. (2025). *OSINT FOR DUMMIES: Jurus Ninja Digital Dalam Mengungkap Rahasia Internet*. Yogyakarta: KBM Indonesia.
- Santoso., Apriyanto, H., Susilo, A. dkk. (2025). *Buku Ajar Pengantar Sistem Informasi*. Jambi: PT.Sonpedia Publishing Indonesia.
- Ambulani, N. (2025). *Manajemen Krisis dan Reputasi*. Jambi: PT. Sonpedia Publishing Indonesia.
- Sudibyo, A. (2023). *Media Massa Nasional Menghadapi Disrupsi Digital*. Jakarta: Kepustakaan Populer Gramedia (KPG).
- Kusnanto., Gudiato, C., Usman., dkk. (2024). *Transformasi Era Digitalisasi Masyarakat Kontemporer*. Jawa Timur: Uwais Inspirasi Indonesia.
- Hatta, R. H., Chafid, N., Rusminingsih, K. N., dkk. (2023). *Analisa Perancangan Sistem Informasi*. Batam: Yayasan Cendikia Mulia Mandiri.
- Arridla, I. H., Ajadtulloh., dan Hartati, S. (2025). *Keamanan Informasi dan Data*. Pekalongan: PT. Nasya Expanding Management (NEM).
- Mose, A. (2024). *Strategi Bisnis: Formulasi Strategi Pemasaran dan Sumber Daya Organisasi Untuk Pertumbuhan Bisnis*. Kota Padang: Penerbit Takaza Innovatix Labs.
- Hastuti, D., Dewintara, P., Syaharuddin, Z. A., dkk. (2024). *Buku Ajar Pengantar Teknologi Informasi*. Jambi: PT. Sonpedia Publishing Indonesia.
- Dewatmoko, S., Mulyani, S. Y., dan Wibisono, T. (2025). *Digital Consumer Behavior: Strategi Pemasaran Berbasis Data dan Artificial Intelligence*. Kota Padang: Penerbit Takaza Innovatix Labs.
- Nasution, P. I. M. (2008). Urgensi Keamanan Pada Sistem Informasi. *Jurnal Iqro'*. 2(2) 41-53.
- Tambunan, A. F. S. dan Nasution, P. I. M. (2023). Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Di E-Commerce. *JEMB*. 2(1). 5-7.
- Ujung, M. A. dan Nasution, P. I. M. (2023). Pentingnya Sistem Keamanan Database untuk Melindungi Data Pribadi. *JISKA*. 1(2). 44-47.
- Zahwani, T. S. dan Nasution, P. I. M. (2023). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital. *JoSES*. 2(2). 105-109.

- Pohan, D. T. dan Nasution, P. I. M. (2023). Perlindungan Hukum Data Pribadi Konsumen Dalam Platfrom E-Commerce. SAMMAJIVA. 1(3). 42-48.
- Lubis, N. S. dan Nasution, P. I. M. (2023). Analisis Penyalahgunaan Data Pribadi Dalam Menggunakan Media Sosial. JoSES. 2(2). 75-78.