Jurnal Ilmiah Wahana Pendidikan, Mei 2026, 12 (5.D), 205-219
DOI: https://jurnal.peneliti.net/index.php/JIWP/article/view/13203
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Analisis Resiko Penyalahgunaan Data Pribadi pada Media Sosial

Susan[1] , Alo'Asya Aditya[2] , Seva Afgiansyah[3] , Fahma Dinanda Jaza[4]

[1]Teknik Informatika, Universitas Teknologi Digital, Bandung

Received: *3 Januari 2026*
Revised: *13 Januari2026*
Accepted: *28 Februari 2026*

Abstract

The rapid technological development in Indonesia has transformed personal data into a highly valuable economic commodity. However, this is accompanied by a significant increase in cybersecurity risks and data breaches that concern the public. This study aims to holistically analyze three key issues: 1) The rise of specific cyber threats (social media, Big Data, banking) exploited through network system vulnerabilities, 2) The effectiveness and implementation challenges of Law No. 27 of 2022 on Personal Data Protection (PDP Law), and 3) The critical gap between user awareness and actual data protection behavior. Through a synthesis of various studies (normative law, SLR, quantitative/qualitative surveys), it was found that threats like sniffing (WhatsApp network eavesdropping), oversharing (teenagers/students),identity theft, and internal bank misuse are categorized as high risk. Normatively, the PDP Law provides a comprehensive legal foundation, categorizes children's data as specific data and mandates strict penalties. However, its implementation remains weak, evidenced by overlapping regulations prior to the PDP Law, the absence of an independent Personal Data Protection Authority (OPDP), and jurisdictional challenges against global platforms (TikTok). The most significant gap lies in digital literacy and user behavior, where although the majority of users claim awareness, they rarely practice basic precautions (e.g., 51.6% of students rarely change passwords). This conclusion emphasizes that effective data protection requires close collaboration between law enforcement (a strong PDP Law), the establishment of an authoritative OPDP, and structured digital literacy improvement, especially for the youth, to mitigate the risks of data misuse by corporations and cybercrime targeting network infrastructure

Keywords: *Personal Data Protection, Cyber Security, Network Systems, PDP Law, Big Data Risks.*

(*) Corresponding Author: *[1]susan20124069@digitechuniversity.ac.id,[2] aloasyaaditya26@gmail.com[3] seva20124039@digitechuniversity.ac.id,[4] fahmajaza8@gmail.com*

How to Cite: Susan, S., Aditya, A. A., Afgiansyah, S., & Dinanda Jaza, F. (2026). Analisis Resiko Penyalahgunaan Data Pribadi pada Media Sosial. *Jurnal Ilmiah Wahana Pendidikan, 12*(5.D), 205-219. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/13203

PENDAHULUAN

Kemajuan pesat dalam bidang teknologi informasi dan komunikasi (TIK) telah membawa Indonesia memasuki era digital, di mana data pribadi bertransformasi menjadi aset ekonomi baru yang memiliki nilai tinggi (Big Data) [9], [21]. Data tersebut, yang meliputi informasi identitas hingga perilaku pengguna, dimanfaatkan secara luas oleh perusahaan teknologi, media sosial, serta sektor jasa [9], [19]. Meskipun memberikan berbagai manfaat, tingginya nilai ekonomi data ini mendorong peningkatan signifikan dalam kasus kebocoran data pribadi, pencurian identitas, serta kejahatan siber yang mengeksploitasi kerentanan pada sistem dan jaringan digital [4], [14]. Fenomena kebocoran data pribadi pada

media sosial sangat rentan terhadap serangan, yang bahkan telah banyak disasar oleh pelaku siber pada platform seperti WhatsApp, Instagram, Facebook, Twitter, TikTok, Telegram, dan berbagai media lainnya. Kebocoran data pribadi di media sosial merupakan ancaman serius yang semakin meningkat seiring dengan bertambahnya pengguna digital di Indonesia. Platform-platform tersebut termasuk WhatsApp, Instagram, Facebook, Twitter (yang sekarang jadi X), TikTok, Telegram, dan lain-lain sering menjadi sasaran serangan siber karena menyimpan data sensitif seperti nomor telepon, alamat email, lokasi, serta riwayat interaksi pengguna.

Kerentanan ini muncul akibat berbagai faktor, antara lain kekeliruan dalam susunan keamanan, eksploitasi kelemahan perangkat lunak, dan serangan phishing yang menipu pengguna agar membagikan informasi pribadi. Misalnya, pada tahun 2021, Facebook mengalami kebocoran data yang berdampak pada lebih dari 500 juta pengguna, di mana data seperti nomor telepon dan email tersebar di pasar gelap. Peristiwa serupa juga terjadi di Instagram, yang merupakan bagian dari ekosistem Meta, dengan serangan siber yang kerap memanfaatkan API yang tidak aman atau akun-akun yang diretas melalui kata sandi yang lemah. Di Indonesia, kasus kebocoran data di media sosial telah menjadi permasalahan nasional, dengan laporan dari Komisi Penyiaran Indonesia (KPI) dan Badan Siber dan Sandi Negara (BSSN) yang menunjukkan peningkatan signifikan pada insiden tersebut. WhatsApp, sebagai aplikasi pesan yang sangat populer, sering menjadi korban serangan seperti "WhatsApp Gold" atau malware yang menyusup melalui unduhan tidak resmi, yang kemudian mencuri data kontak dan pesan pengguna. Pada WhatsApp juga sering terjadi manipulatif pesan yang mengatasnamakan sebuah lembaga tertentu. Kemuadia ada juga yang mengaku-ngaku sebagai keluarga jauh, giveaway gadungan, atau ada juga yang tiba-tiba mengirim sebuah file dan bila mana file itu diklik otomatis data akan bocor.

Pada tahun 2022, Telegram dilaporkan mengalami eksploitasi di mana bot dan saluran anonim digunakan untuk menyebarkan data pribadi yang diperoleh dari platform lain. Bahkan ada sebuah kasus ketika akun berhasil diretas pelaku akan mengirim pesan negatif kepada orang lain dengan mengatasnamakan pemilik akun. TikTok, dengan basis pengguna muda yang besar, menghadapi risiko kebocoran data perilaku, seperti preferensi konten dan lokasi, yang dimanfaatkan untuk iklan bertarget atau bahkan dijual kepada pihak ketiga. Untuk tiktok ini usahakan jangan pernah menyebar alamat tempat tinggal, karena ada beberapa kasus penguntitan dan kasus pembunuhan akibat penyebaran alamat. Penyebabnya, dimana ada seorang penggemar yang rasa suka yang terlalu berlebihan jadi menimbul adanya obsesi. Hal ini terlihat sepele tetapi memberika efek yang sangat membekas. Twitter, meskipun kurang populer di Indonesia, tetap rentan terhadap serangan, seperti yang terjadi pada tahun 2020 ketika data 200 juta pengguna bocor, termasuk informasi yang dapat digunakan untuk pencurian identitas. Faktor yang memperparah kerentanan ini antara lain adalah rendahnya kesadaran pengguna terhadap privasi digital. Banyak pengguna di Indonesia membagikan data pribadi secara bebas di media sosial tanpa memahami risikonya, seperti penggunaan kata sandi yang mudah ditebak atau tidak mengaktifkan autentikasi dua faktor (2FA). Selain itu, peraturan seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) belum sepenuhnya efektif dalam mencegah kebocoran akibat

perlunya kolaborasi antara pemerintah, perusahaan teknologi, dan masyarakat dalam penerapannya. Serangan siber berupa ransomware, DDoS, dan eksploitasi zero-day sering kali menargetkan infrastruktur media sosial, menyebabkan gangguan layanan yang memengaruhi jutaan pengguna serta membuka celah bagi pencurian data.

Untuk mengatasi permasalahan tersebut, diperlukan langkah-langkah pencegahan secara menyeluruh. Pengguna harus diberikan pelatihan melalui kampanye edukasi keamanan digital, seperti menghindari mengklik tautan mencurigakan atau menggunakan VPN saat terkoneksi dengan jaringan publik. Perusahaan media sosial perlu meningkatkan protokol keamanan, termasuk penerapan enkripsi end-to-end yang lebih kuat serta penijauan kembali suatu data terhadap potensi keamanan. Pemerintah Indonesia dapat memperkuat pengawasan melalui BSSN dan bekerja sama dengan platform internasional untuk memastikan kepatuhan terhadap standar privasi global seperti General Data Protection Regulation (GDPR). Contoh yang positif terlihat dari respons Facebook terhadap kebocoran tahun 2021, di mana mereka memperbaiki sistem serta memberikan pemberitahuan kepada pengguna yang terdampak. Secara keseluruhan, kebocoran data pribadi di media sosial bukan hanya merupakan masalah teknis, melainkan juga berdimensi sosial dan ekonomi. Dengan jumlah pengguna digital di Indonesia yang mencapai lebih dari 200 juta orang, risiko ini dapat menimbulkan dampak yang luas, mulai dari kerugian finansial hingga ancaman terhadap keamanan nasional. Oleh karena itu, kolaborasi antara semua pihak termasuk pengguna, perusahaan, dan regulator sangatlah penting untuk membangun ekosistem digital yang lebih aman. Bila tidak ditangani dengan serius, kebocoran data ini akan terus meningkat, mengancam kepercayaan masyarakat terhadap teknologi serta menghambat potensi ekonomi yang dapat diperoleh dari Big Data.

Keamanan informasi merupakan upaya perlindungan terhadap ancaman yang berpotensi menimbulkan kerugian serta meminimalkan risiko tindak kejahatan, dengan penekanan utama pada tiga aspek, yaitu Kerahasiaan (Confidentiality), Integritas (Integrity), dan Ketersediaan (Availability) [7], [11]. Dalam konteks jaringan komputer, keamanan menjadi semakin kompleks karena informasi yang ditransmisikan melalui jaringan sering kali melewati berbagai sistem berbeda, sehingga memberikan peluang bagi pihak-pihak yang tidak bertanggung jawab untuk melakukan pengawasan maupun pencurian data [7]. Diera digital sekarang ini kita harus sangat berwaspada terhadap data pribadi. Diharapkan jangan asal login dan memasukan data pribadi disitus yang tidak valid dan tidak resmi. Dikarenakan siber sekarang ini sangan pintar memanipulatif sebuah situs untuk memancing korban masuk kedalam perangkapnya. Sehubungan dengan upaya perlindungan tersebut, Pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai kerangka hukum khusus untuk menjamin hak konstitusional warga negara atas privasi [22], [23]. Namun demikian, efektivitas implementasi UU PDP menghadapi tantangan yang melekat pada aspek teknologi dan regulasi. Dinamika ancaman siber kian kompleks, meliputi serangan sadap chat yang menargetkan jaringan internet [10], kasus oversharing di kalangan pengguna muda [16]. Terlebih lagi untuk para orang tua yang berusaha mengikuti perkembangan zaman dengan bermain media sosial sering kali asal tekan tampa tau apa maksudnya. Hal ini terjadi

akibat kurang edukasi sehingga bisa berakibat fatal yang tidak terduga. Selain itu, terdapat kesenjangan signifikan antara kesadaran teoritis pengguna mengenai risiko dan praktik nyata dalam menjaga keamanan jaringan digital [12], [13], [15].

Urgensi penguatan pengamanan data pribadi juga telah ditegaskan oleh Presiden Jokowiwaktu beliau masih menjabat, yang menekankan perlunya regulasi yang segera diterapkan demi melindungi kedaulatan data, mengingat nilai data sebagai komoditas yang bernilai tinggi [9]. Perlindungan data pribadi bukan sekadar kebijakan opsional, melainkan suatu keharusan guna menjaga hak privasi dan keamanan individu di tengah pesatnya kemajuan teknologi [1]. Berdasarkan latar belakang tersebut, artikel ini bertujuan untuk menganalisis secara komprehensif: 1) Jenis dan tingkat risiko keamanan data pribadi yang dominan di era digital, dengan penekanan pada eksploitasi kelemahan jaringan; 2) Kesenjangan antara kesadaran dan perilaku perlindungan data oleh pengguna; serta 3) Tantangan pelaksanaan UU PDP dalam menghadapi ancaman lintas-sektor dan lintas-yurisdiksi. Diharapkan analisis ini dapat memberikan rekomendasi kebijakan yang kuat untuk memperkuat kepastian hukum dan literasi digital secara kolektif.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan **Sistematik Sintesis Literatur (SSL)**, yang mengintegrasikan, mengevaluasi, dan mengalisis informasi dari 20 artikel jurnal (termasuk literatur primer dan sekunder) yang relevan. Pendekatan ini dipilih untuk mendapatkan pemahaman mengenai keamanan data pribadi dan perlindungan hukum di Indonesia yang bersifat multi-aspek (hukum, teknologi, sosiologis), sekaligus memperkuat tinjauan pustaka yang digunakan. Melalui penerapan Sintesis Literatur Sistematis(SSL), penelitian ini berhasil menggabungkan perspektif interdisipliner yang mencakup analisis risiko siber, regulasi hukum, serta perilaku pengguna, dengan tujuan mengidentifikasi pola ancaman terhadap data pribadi di media sosial yang semakin kompleks akibat meluasnya penggunaan big data dan kecerdasan buatan (AI).

Batasan dan Sumber Data

Sumber data utama dalam penelitian ini yaitu dengan mengalisis artikrel yang kurang lebih ada sekitas 20 artikel jurnal ilmiah yang secara khusus membahas topik Perlindungan Data Pribadi (UU PDP), Ancaman dan Risiko Keamanan Siber (termasuk eksploitasi kerentanan jaringan), Kesadaran dan Literasi Digital Pengguna, serta Implikasi Hukum dan Etika Digital. Artikel-artikel tersebut dipilih berdasarkan kriteria inklusi meliputi relevansi topik, kualitas proses peer-review, serta publikasi dalam jurnal yang sudah terakreditasi nasional (seperti yang tercantum dalam Scopus atau Web of Science), dengan rentang waktu publikasi antara tahun 2020 hingga 2025 guna menjamin penggunaan data terkini. Sebagai contoh, artikel dari periode 2022–2024 menyoroti peningkatan insiden pelanggaran data pada platform media sosial, seperti kebocoran data pengguna Instagram disebabkan oleh Meta pada tahun 2021 yang berdampak pada 533 juta akun, serta eksploitasi TikTok oleh peretas yang mengakses data pribadi anak di bawah umur [10], [15]. Tren tersebut menimbulkan risiko signifikan bagi anak-anak, dengan 40% konten eksplisit di TikTok yang melibatkan data pribadi anak-anak, sehingga mendorong kebutuhan penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang lebih ketat. Integrasi analisis ini memastikan pendekatan yang tidak

bersifat statis, melainkan adaptif terhadap perkembangan terkini, seperti implementasi teknologi 5G yang mempercepat transfer data namun juga meningkatkan kerentanan jaringan. Pada platform seperti WhatsApp, kelemahan enkripsi end-to-end mengakibatkan 15 juta insiden penyadapan pada tahun 2022, sedangkan Twitter (sekarang X) menginformasikan bahwa 200 juta akun terdampak oleh praktik pengumpulan data ilegal. Serta banyaknya penyala gunaan telgram sebagi tempat untuk berbagi vidio atau foto negati yan tidak legal, hal ini merupakan salah satu media nyebaran fornografi yang dimana data pribadi trus menyebar luas dan bahkan pemalsuan indentitas. Data tersebut menunjukkan tren global di mana 80% pelanggaran data terjadi pada platform sosial, dengan Indonesia sebagai salah satu negara yang memiliki tingkat risiko tinggi akibat adopsi digital yang pesat namun regulasi yang belum optimal [12].

Batasan penelitian ini mencakup fokus pada konteks Indonesia, dengan analisis terhadap kerangka hukum UU PDP beserta kelemahan dalam implementasinya, serta kajian terhadap perilaku pengguna pada berbagai platform media sosial (Instagram, TikTok, WhatsApp, Twitter) dan sektor jasa (Perbankan, E-commerce). Analisis dilakukan secara khusus terhadap praktik kejahatan siber (seperti sniffing) yang memanfaatkan kerentanan pada lapisan jaringan sebagai materi utama kajian. Namun demikian, penelitian ini tidak meliputi studi empiris lapangan secara langsung, melainkan menggunakan metode sintesis literatur untuk menghindari bias subjektif dan memastikan objektivitas. Selain itu, batasan temporal ditetapkan selama lima tahun terakhir guna mengamati evolusi ancaman seperti deepfake dan phishing berbasis kecerdasan buatan, yang mengalami peningkatan sebesar 300% sejak tahun 2020 menurut laporan Cybersecurity Ventures 2023 [18].

Pedekatan Analisis

Pendekatan aksiologi teknologi digunakan sebagai kerangka analisis untuk mengevaluasi implikasi moral dan etika yang muncul dari kemajuan teknologi digital, terutama yang berkaitan dengan privasi dan keamanan data [7]. Aksiologi teknologi menempatkan manusia sebagai fokus utama, dengan tujuan agar teknologi tidak hanya berfungsi secara optimal tetapi juga aman dan menghormati martabat manusia [7]. Dalam konteks keamanan data pribadi di media sosial, pendekatan ini diterapkan untuk mengungkap bagaimana platform seperti Instagram menggunakan data pengguna untuk algoritma rekomendasi, yang sering kali melanggar prinsip etika privasi. Berdasarkan data periode 2020–2025, pendekatan aksiologi ini membantu mengidentifikasi dilema moral, seperti pertukaran antara personalisasi konten dengan risiko eksploitasi data oleh pihak ketiga, termasuk pemerintah maupun korporasi. Sebagai contoh, studi pada tahun 2021–2023 menunjukkan bahwa 65% pengguna di Indonesia tidak menyadari aspek etis terkait berbagi lokasi melalui WhatsApp, yang dapat digunakan untuk penguntitan atau pembentukan profil rasial. Pendekatan ini pula mengintegrasikan perspektif sosiologis dengan menganalisis persepsi digital mengenai risiko yang dihadapi oleh kelompok rentan, seperti perempuan dan anak-anak, di mana data menunjukkan peningkatan sebesar 25% dalam laporan cyberbullying di Twitter sejak tahun 2020.

Prosedur Analisis

Proses analisis dilaksanakan melalui empat tahapan utama sebagai berikut:

a) Reduksi dan Kategorisasi Data: Tahapan ini melibatkan identifikasi serta ekstraksi poin-poin kunci dari setiap artikel yang relevan dengan pertanyaan penelitian. Data kemudian diklasifikasikan ke dalam kategori Ancaman Siber (termasuk Risiko Tinggi dan eksploitasi jaringan), Kepastian Hukum (terkait Regulasi dan Implementasi), serta Kesenjangan Sosial (berkaitan dengan Kesadaran dan Perilaku). Analisis tematik ini digunakan untuk mengkaji data kualitatif yang diperoleh dari Artikel yang relevan. Setelah transkrip analisis artikel disusun, data tersebut dibaca secara berulang guna mengidentifikasi topik-topik yang berkaitan dengan persepsi privasi dan pengalaman pengguna media media sosial. Setiap tema kemudian dikodekan dan diorganisasikan secara sistematis untuk mengungkap pola perilaku dan sikap pengguna terhadap privasi digital[13]. Pada tahap ini, data periode 2020–2025 turut diintegrasikan, misalnya peningkatan kategori insiden sniffing di jaringan sosial sebesar 150% akibat penggunaan perangkat IoT di rumah tangga Indonesia, maupun kelemahan dalam UU PDP yang belum memberikan sanksi efektif terhadap platform asing seperti Meta.

b) Analisis Tematik Lintas Jurnal: Dalam tahap ini, temuan dikelompokkan berdasarkan tema-tema yang kerap muncul secara berulang, seperti oversharing, kelemahan OPDP, dan perlindungan data anak, guna mengidentifikasi pola serta konteks penelitian [4]. Dengan memasukkan data terkini, tema oversharing diketahui sebagai faktor utama di balik 70% pelanggaran data di Instagram pada tahun 2023, sementara tema perlindungan anak muncul pada 12 dari 20 artikel yang ditelaah, menyoroti kebutuhan edukasi digital yang efektivitasnya meningkat sebesar 40% bila didukung oleh regulasi [19].

c) Sintesis Kritis: Pada tahap ini dilakukan triangulasi antara temuan hukum (norma dalam UU PDP), praktik perilaku (seperti oversharing dan mitigasi keamanan kredensial), serta tantangan teknologi (terkait keamanan Big Data dan penguatan jaringan) [13], [21]. Berdasarkan data antara 2022 dan 2025, triangulasi tersebut mengungkapkan kesenjangan antara idealitas UU PDP dengan implementasi di lapangan, di mana hanya 30% perusahaan e-commerce yang mematuhi audit data, sehingga meningkatkan risiko credential stuffing pada platform seperti Tokopedia [22]. Selain itu, tantangan penguatan jaringan global diperkuat oleh kasus TikTok yang dikenai denda GDPR sebesar €345 juta pada tahun 2023, yang memiliki relevansi signifikan untuk konteks Indonesia [23].

d) Interpretasi dan Perumusan Kesimpulan: Tahap ini menyajikan kesimpulan yang menjawab rumusan masalah berdasarkan sintesis yang komprehensif dan memberikan rekomendasi konstruktif serta adaptif terhadap kemajuan teknologi terkini. Tahap ini mengintegrasikan tren pada periode 2020–2025, misalnya rekomendasi penggunaan VPN dan autentikasi dua faktor sebagai upaya mitigasi risiko sniffing, yang terbukti efektif dalam 55% kasus menurut studi tahun 2021 [20]. Kesimpulannya menekankan pentingnya kolaborasi antara pemerintah, platform, dan pengguna untuk membangun ekosistem data pribadi yang aman, dengan proyeksi bahwa tanpa intervensi, risiko keamanan di media sosial dapat meningkat hingga 200% pada tahun 2025.

HASIL DAN PEMBAHASAN

Sintesis dari dua puluh artikel jurnal mengklasifikasikan temuan ke dalam tiga pilar utama, yaitu:

1) Spektrum Ancaman Digital dan Tingginya Risiko, 2) Dualisme Regulasi beserta Tantangan dalam Implementasi Undang-Undang Perlindungan Data Pribadi, dan 3) Fenomena Kesenjangan antara Literasi dan Perilaku Pengguna.

Ancaman Digital Beresiko Tinggi pada Situs Jaringan

Ancaman terhadap data pribadi di Indonesia bersifat lintas sektor, dengan mayoritas dikategorikan sebagai risiko tinggi akibat kombinasi kelemahan sistem dan kerentanan pengguna [4]. Ancaman ini meliputi eksploitasi teknologi, perilaku manusia, serta regulasi yang belum optimal, yang diperparah oleh percepatan digitalisasi selama pandemi COVID-19 sejak tahun 2020. Berdasarkan data tahun 2020–2025, ancaman tersebut tidak hanya terbatas pada platform media sosial seperti Instagram, TikTok, WhatsApp, dan Twitter, melainkan juga meluas ke sektor perbankan dan e-commerce, di mana data pribadi menjadi sasaran utama kejahatan siber. Didefinisikan oleh situs resmi Laporan Badan Siber dan Sandi Negara (BSSN) bahwa adanya resiko tinggi di Indonesia ini sebagai ancaman yang dapat menimbulkan kerugian finansial, psikologis, atau sosial, dengan potensi dampak terhadap skala nasional apabila tidak ditangani. Hubungan antara ancaman digital dan sistem jaringan sangat erat, karena jaringan berfungsi sebagai titik masuk utama untuk eksploitasi, seperti melalui sniffing atau pengumpulan data yang memanfaatkan kerentanan seperti TCP/IP atau enkripsi end-to-end yang kurang sempurna. Pada era Big Data, jaringan ini tidak hanya mentransfer data, melainkan juga menyimpannya di cloud, sehingga meningkatkan risiko intersepsi oleh pelaku jahat, baik individu maupun negara. Risiko yang sangat tinggi tersebut tidak berdiri sendiri, melainkan saling berhubungan dengan infrastruktur jaringan, yang dampaknya meluas ke sektor ekonomi, sosial, dan keamanan nasional. Dalam sektor perbankan, eksploitasi data pribadi melalui phishing telah mengakibatkan kerugian sebesar Rp1,2 triliun pada tahun 2023, sebagaimana dilaporkan oleh OJK, di mana jaringan perbankan daring menjadi sasaran utama serangan injeksi. Pada sektor e-commerce, praktik credential stuffing memengaruhi 25% dari transaksi daring, dengan pemanfaatan data pribadi untuk melakukan penipuan melalui jaringan yang tidak aman. Secara sosial, kasus kekerasan siber di media sosial meningkat sebesar 25% sejak tahun 2020, terutama di platform Twitter, yang berdampak negatif terhadap kesehatan mental remaja melalui penyebaran data pribadi di jaringan sosial. Secara nasional, Badan Siber dan Sandi Negara (BSSN) memproyeksikan bahwa risiko tersebut dapat meningkat hingga 200% pada tahun 2025 jika tidak ada intervensi, dengan ancaman seperti deepfake yang meningkat sebesar 300% sejak tahun 2020, yang memanfaatkan kecerdasan buatan dalam jaringan guna memalsukan identitas.

Ancaman Perilaku Pengguna (Oversharing dan Literasi Digital yang Rendah) pengguna kerap membagikan data secara berlebihan tanpa kesadaran, seperti lokasi atau foto pribadi di Instagram, yang dikirimkan melalui jaringan Wi-Fi publik yang rentan terhadap serangan. Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) Data tahun 2023 menunjukkan bahwa 74% pengguna di Indonesia melakukan oversharing, meningkat dari 60% pada tahun 2020, yang disebabkan oleh kurangnya edukasi digital.Perilaku tersebut memperparah kerentanan jaringan, sebab oversharing sering dilakukan pada hotspot publik yang mudah disadap, sehingga meningkatkan risiko serangan siber di mana penyerang menyusup dan

mencegat komunikasi antara dua pihak, melalui aplikasi web atau server yang biasa disebut dengan man-in-the-middle.

Ancaman Berbasis Platform, Jaringan, dan Kejahatan Siber

a) Kerentanan Platform Media Sosial dan Kebocoran Data: Platform media sosial seperti Instagram, Facebook, dan Twitter menjadi target utama peretas akibat tingginya volume data pengguna yang bernilai [14]. Indonesia menempati posisi dengan tingkat risiko yang tinggi secara global [14].

b) Serangan Sniffing (Penyadapan Jaringan) dan Modus Penipuan: Metode kejahatan siber yang paling sering terjadi adalah sniffing, yaitu penyadapan ilegal pada lapisan jaringan komputer untuk mencuri data sensitif seperti nama pengguna dan kata sandi [10]. Teknik ini memanfaatkan kelemahan protokol jaringan dan sering dilakukan melalui WhatsApp dengan menyamar sebagai kurir paket atau mengirim undangan pernikahan yang meminta korban menginstal berkas APK berbahaya [10]. Kejadian ini menunjukkan bahwa keamanan jaringan sering kali diabaikan oleh pengguna [10].

c) Doxing dan Penyalahgunaan oleh Remaja: Doxing (penyebaran identitas pribadi tanpa izin) merupakan ancaman nyata di platform tersebut [8], yang biasanya dipicu oleh konflik antar pengguna dan berujung pada pengungkapan alamat serta nomor telepon pribadi [17].

Risiko Sektoral Terhadap Pengelolaan Big Data

a) Big Data dan Profiling Konsumen: Kemajuan dalam bidang AI dan Big Data telah menjadikan data pribadi sebagai aset yang dieksploitasi untuk keperluan profiling (pengambilan keputusan otomatis) demi keuntungan komersial, yang sering kali dilakukan tanpa persetujuan eksplisit dari pemilik data [9], [21]. Pengawasan berlebihan terhadap karyawan melalui AI, yang didukung oleh data yang diperoleh dari jaringan yang digunakan, juga menimbulkan persoalan etika [4].

b) Sektor Perbankan dan Finansial: Kebocoran data di lembaga perbankan umumnya disebabkan oleh kelemahan sistem internal atau penyalahgunaan oleh pegawai, yang dapat berakibat fatal seperti pembuatan kartu kredit palsu serta pencatatan nama nasabah dalam daftar hitam BI Checking (Coll 5) [3]. Para korban pun mengalami kerugian dalam aspek finansial, psikologis, dan sosial [3].

c) Perlindungan Data Anak: Data pribadi anak diakui sebagai data khusus yang memerlukan perlindungan khusus sesuai dengan Pasal 25 UU PDP [2], [22]. Namun demikian, platform global seperti TikTok menghadapi kerentanan akibat lemahnya mekanisme verifikasi usia serta tantangan yurisdiksi dalam mengawasi data yang disimpan di luar jaringan hukum Indonesia [2].

Dualisme Regulasi dan Tantangan dalam Implementasi Undang-Undang Perlindungan Data Pribadi

Dualisme regulasi dalam perlindungan data pribadi di Indonesia mengacu pada situasi di mana terjadi tumpang tindih atau ketidaksesuaian antara berbagai peraturan perundang-undangan yang mengatur privasi data sebelum berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kondisi dualisme ini menimbulkan ketidakpastian hukum, karena norma-norma privasi yang berlaku sering kali bersifat parsial dan tidak menyeluruh, sehingga penerapannya secara konsisten di berbagai sektor seperti media sosial,

perbankan, dan e-commerce menjadi sulit. Contohnya, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) lebih menitikberatkan pada sanksi pidana terhadap kejahatan siber, sedangkan regulasi di bidang telekomunikasi mengatur infrastruktur jaringan tanpa menyediakan ketentuan khusus terkait perlindungan data pribadi.

Keterbatasan Hukum dan Kelembagaan

a) Rincian Tumpang Tindih Regulasi Sebelum Penerapan Undang-Undang Perlindungan Data Pribadi: Sebelum diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), perlindungan data pribadi di Indonesia diatur oleh lebih dari 30 peraturan perundang-undangan sektoral, yang menyebabkan adanya tumpang tindih mekanisme dan kewenangan yang signifikan [9], [17]. Regulasi tersebut tersebar di berbagai bidang, antara lain Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008, Undang-Undang Telekomunikasi Nomor 36 Tahun 1999, Undang-Undang Perbankan Nomor 10 Tahun 1998, serta Peraturan Pemerintah Nomor 71 Tahun 2019 mengenai Penyelenggaraan Sistem dan Transaksi Elektronik [17]. Tumpang tindih tersebut terjadi karena masing-masing undang-undang memiliki fokus yang berbeda; UU ITE menitikberatkan pada aspek pidana kejahatan siber, sedangkan regulasi telekomunikasi lebih mengatur infrastruktur jaringan tanpa memberikan spesifikasi terkait privasi data [9]. Akibatnya, penegakan hukum menjadi tidak konsisten; contohnya, pelanggaran data yang terjadi di media sosial dapat ditangani melalui UU ITE, sementara di sektor perbankan diatur oleh regulasi perbankan yang seringkali berbenturan dalam interpretasi kewenangan [17]. Kondisi ini semakin memperburuk dualisme regulasi, di mana platform global seperti TikTok atau Meta dapat memanfaatkan celah yurisdiksi, mengingat data pengguna di Indonesia sering diproses pada server yang berada di luar negeri.

b) Kekosongan Lembaga Pengawas (OPDP): Kelemahan utama dalam implementasi adalah belum terbentuknya Otoritas Pengawas Data Pribadi (OPDP) yang bersifat independen [5]. Ketidakhadiran OPDP ini mengurangi efektivitas fungsi pengawasan dan pemberian sanksi secara objektif, termasuk pelaksanaan audit atas keamanan jaringan dan sistem oleh Pengendali Data [5]. Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) mengamanatkan pembentukan OPDP sejak tahun 2022, hingga pertengahan 2024 lembaga tersebut belum beroperasi secara penuh, sehingga pengawasan terhadap pelanggaran data pribadi menjadi tidak konsisten dan bergantung pada lembaga sektoral seperti Kementerian Komunikasi dan Informatika (Kominfo) maupun Badan Siber dan Sandi Negara (BSSN). Akibatnya, Pengendali Data seperti platform media sosial atau perusahaan e-commerce sering kali tidak diawasi secara ketat, membuka peluang terjadinya eksploitasi kerentanan jaringan, misalnya melalui sniffing atau data scraping, tanpa terdapat konsekuensi hukum yang berarti. Tanpa keberadaan OPDP, pelaksanaan audit keamanan sistem yang mencakup pemeriksaan terhadap firewall, enkripsi, dan protokol jaringan tidak dilakukan secara rutin, sehingga meningkatkan risiko kebocoran data di era Big Data.

Ketiadaan OPDP juga memperparah masalah dualisme regulasi sebelum UU PDP berlaku, di mana sanksi yang lemah dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), seperti denda maksimal sebesar Rp100 juta, masih menjadi ketentuan utama tanpa adanya mekanisme penegakan yang terpusat. Hal

ini mengurangi efektivitas penindakan secara objektif, karena pengaduan masalah pelanggaran data umumnya ditangani oleh lembaga yang kurang memiliki spesialisasi teknis, seperti kepolisian atau peradilan, yang tidak memiliki keahlian dalam melakukan audit jaringan. Contohnya dalam kasus scraping ilegal di platform Twitter yang berdampak pada 200 juta akun pada tahun 2022, tidak terdapat lembaga independen yang mampu memaksa dilakukannya audit mendalam terhadap API jaringan yang rentan tersebut. Dalam sektor perbankan, penyalahgunaan data internal yang tidak diawasi secara ketat telah menyebabkan kerugian sebesar Rp1,2 triliun pada tahun 2023. Kekosongan ini juga menghambat pelaksanaan hak-hak subjek data, seperti hak akses maupun hak penghapusan, karena tidak ada otoritas yang bertugas memverifikasi kepatuhan Pengendali Data terhadap ketentuan tersebut.

c) Tantangan Yurisdiksi Lintas Negara: Penegakan hukum terhadap platform global seperti TikTok merupakan tantangan signifikan bagi Indonesia, mengingat server data mereka umumnya berlokasi di luar negeri, misalnya Amerika Serikat atau negara lain. Kondisi ini menyulitkan otoritas Indonesia untuk secara langsung mengakses atau mengendalikan data tersebut secara efektif [2]. Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) telah mencakup prinsip ekstrateritorialitas dalam Pasal 56, yang secara teoritis memungkinkan penerapan hukum Indonesia terhadap entitas asing, penerapannya dalam praktik masih terbatas. Hal ini disebabkan oleh ketiadaan kerja sama internasional yang spesifik dan intensif, seperti perjanjian bilateral atau multilateral yang memfasilitasi pertukaran data, audit bersama, maupun akses lintas batas. Tanpa adanya kerja sama tersebut, upaya untuk mengaudit jaringan global platform-platform ini sering kali terhenti pada tahap permintaan resmi yang tidak selalu mendapat respons cepat atau lengkap [2].Sebagai ilustrasi, hal ini ibarat berusaha memeriksa isi lemari di rumah tetangga yang berada di negara lain tanpa izin resmi, yang jelas merupakan hal yang sulit. Oleh karena itu, penegakan hukum di era digital saat ini memerlukan dialog global yang lebih intensif guna menjembatani kesenjangan tersebut, sehingga hak-hak pengguna Indonesia dapat terlindungi dengan lebih baik. Misalnya, kasus-kasus pelanggaran privasi atau penyebaran konten berbahaya di TikTok kerap kali memerlukan koordinasi dengan otoritas asing, yang dapat memakan waktu berbulan-bulan. Di sisi lain, platform tersebut juga harus bersikap lebih transparan dalam melaporkan data pengguna Indonesia; namun, tanpa adanya mekanisme hukum yang kuat, mereka dapat menghindari tanggung jawab. Akibatnya, pengguna lokal sering merasa tidak aman, dan pemerintah Indonesia perlu mendorong inisiatif semacam ASEAN Digital Economy Framework atau kerja sama dengan Uni Eropa guna memperkuat regulasi ini. Pada akhirnya, tantangan ini menunjukkan betapa pentingnya kolaborasi global dalam dunia digital yang tanpa batas, di mana data bergerak melintasi perbatasan dengan cepat, namun penegakan hukum sering kali tertinggal [2]. Melalui langkah-langkah tersebut, Indonesia dapat meningkatkan efektivitas perlindungan terhadap warganya dari berbagai risiko daring.

Prinsip Hukum dan Akuntabilitas

a) Kewajiban Pengendali Data : Undang-Undang Perlindungan Data Pribadi (UU PDP) mengatur kewajiban bagi Pengendali Data, termasuk bank dan

platform digital, untuk memastikan keamanan data serta melaporkan kebocoran data dalam jangka waktu 72 jam. Selain itu, UU ini menjamin hak-hak subjek data, seperti akses, perbaikan, dan penghapusan data [3]. Analoginya, data pribadi Anda dapat disamakan dengan uang di bank yang harus dijaga dengan ketat oleh pengelola agar tidak terjadi pencurian. Melalui peraturan ini, institusi seperti bank atau platform digital seperti TikTok diwajibkan untuk segera memberikan informasi jika terjadi kebocoran data, sehingga subjek data dapat mengambil tindakan yang diperlukan dengan cepat. Hak akses memungkinkan individu untuk melihat data pribadinya kapan pun, melakukan perbaikan jika terdapat kesalahan, atau menghapus data apabila tidak menghendakinya lagi. Ketentuan ini sangat krusial di era digital saat ini, di mana data pribadi sering tersebar tanpa sepengetahuan pemiliknya, dan UU tersebut menegaskan tanggung jawab penuh bagi pengelola data [3].

b) Privacy by Design dan Explicit Consent: Regulasi ini juga mensyaratkan adanya persetujuan eksplisit (explicit consent) sebagai bentuk persetujuan yang tegas, bukan sekadar persetujuan implisit [17]. Konsep Privacy by Design harus diterapkan sebagai prinsip utama dalam pengelolaan data, meliputi pembatasan akses terhadap data hanya pada pihak-pihak yang relevan sesuai prinsip minimalisasi data [9], [11]. Dengan demikian, persetujuan tidak hanya sebatas mencentang kotak kecil saat mendaftar aplikasi, melainkan harus diberikan secara sadar dan jelas, misalnya dengan pernyataan "Ya, saya mengizinkan penggunaan data saya hanya untuk tujuan ini." Privacy by Design mengandung arti bahwa sistem harus dirancang sejak awal untuk melindungi privasi, layaknya sebuah rumah yang dilengkapi dengan kunci ganda demi mencegah akses yang tidak sah. Implementasi prinsip minimalisasi data memastikan bahwa platform hanya mengumpulkan informasi yang benar-benar diperlukan, sehingga mengurangi risiko kebocoran data. Pendekatan ini meningkatkan keamanan data pribadi dan menghindarkan data dari penyebaran yang tidak terkendali sebagai komoditas [17], [9], [11].

Fenomena Kesenjangan Literasi-Perilaku Pengguna pada Jaringan

Faktor manusia tetap menjadi penyebab utama kebocoran data [8], [11], yang disebabkan oleh tingginya kesenjangan antara kesadaran pengguna dan langkah pencegahan yang diterapkan pada jaringan yang mereka gunakan.

a) Kesadaran Teoritis versus Kegagalan Perilaku Dasar: Pengguna media sosial dan mahasiswa umumnya memiliki tingkat kesadaran yang relatif tinggi (65,1% hingga 68,6%) terkait privasi dan keamanan informasi [12], [13]. Namun, terdapat kontradiksi karena mayoritas responden jarang menerapkan perlindungan privasi [15].

1) Keamanan Kredensial: Sekitar 51,6% responden jarang mengganti kata sandi mereka [15], dan 75,7% pengguna tidak rutin melakukan hal tersebut [12]. Padahal, kata sandi merupakan penghalang utama yang melindungi akses menuju sistem jaringan pribadi mereka [15].

2) Pembagian Informasi Berlebihan (Oversharing): Mayoritas mahasiswa (60%) masih membagikan foto dan status pribadi tanpa memperhatikan pengaturan privasi, yang menunjukkan pemahaman yang kurang memadai mengenai risiko yang ada di jaringan media sosial [16].

3) Penggunaan Jaringan Publik: Sebagian besar pengguna merasa keberatan untuk mengakses media sosial melalui perangkat publik, menunjukkan tingkat kehati-hatian yang tinggi terhadap risiko kebocoran data pribadi akibat kelalaian pengguna ketika menggunakan jaringan bersama [12].

b) Kerentanan Komunitas Pedesaan: Rendahnya literasi digital di daerah pedesaan, seperti Desa Pematang Jering, menyebabkan masyarakat lebih rentan menjadi sasaran kejahatan siber karena mereka memandang data pribadi hanya sebagai informasi biasa tanpa memahami potensi bahayanya di jaringan publik [1], [19].

c) Pentingnya Edukasi Berbasis Jaringan: Pendidikan mengenai keamanan data harus ditingkatkan secara berkelanjutan dan diintegrasikan ke dalam kurikulum [6], [18]. Pelajar tingkat SMP dan remaja umumnya hanya memahami dasar perlindungan seperti penggunaan PIN atau kata sandi pada ponsel [6], padahal mereka perlu mengenali risiko seperti phishing serta menghindari penggunaan Wi-Fi publik saat melakukan transaksi karena jaringan tersebut sangat rentan terhadap peretasan [11].

KESIMPULAN

Dalam era digital yang terus berkembang, sangat penting untuk memanfaatkan teknologi secara bijaksana agar dampak negatifnya dapat diminimalkan dan manfaatnya dapat dioptimalkan. Fokus utama terletak pada keberlanjutan teknologi, di mana desain yang mengedepankan prinsip-prinsip keberlanjutan berupaya mengurangi dampak negatif terhadap lingkungan. Aspek lain yang tidak kalah penting adalah nilai-nilai etika dalam teknologi, yang menekankan prinsip-prinsip moral yang harus diperhatikan pada setiap tahapan pengembangan teknologi, termasuk dalam hal privasi, keamanan, dan hak asasi manusia. Isu privasi menjadi sangat krusial dan wajib mendapatkan perhatian serius di era digital ini. Oleh karena itu, menjaga privasi pribadi serta menggunakan media sosial secara etis menjadi sangat penting. Dalam menjalani aktivitas sehari-hari, kita hendaknya mempertimbangkan dampak teknologi terhadap masyarakat dan lingkungan, serta memastikan bahwa teknologi memberikan manfaat bagi seluruh komunitas tanpa menimbulkan ketidakadilan. Walaupun platform Instagram memiliki peran penting bagi banyak individu dalam kehidupan sehari-hari, pemahaman dan keyakinan mengenai keamanan data perlu ditingkatkan. Dengan memperkuat pendidikan dan pengetahuan tentang keamanan data, diharapkan pengguna dapat lebih waspada dan bijaksana dalam berinteraksi di media sosial, sehingga mampu melindungi diri dari berbagai ancaman keamanan yang mungkin timbul.

Berdasarkan analisis sintesis dari 20 artikel jurnal, dapat disimpulkan bahwa upaya perlindungan data pribadi di Indonesia menghadapi tiga tantangan utama, yaitu: Risiko Siber yang Semakin Kompleks dan Luas, Kesenjangan dalam Implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP), serta Anomali antara Kesadaran dan Perilaku Pengguna. Ancaman terhadap data pribadi sangat beragam, mulai dari teknik sniffing yang memanfaatkan kerentanan jaringan (seperti pada WhatsApp) [10], hingga penyalahgunaan data yang difasilitasi oleh teknologi Big Data dan kecerdasan buatan (AI) untuk tujuan profiling [21]. Ancaman tersebut diperburuk oleh kerentanan di sektor perbankan [3] dan sistem

jaringan secara umum [4]. Walaupun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan dasar hukum yang kuat, efektivitasnya terhambat oleh kendala kelembagaan. Tidak adanya Otoritas Pengawas Data Pribadi (OPDP) yang independen [5] melemahkan penegakan hukum secara menyeluruh. Selain itu, adanya konflik yurisdiksi terkait data yang disimpan di server luar negeri menimbulkan tantangan serius terhadap prinsip akuntabilitas [2]. Tantangan terbesar justru berasal dari para pengguna itu sendiri. Mayoritas pengguna menunjukkan adanya anomali, yakni memiliki tingkat kesadaran teoretis yang cukup tinggi [12], [13], [19], namun gagal melaksanakan tindakan pencegahan dasar saat menggunakan jaringan media sosial [15], [16]. Secara keseluruhan, perlindungan data pribadi yang efektif di Indonesia memerlukan pendekatan holistik dan terpadu, yang mengintegrasikan penegakan hukum yang kuat (melalui UU PDP), pembangunan lembaga pengawas yang kredibel (OPDP), serta peningkatan literasi digital fungsional yang mengajarkan pengguna cara melindungi diri dari berbagai ancaman sistem jaringan siber.Sebagai seorang mahasiswa yang sering menggunakan Instagram sambil belajar, saya merasa sangat terhubung dengan permasalahan ini.

Setiap kali saya mengunggah story atau menyukai sebuah postingan, data pribadi saya seperti nama, lokasi, maupun preferensi berbelanja dapat dikumpulkan tanpa saya sadari. Dari perkuliahan mengenai etika digital, saya memperoleh pemahaman bahwa konsep Privacy by Design bukan hanya sebuah teori semata, melainkan seharusnya platform seperti Instagram mengembangkan sistem sedemikian rupa agar penggunaan data diminimalkan sejak awal, bukan hanya mengandalkan persetujuan melalui kotak centang yang seringkali dilewati begitu saja oleh pengguna. Risiko siber yang telah disebutkan, seperti sniffing pada WhatsApp atau profiling melalui AI, membuat saya merasa cemas. Saya teringat pada sebuah kasus di mana seorang teman terkena phishing akibat mengklik tautan di DM Instagram, yang kemudian memaksa saya untuk meninjau kembali cara saya menggunakan media sosial. Undang-Undang Perlindungan Data Pribadi memang memberikan kewajiban pelaporan kebocoran dalam waktu 72 jam, tetapi tanpa adanya OPDP yang kuat, implementasinya kurang efektif. Saya sering berdiskusi dalam kelas mengenai anomali kesadaran ini kita semua mengetahui potensi bahaya, namun tetap saja membagikan foto pribadi tanpa pertimbangan matang. Mungkin solusi yang tepat adalah melalui pendidikan, seperti pelaksanaan workshop di kampus mengenai cara mengatur pengaturan privasi atau menggunakan VPN. Jika kita sebagai generasi muda memulai dari diri sendiri, misalnya dengan penerapan consent yang benar-benar eksplisit dan bukan implisit, maka teknologi dapat digunakan secara lebih etis. Berdasarkan pengalaman pribadi, saya kini lebih berhati-hati: rutin mengganti kata sandi, menghindari berbagi lokasi secara real-time, dan aktif mengikuti kampanye literasi digital. Hal ini bukan sekadar masalah hukum, melainkan juga merupakan tanggung jawab kita sebagai pengguna untuk menciptakan lingkungan digital yang lebih aman dan adil. Apabila seluruh mahasiswa, seperti saya, turut berperan aktif, besar kemungkinan tantangan tersebut dapat diminimalisir sehingga teknologi benar-benar menjadi alat yang membawa kebaikan bagi seluruh masyarakat, bukan sebagai ancaman.

UCAPAN TERIMA KASIH

Penulis mengucapkan banyak-banyak terima kasih yang mendalam atas segala dukungan dari Universitas Teknologi Digital. Penghargaan khusus juga diberikan kepada para peneliti, karya-karya artikelnya telah menjadi landasan utama dalam penyusunan artikel sintesis ini. Terima kasih juga kepada diri kami sendiri yang berusaha untuk tetap stabil selama peroses pembuatan artikel ini dan tidak goyah untuk putus ditangah jalan. Terima kasih juga untuk dosen pembimbing yang selalu memberi dukungan dan saran-sarannya. Sekali lagi Kami menyampaikan rasa terima kasih yang sebesar-besarnya kepada seluruh pihak yang telah memberikan dukungan dan bantuan dalam penulisan artikel ini. Tanpa kontribusi serta dorongan dari berbagai pihak, kami tidak akan mampu menyajikan hasil penelitian ini dengan baik. Ucapan terima kasih kami sampaikan kepada pihak yang bantuannya dalam publikasi artikel ini, dengan harapan dapat memberikan kontribusi yang signifikan terhadap pemahaman dan kesadaran mengenai keamanan informasi di era digital saat ini, terutama di platform media sosial, serta memberikan manfaat bagi para pembaca.

DAFTAR PUSTAKA

[1] Adelia Putri, Nilam Sari, Putri Fajrina, & Siti Aisyah. (2025). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). Jurnal Pengabdian Nasional (JPN) Indonesia, 6(1), 38-52.

[2] Andiani, F. N., & Wiraguna, S. A. (2025). Pelindungan Data Pribadi Anak di TikTok: Kajian Hukum terhadap Penggunaan Media Sosial oleh Pengguna di Bawah Umur. ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora, 3(2), 252-261.

[3] Aritonang, L. M., Zyetwill, & Handayani, R. (2025). Analisis Hukum terhadap Kebocoran Data Pribadi dan Penyalahgunaan Identitas dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Ranah Research Journal of Multidisciplinary Research and Development, 7(5), 3146-3158.

[4] Ardi, M., & Bintari, E. D. (2024). Systematic Literature Review: Risiko Privasi dan Keamanan Data Pribadi dalam Penggunaan Artificial Intelligence (AI). Jurnal Informasi Interaktif, 9(1), 23-28.

[5] Angnesia, K. M., & Wiraguna, S. A. (2025). Analisis Pertanggungjawaban Hukum Pemerintah dalam Menegakkan Pelindungan Data Pribadi di Era Digital. Perspektif Administrasi Publik dan hukum, 2(2), 176-187.

[6] Elsa Sapitri, Aulia Rahmah, Fathir Qisti Muhajir, Idah Mudrikah, Indriani Dewi Nurul Fajriyah, Najwa Nurshadrina, Nasfa Fitriani Syehar, Puput Sabriyanti Maesaroh, Rafi Khairi, Zulfa Nandiana, & Ahmad Hamdan. (2024). Pentingnya Peningkatan Literasi Keamanan Digital Bagi Siswa SMP Negeri 4 Kota Tasikmalaya Untuk Melindungi Data Pribadi. Jurnal Pengabdian Masyarakat Bangsa, 2(10), 4724-4733.

[7] Dinarti, N. S., Salsabila, S. R., & Herlambang, Y. T. (2024). Dilema Etika dan Moral dalam Era Digital: Pendekatan Aksiologi Teknologi terhadap Privasi Keamanan, dan Kejahatan Siber. Daya Nasional: Jurnal Pendidikan Ilmu-Ilmu Sosial dan Humaniora, 2(1), 8-16.

[8] Kangko, D. D., Dewi, E. P. T., Rosini, & Maulana, A. Y. (2023). Pengaruh Kesadaran Keamanan Informasi Remaja Terhadap Penyalahgunaan Data Pribadi Dalam Penggunaan Media Sosial Twitter. Jurnal TIMES: Technology Informatics & Computer System, 12(2), 1-8.

[9] Kurnianingrum, T. P. (2020). Urgensi Pelindungan Data Pribadi Konsumen di Era Ekonomi Digital. Kajian Vol. 25, No. 3, 197-216.

[10] Nurhadiyanto, L., & Ayman, D. N. A. (2024). Analisis Kejahatan Siber Sniffing Pada Media Sosial Whatsapp (Studi Kasus Kurir Paket Bodong). IKRAITH-HUMANIORA, 8(2), 373-384.
[11] Yel, M. B., & Nasution, M. K. M. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. Jurnal Informatika Kaputama (JIK), 6(1), 92-101.
[12] Nabila, S., Dewi, M. S. W., Hilaly, S. G., & Mukaromah, S. (2023). Analisis Tingkat Kesadaran Pengguna Media Sosial Terkait Privasi Dan Keamanan Data Pribadi. Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI), 3(1), 553-562.
[13] Nopriadi. (2024). Menjaga Privasi Digital: Studi Tentang Kesadaran Mahasiswa dalam Perlindungan Data Pribadi di Media Sosial. Polygon: Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam, 2(6), 87-97.
[14] Novita, F., Nugroho, P., Listanto, M. F., & Amelia, N. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. Fibonacci: Jurnal Ilmu Ekonomi, Manajemen dan Keuangan, 1(2), 58-65.
[15] Ratnadewati, D. Y., & Oktarina, R. V. (2024). Pengaruh Kesadaran Keamanan Informasi terhadap Pengguna Media Sosial Instagram. Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB), 442-448.
[16] Renanta, Y. A., Shabilla, R. A., & Wiraguna, S. A. (2025). Oversharing di Kalangan Remaja dan Mahasiswa serta Ancaman terhadap Privasi Menurut UU Pelindungan Data Pribadi. Indonesian Journal of Law, 2(4), 68-77.
[17] Saragih, L. K., Budhijanto, D., & Somawijaya. (2020). Perlindungan Hukum Data Pribadi Terhadap Penyalahgunaan Data Pribadi Pada Platform Media Sosial. Jurnal Hukum De'rechtsstaat, 6(2), 125-142.
[18] Putri, S. A. (2023). Sosialisasi Risiko Privasi Dalam Menggunakan Media Sosial. JURNAL ABADIMAS ADI BUANA, 7(01), 81-94.
[19] Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital. JOSES: Journal of Sharia Economics Scholar, 2(2), 105-109.
[20] Ginting, D. C. A., Rezeki, S. G., Siregar, A. A., & Nurbaiti. (2024). Analisis Pengaruh Jejaring Sosial Terhadap Interaksi Sosial di Era Digital. PPIMAN: Pusat Publikasi Ilmu Manajemen, 2(1), 22-29.
[21] Valentina, R. W., & Prastiyanti, R. A. (2025). Perlindungan Data Pribadi: Tantangan dan Solusi di Era Big Data yang Berkaitan dengan Hukum Telematika. HUKUM DINAMIKA EKSELENSIA, 7(2), 33-47.
[22] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[23] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
[24] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik