Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI) 2023
Surabaya, 6 – 7 September 2023

PRIVASI DAN KEAMANAN DATA DI MEDIA SOSIAL: DAMPAK NEGATIF DAN STRATEGI PENCEGAHAN

DATA PRIVACY AND SECURITY IN SOCIAL MEDIA: NEGATIVE IMPACT AND PREVENTION STRATEGIES

Dian Rahmawati[1*], Muhammad Darriel Aqmal Aksana[1], Siti Mukaromah[1]
*E-mail: diianrhma06@gmail.com

[1] Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

Privasi dan keamanan data menjadi isu krusial dalam penggunaan media sosial saat ini. Fokus dari penelitian ini adalah mengetahui dampak negatif yang dapat timbul serta strategi pencegahan yang dapat dilakukan. Penulis melakukan penelitian kasus-kasus pelanggaran privasi dan keamanan data yang terjadi di berbagai platform media sosial seperti Facebook, Twitter, dan Linkedin. Contohnya, kasus pencurian dan keamanan data yang terjadi selama periode 2005-2018 di Facebook, penyebaran konten pornografi di Twitter pada tahun 2020, kebocoran data pribadi pengguna di Linkedin pada tahun 2021, pelanggaran privasi dan keamanan data pengguna dibawah umur pada Instagram dan Tiktok di tahun 2022 dan 2023. Metode yang digunakan dalam penelitian ini adalah pendekatan kualitatif dengan menggunakan studi literatur dan analisis deskriptif untuk memperkuat temuan. Temuan penelitian menyoroti rendahnya kesadaran privasi oleh pengguna, di mana banyak individu yang menerima iklan atau berita yang berpotensi terhadap kebocoran data, kurangnya perhatian menyeluruh terkait privasi dan keamanan data. Selain itu, tidak mengubah password secara berkala, akun media sosial yang masih terbuka umum dan tidak menerapkan pengaturan privasi yang memadai. Dengan demikian, temuan ini menunjukkan bahwa kurangnya kesadaran pengguna terhadap privasi dan keamanan data di media sosial dapat memiliki dampak negatif. Untuk mengatasi isu ini, penulis memberikan beberapa strategi pencegahan untuk melindungi privasi dan keamanan data, seperti penggunaan password yang kuat, pembatasan informasi yang diberikan, membaca dengan cermat syarat dan ketentuan, meningkatkan kesadaran pengguna, memantau aktivitas dan riwayat akun, serta menggunakan aplikasi resmi dan terpercaya.

Kata Kunci: *privasi, keamanan, medsos, dampak, strategi.*

Abstract

Data privacy and security are crucial issues in the current use of social media. The focus of this study is to find out the negative impacts that can arise and prevention strategies that can be done. The author conducted research on cases of privacy and data security violations that occurred on various social media platforms such as Facebook, Twitter, and Linkedin. For example, data theft and security cases that occurred during the period 2005-2018 on Facebook, the spread of pornographic content on Twitter in 2020, the leak of users' personal data on Linkedin in 2021, breaches of privacy and security of underage user data on Instagram and Tiktok in 2022 and 2023. The method used in this study is a qualitative approach using literature studies and descriptive analysis to strengthen the findings. The research findings highlight the low privacy awareness by users, where many individuals receive advertisements or news that have the potential for data leaks, and a lack of overall attention related to data privacy and security. In addition, do not change passwords regularly, social media accounts that are still public and do not apply adequate privacy settings. Thus, these findings suggest that users' lack of awareness of

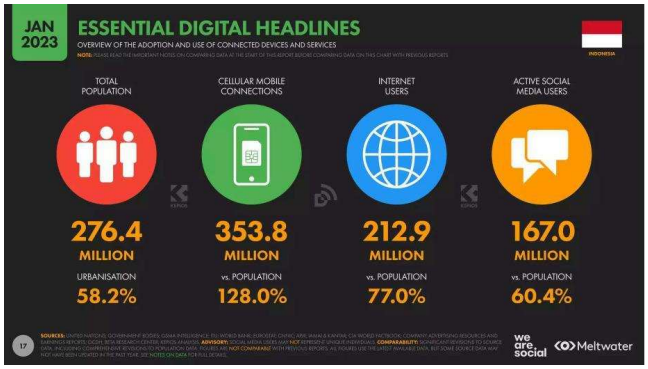
data privacy and security on social media can have a negative impact. To overcome this issue, the author provides several preventive strategies to protect data privacy and security, such as the use of strong passwords, restrictions on information provided, carefully reading terms and conditions, increasing user awareness, monitoring account activity and history, and using official and trusted applications.
Keywords: *privacy, security, socmed, impact, strategies.*

1. PENDAHULUAN

Di era *Internet of Things* saat ini, kemajuan pada teknologi dan informasi telah mengalami kenaikan yang signifikan dan sangat pesat. Diambil dari data yang dihasilkan oleh We Are Social pada awal januari 2022, disebutkan jika pengguna aktif dari berbagai sosial media di Indonesia telah meningkat sebanyak 12,35% atau sebanyak 191 juta orang dari 170 juta orang pada tahun 2020 [1] dan pada tahun 2023 terjadi penurunan pengguna sebanyak 12,57% atau sebanyak 167 juta orang[2]. Gambar 1 adalah data statistik pengguna aktif media sosial dari tahun 2015-2023.

Gambar 1. Pengguna aktif media sosial tahun 2015-2023
Sumber: DataIndonesia.id (2023)

Walaupun pengguna sosial media secara persentase menurun, pengguna internet di Indonesia tahun 2023 tercatat sebanyak 212,9 juta orang yang artinya sebanyak 77% warga Indonesia telah tersambung dengan internet [3] seperti yang ditunjukkan dalam gambar 2.



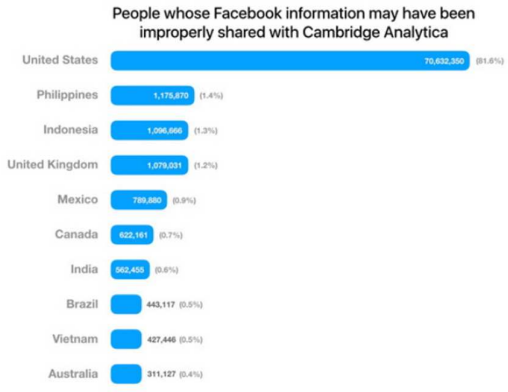
Gambar 2. Pengguna internet dan media sosial di Indonesia pada Januari 2023
Sumber: *We are social* (2023)

Media sosial merupakan hasil dari kemajuan teknologi dan informasi yang memungkinkan manusia untuk terhubung dan berkomunikasi secara bebas melalui berbagai platform yang memfasilitasi penyebaran informasi contohnya seperti Facebook, Twitter, Instagram, dan

lainnya[4]. Namun, Kemajuan dari teknologi dan informasi dalam media sosial tidak luput dari adanya pelanggaran privasi di masyarakat karena media sosial telah menjadi kegiatan keseharian masyarakat umum.

Penggunaan dari media sosial telah mengubah bagaimana manusia sebagai makhluk sosial berinteraksi, bersosialisasi, dan memberikan dampak positif yang menguntungkan juga dapat memberi dampak negatif yang menimbulkan kerugian bagi pengguna [5]. Agar bisa mengakses atau menggunakan fitur-fitur di media sosial, pengguna perlu mengikuti aturan yang telah ditentukan. Langkah pertama yang dilakukan adalah mengisi beberapa informasi pribadi yang diperlukan saat melakukan pendaftaran pada platform tersebut. Informasi pribadi tersebut meliputi nama, alamat email, nomor handphone, lokasi tempat tinggal, dan aspek personal lainnya seperti latar belakang pribadi dan detail kontak [6]. Setelah memberikan informasi yang dibutuhkan, akan ditampilkan syarat dan ketentuan yang mencakup keamanan dan privasi yang harus dipahami terlebih dahulu oleh pengguna dan diminta untuk mendapatkan persetujuan oleh platform tersebut apakah pengguna menyetujui syarat dan ketentuan yang diberikan. Syarat dan ketentuan akan terus berkembang setelah platform tersebut diluncurkan. Platform media sosial seperti Facebook dan whatsapp sekarang sudah menerapkan pengendalian privasi yang berpusat pada pengguna, yang memungkinkan untuk mengatur siapa saja yang dapat melihat dan mengakses informasi yang mereka berikan. Hal ini ternyata berpengaruh terhadap pengguna dalam memberikan lebih banyak data-data yang bersifat pribadi untuk dapat menggunakan fitur baru [7].

Tidak semua pengguna merespons dengan positif terhadap perkembangan ketentuan keamanan akses pengguna. Menurut penelitian yang telah dilakukan, pembaruan terhadap ketentuan dari privasi WhatsApp yang terjadi di tahun 2021 mendapat respons yang negatif dari pengguna. WhatsApp memberi izin kepada platform media sosial yaitu Facebook untuk mengelola informasi-informasi yang dikumpulkan, menggunakan data, dan mengumpulkan data-data pengguna yang berasal dari WhatsApp. Salah satu poin dalam pembaruan tersebut menyatakan bahwa data pengguna akan dikumpulkan lalu disimpan pada pusat data Facebook di seluruh dunia [8]. Hingga saat ini, telah terjadi banyak kasus dari informasi pribadi pengguna yang bocor di platform media sosial. Jutaan data pribadi dan identitas yang dapat ditemukan di media sosial. Dampak dari perkembangan ini adalah bahwa data-data tersebut menjadi lebih mudah diakses oleh siapa pun, sehingga pelanggaran terhadap privasi menjadi lebih mudah terjadi [9].



Gambar 3. Data pengguna Facebook yang bocor
Sumber: Facebook (2018)

Salah satu contoh kasus pelanggaran terhadap privasi terjadi pada tahun 2018, masyarakat umum dikagetkan dengan berita kebocoran data pengguna dengan jumlah kisaran 87 juta data-data yang bersifat pribadi oleh pengguna Facebook dimana data-data dari penggunanya diambil oleh Firma

Cambridge Analytica, dimana kisaran satu juta data tercuri yang asalnya dari warga negara Indonesia [10]. Hal ini tentunya menimbulkan kecemasan pengguna Facebook terhadap data-data pribadi yang telah bocor.

IUIPC (Internet User's Information Privacy Concern) mengacu kepada kekhawatiran yang dirasakan oleh pengguna-pengguna internet yang berkaitan dengan bagaimana suatu sebuah organisasi atau instansi mengelola ketentuan-ketentuan yang dimana ketentuan ini dapat mempengaruhi keamanan dari informasi data pribadi mereka [11]. Kekhawatiran ini juga muncul karena adanya tindakan seperti pencurian data pribadi, *cyber stalking*, *blackmail*, dan *spam* [12] yang melibatkan berbagi informasi pribadi. Pelanggaran keamanan data pribadi tidak hanya berpotensi menyebabkan kerugian finansial bagi pengguna, tetapi juga dapat merusak reputasi mereka di masyarakat. Berdasarkan dari latar belakang yang telah dijelaskan, tujuan dari penulisan penelitian ini adalah mencari apa saja dampak-dampak negatif dari penggunaan sosial media terhadap privasi dan keamanan terhadap pengguna, serta mengetahui strategi yang dapat dilakukan untuk menghindari pelanggaran privasi dan keamanan data.

2. METODOLOGI

Gambar 3. Alur Penelitian

Berdasarkan alur penelitian pada gambar 3, langkah-langkah yang dilakukan sebagai berikut:

a. Identifikasi Masalah
   Pada tahap ini penulis melakukan identifikasi masalah mengenai topik yang akan dibahas pada penelitian. Topik permasalahan yang dibahas yaitu terkait privasi dan keamanan data di media sosial dengan memfokuskan pada dampak negatif dan strategi pencegahannya.
b. Studi Literatur
   Studi literatur dilakukan dengan mengumpulkan dan menganalisis sumber yang relevan dalam bidang privasi dan keamanan data di media sosial. Sumber data yang menjadi acuan meliputi artikel jurnal, berita, situs web terpercaya, dan sumber lainnya yang relevan dengan topik pembahasan.
c. Pengumpulan Data
   Penulis mengumpulkan informasi yang relevan dari studi literatur yang telah dilakukan sebelumnya. Data tersebut akan digunakan untuk memperkuat argumen dan temuan dalam penelitian ini. Selanjutnya, data tersebut akan dianalisis untuk mendapatkan hasil yang dapat diinterpretasikan.
d. Analisis Deskriptif
   Analisis deskriptif dilakukan untuk mengorganisir dan merangkum data yang telah dikumpulkan dalam penelitian. Tujuannya adalah memberikan gambaran yang jelas dan terstruktur. Dalam penelitian ini penulis memvisualisasikan data dalam bentuk tabel agar mudah dipahami bagi pembaca.

e. Penarikan Kesimpulan dan Saran
   Pada tahap akhir, penulis menyusun kesimpulan berdasarkan hasil dari temuan yang telah diperoleh dalam penelitian ini. Selain itu, penulis juga memberikan saran mengenai

beberapa strategi yang dapat digunakan untuk melindungi privasi dan keamanan data dalam penggunaan media sosial.

3. HASIL DAN PEMBAHASAN

3.1 Dampak Negatif Penggunaan Media Sosial terhadap Privasi dan Keamanan Data

Pertumbuhan internet yang pesat memiliki dampak negatif terhadap privasi dan keamanan data di dunia maya. Masalah ini sering dihadapi oleh pengguna internet secara keseluruhan salah satunya media sosial. Kebocoran data pribadi atau informasi sensitif yang tidak disengaja dapat berdampak negatif seperti eksploitasi akun, spam, atau kerugian material. Banyak pengguna media sosial yang memiliki kesadaran dan serius menghadapi permasalahan terkait kebocoran data pribadi atau informasi sensitif secara online. Namun, hanya sekitar 30% dari total populasi orang dewasa di Amerika Serikat yang benar-benar mengambil tindakan nyata untuk melindungi privasi mereka, seperti melakukan perubahan pengaturan privasi di platform media sosial [13]. Dampak negatif penggunaan media sosial terhadap privasi dan keamanan data adalah pelanggaran yang terkait dengan pencurian data digital yaitu 1) ancaman, penghinaan, dan kekerasan seksual, 2) penyebaran data pribadi, foto dan data peminjaman, 3) penggunaan data KTP atau identitas orang lain untuk melakukan pinjaman online atau aktivitas yang dapat merugikan pemilik identitas tersebut [14]. Berikut adalah beberapa kasus pelanggaran terkait privasi dan keamanan data yang pernah terjadi di media sosial dapat dilihat pada tabel 1.

Tabel 1. Kasus Pelanggaran Privasi dan Keamanan Data

Sumber	Media Sosial	Tahun	Jenis Pelanggaran
[15]	Facebook	2005 - 2018	Pencurian dan keamanan data.
[16]	Twitter	2020	Penyebaran konten pornografi.
[17], [18]	Linkedin	2021	Pencurian identitas pengguna.
[19]	Instagram	2022	Privasi data pengguna dibawah umur
[20]	Tiktok	2023	Keamanan data pengguna dibawah umur

Pada tabel 1 dapat diketahui bahwa media sosial Facebook mengalami kasus pencurian dan keamanan data. Perlindungan privasi pengguna Facebook telah terkenal buruk dalam hal keamanan data dan informasi. Saat ini, terdapat berbagai cara yang dapat dilakukan dalam melemahkan sistem keamanan komputer dan jaringan pengguna yaitu dengan menyebarkan informasi palsu (*fake news*) atau menggunakan tautan menarik dan menjebak (*clickbait*) yang mengarahkan pengguna ke halaman situs yang mengandung virus tersembunyi. Hal ini berpotensi merusak keamanan sistem komputer dan bertujuan untuk mengakses data atau informasi pribadi pengguna Facebook [15].

Selama periode Januari hingga September 2020, Kementerian Komunikasi dan Informatika mencatat penanganan terhadap 1,3 juta konten negatif di media sosial. Dari jumlah tersebut,

sebanyak 1.062.558 konten merupakan konten pornografi. Platform media sosial yang paling banyak terkena pemblokiran karena konten pornografi adalah Twitter, diikuti oleh Facebook, Instagram, Youtube, Google, dan Telegram. Twitter juga sering kali menjadi sumber awal penyebaran konten pornografi sebelum menyebar ke media sosial lainnya [16].

Pada tahun 2021, terjadi kebocoran data pengguna LinkedIn yang berdampak pada privasi dan keamanan pengguna. Data seperti nomor telepon, alamat, dan informasi profil LinkedIn dicuri, yang dapat digunakan untuk kegiatan yang merugikan, termasuk pencurian identitas [17]. LinkedIn telah mengkonfirmasi pelanggaran keamanan data pengguna pada bulan April dan Juni. Dalam pelanggaran pertama, sekitar 500 juta data pengguna terdampak, sedangkan pelanggaran kedua melibatkan sekitar 700 juta data pengguna [18].

Kasus selanjutnya terjadi pada platform Instagram, dimana selama 2 tahun dilakukannya penyelidikan oleh Protection Commissioner (DPC) Irlandia ditemukan terdapat pelanggaran privasi data pengguna berumur 13 hingga 17 tahun dimana mereka dapat membuat akun bisnis sehingga data mengenai email dan nomor telepon bisa dilihat secara umum yang dinilai DPC melanggar keamanan data pengguna yang akhirnya Instagram di denda sebanyak Rp.6 miliar [19].

Hal serupa juga terjadi pada aplikasi bernama Tiktok yang dimana terjadi pelanggaran terhadap keamanan data yaitu Tiktok mengumpulkan data-data anak dibawah 13 tahun tanpa persetujuan orang tua dimana setelah dilakukan penyelidikan oleh pihak regulator keamanan data Inggris dari Mei 2018 - Juli 2020, Tiktok melanggar hukum Inggris yang berisikan tentang undang undang pemrosesan data pribadi anak sehingga tiktok di denda oleh inggris sebesar Rp.442,5 M pada tahun 2023 [20].

3.2 Penelitian Terkait Privasi dan Keamanan Data di Media Sosial

Privasi dapat didefinisikan sebagai hak seorang individu dalam menentukan seberapa jauh mereka ingin membuka jati dirinya kepada orang lain. Privasi juga dapat diartikan juga sebagai hak untuk tidak diganggu. Kehadiran privasi sangat penting bagi individu, lembaga, maupun dalam instansi. Ketika informasi yang bersifat privasi yang seharusnya tidak diketahui oleh publik telah tersebar dan diketahui oleh banyak orang, kejadian ini dapat berpotensi membahayakan posisi dan kredibilitas individu atau instansi yang terkait [21]. Privasi mempunyai tiga fungsi utama, yaitu sebagai mengontrol dan mengatur interaksi interpersonal, merencanakan dan strategi berhubungan dengan orang lain, menjaga dan memperjelas identitas diri [22]. Berikut adalah hasil penelitian dari beberapa jurnal terdahulu terkait privasi dan keamanan data di media sosial terlampir pada tabel 2.

Tabel 2. Hasil Penelitian Terdahulu

Sumber	Hasil Penelitian
[23]	Hasil penelitian dari 416 responden ditemukan bahwa sekitar 6,9% atau 29 orang masih memiliki kesadaran privasi yang kurang. Responden dalam kategori ini memiliki risiko tinggi terhadap pencurian data oleh peretas. Selain itu, sekitar 29,3% atau 122 orang sering menerima iklan atau berita di media sosial yang dapat mengindikasikan adanya kebocoran informasi pribadi mereka. Sekitar 45,4% atau 189 orang masih kurang memperhatikan privasi mereka. Artinya, mereka tidak terlalu peduli dengan perlindungan privasi mereka. Selanjutnya, sekitar 15,8% atau 66 orang memiliki kesadaran privasi di atas rata-rata, namun cenderung tidak memperhatikan izin dari aplikasi-aplikasi yang mereka gunakan.
[24]	Hasil penelitian dari 133 responden, ditemukan bahwa mayoritas dari mereka (85%) memiliki pemahaman tentang betapa pentingnya keamanan dari informasi. Namun, tidak selalu terlihat bahwa perilaku mereka mencerminkan tingkat keamanan informasi yang diinginkan. Sebanyak 75% responden tidak mengganti password secara berkala,

menunjukkan kurangnya kesadaran akan pentingnya mengubah password secara rutin. Selain itu, mereka cenderung mengakses media sosial di tempat umum tanpa mengetahui tingkat keamanan sistemnya. Lebih dari 40,6% akun media sosial responden masih terbuka untuk umum, sehingga informasi penting yang terkait dengan akun tersebut dapat diakses oleh siapa saja. Selanjutnya, sebanyak 54,9% responden tidak menerapkan pengaturan privasi yang memadai, mengindikasikan bahwa informasi mereka tidak dilindungi dengan baik dan dapat diakses oleh orang lain dengan bebas.

[25] Hasil penelitian dari 51 responden ditemukan bahwa sebanyak 58,8% atau 30 orang membaca *privacy policy* sebelum menyetujui ketentuannya. sebanyak 23,5% atau 12 orang menjawab mungkin, dan 17,7% menjawab tidak peduli. 41,2% atau 21 orang menjawab yakin dengan keamanan layanan yang menyimpan data informasi pribadi mereka. 49% atau 25 orang menjawab mungkin dan 9,8% atau 5 orang tidak peduli terkait hal itu. 32,3% atau 19 orang yakin dengan pertanyaan meminta persetujuan. 53.9% atau 27 orang menjawab mungkin dan 11,8% atau 6 orang tidak peduli. 74,5% atau 38 orang menyadari resiko yang dapat terjadi dengan informasi pribadinya. 13,7% atau 7 orang menjawab mungkin dan 11,8% atau 6 orang menjawab tidak. 90,2% atau 46 orang menjawab menyadari pentingnya perlindungan privasi. 5,9% atau 3 orang menjawab mungkin dan 3.9% atau 2 orang tidak peduli. 60,8 atau 31 orang memahami resiko pelanggaran privasi, 29,4% menjawab mungkin dan 9,8% atau 5 orang menjawab tidak.

Berdasarkan data tersebut dapat disimpulkan bahwa mayoritas orang masih kurangnya kesadaran dalam memahami akan pentingnya privasi dan keamanan data, yang membuat mereka rentan terhadap pencurian atau pemerasan oleh peretas atau oknum yang tidak bertanggung jawab. Hal ini menunjukkan perlunya peningkatan kesadaran dan tindakan yang lebih baik dalam melindungi privasi dan keamanan data pribadi media sosial.

3.3 Strategi Pencegahan

Berdasarkan topik permasalahan yang dibahas, perlu untuk mengetahui strategi pencegahan dalam melindungi privasi dan keamanan data menggunakan media sosial.

1. Penggunaan password yang kuat dengan mengkombinasikan huruf besar, huruf kecil, angka dan simbol serta melakukan penggantian berkala.
2. Mengatur batas terkait postingan, siapa yang dapat melihat informasi dan membatasi akses pihak ketiga ke data pengguna.
3. Berhati-hati dalam memberikan informasi pribadi yang bersifat sensitif seperti tanggal lahir, alamat, nama ibu kandung.
4. Membaca syarat dan ketentuan dengan teliti sebelum menyetujui terkait informasi yang dibagikan.
5. Meningkatkan kesadaran dan mengedukasi pengguna terkait pentingnya privasi dan keamanan data.
6. Memantau aktivitas dan riwayat akun jika terjadi aktivitas yang mencurigakan atau akses yang tidak sah.
7. Menggunakan aplikasi resmi dan terpercaya (Jangan menggunakan aplikasi tidak resmi atau modifikasi)
8. Selalu waspada dalam mengklik tautan link dan mendownload file.

Dengan menerapkan strategi pencegahan ini, pengguna media sosial diharapkan dapat meningkatkan keamanan dan juga privasi dari data mereka.

4. KESIMPULAN DAN SARAN

Berdasarkan data yang telah dikumpulkan ditemukan pelanggaran privasi dan keamanan data yang telah terjadi pada beberapa platform media sosial. Facebook mengalami pencurian dan keamanan data dari tahun dari tahun 2005-2018, Twitter menjadi media penyebaran konten pornografi pada tahun 2020, selanjutnya, pada tahun 2021 Linkedin mengalami kebocoran data terkait informasi pribadi penggunanya. kasus pelanggaran keamanan data pengguna dibawah umur juga ditemukan di media sosial Instagram pada tahun 2022 dan Tiktok pada tahun 2023. Dalam penelitian sebelumnya, ditemukan bahwa 6,9% atau 29 orang masih memiliki kesadaran privasi yang rendah. Sekitar 29,3% atau 122 orang sering menerima iklan atau berita di media sosial yang menunjukkan potensi adanya kebocoran informasi pribadi. Sekitar 45,4% atau 189 orang kurang memperhatikan privasi secara keseluruhan. Sementara sekitar 15,8% atau 66 orang memiliki kesadaran privasi yang tinggi, namun cenderung tidak memperhatikan izin dari aplikasi. Sekitar 75% orang tidak mengganti password secara berkala, lebih dari 40,6% akun media sosial responden masih terbuka untuk umum, 54,9% responden tidak menerapkan pengaturan privasi yang memadai. Hal ini menunjukkan bahwa kurangnya kesadaran pengguna terhadap privasi dan keamanan data di media sosial dapat memiliki dampak negatif. Penulis memberikan beberapa strategi pencegahan untuk melindungi privasi dan keamanan data, seperti menggunakan password yang kuat, membatasi informasi yang diberikan, membaca dengan cermat syarat dan ketentuan, meningkatkan kesadaran, memantau aktivitas dan riwayat akun, serta menggunakan aplikasi resmi dan terpercaya. Saran untuk penelitian selanjutnya dapat berfokus pada pemahaman dan kesadaran pengguna dengan menguji efektivitas strategi pencegahan untuk meningkatkan kesadaran dan pemahaman pengguna mengenai privasi dan keamanan data di media sosial.

5. DAFTAR RUJUKAN

[1] D. Revilia dan N. Irwansyah, "Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness," Jurnal Penelitian Komunikasi Dan Opini Publik, vol. 24, no. 1, pp. 1–15, 2020. [Online]. Tersedia: https://doi.org/10.33299/jpkop.24.1.2375

[2] S. Widi, "Pengguna Media Sosial di Indonesia Sebanyak 167 Juta pada 2023," data indonesia.id, 3 February 2020. [Online]. Available: https://dataindonesia.id/internet/detail/pengguna-media-sosial-di-indonesia-sebanyak-167-juta-pada-2023. [Accessed 1 6 2023].

[3] Hootsuite (We are Social), "Hootsuite (We are Social): Indonesian Digital Report 2020 – Andi Dwi Riyanto, Dosen, Praktisi, Konsultan, Pembicara: E-bisnis/Digital Marketing/Promotion/Internet marketing, SEO, Technopreneur, Fasilitator Google Gapura Digital yogyakarta," *Andi.Link/Hootsuite-We-Are-Social-Indonesian-Digital-Report*. p., 2020,[Online].Available:https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2020/.

[4] I. T. Islamy, S. T. Agatha, R. Ameron, B. Humaidi, Evan Fuad, and N. A. Rakhmawati, "Pentingnya memahami penerapan privasi di era teknologi informasi," Jurnal Teknologi Informasi dan Pendidikan, vol. 11, no. 2, pp. 21-28, 2018.

[5] S. Ikhtiara, "Pencegahan Privacy violation di media sosial pada kalangan remaja," Kalijaga Journal of Communication, vol. 1, no. 2, pp. 155-164, 2019.

[6] E. Aghasian, S. Garg, L. Gao, S. Yu, dan J. Montgomery, "Scoring Users' Privacy Disclosure Across Multiple Online Social Networks," IEEE Access, vol. 5, hal. 13118-13130, 2017. doi: 10.1109/ACCESS.2017.2720187

[7] A. Soumelidou dan A. Tsohou, "Effects of Privacy Policy Visualization on Users' Information Privacy Awareness Level: The case of Instagram," Information Technology and People, vol. 33, no. 2, hal. 502-534, 2019. doi: 10.1108/ITP-08-2017-0241.

[8] H. Wijoyo, N. Limakrisna, dan S. Suryanti, "The Effect of Renewal Privacy Policy Whatsapp to Customer Behavior," Insight Management Journal, vol. 1, no. 2, hal. 26-31, 2021. [Online]. Tersedia: https://journals.insightpub.org/index.php/imj
[9] R. F. Anggitafani, "Perlindungan hukum data pribadi peminjam pinjaman online perspektif POJK No. 1/POJK. 07/2013 tentang perlindungan konsumen sektor keuangan dan aspek kemaslahatan," Journal of Islamic Business Law, vol. 5, no. 2, pp. 55-72, 2021.
[10] D. Revilia, "Literasi Media Sosial : Kesadaran Keamanan Dan Privasi Dalam Perspektif Generasi Milenial Social Media Literacy : Millennial's Perspective Of Security And Privacy Awareness," pp. 1–15, 2020.
[11] N. Mohamed dan I. H. Ahmad, "Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence from Malaysia," Computers in Human Behavior, vol. 28, no. 6, hal. 2366-2375, 2012. doi: 10.1016/j.chb.2012.07.008.
[12] S. D. Nade, "Default Privacy vs Custom Privacy: Embodiment of Privacy by Adolescents during the Usage of Social Networking Site," IMPACT: International Journal, vol. 7, no. 2, hal. 87-98, 2019.
[13] V. Okditazeini dan Irwansyah, "Ancaman Privasi Dan Data Mining Di Era Digital: Analisis Meta-Sintesis Pada Social Networking Sites (SNS)," Jurnal Studi Komunikasi Dan Media, vol. 22, no. 2, pp. 109-122, Dec. 2018.
[14] I. P. Nurdiani, "Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime," J. Kriminologi Indonesia., vol. 16, pp. 1–10, 2020.
[15] R. Vebryto dan I. Irwansyah, "Pencurian Data dan Informasi di Media Sosial melalui Informasi Hoax: Studi Kasus pada Media Sosial Facebook," PERSPEKTIF, vol. 9, no. 2, pp. 366-377, 2020. [Online]. Available: http://ojs.uma.ac.id/index.php/perspektif. [Accessed: 1 June 2023].
[16] Kominfo. (2020). "Kominfo: Aduan Konten Negatif Didominasi Pornografi."Retrieved https://www.kominfo.go.id/content/detail/24960/kominfo-aduan-konten-negatif-didominasi-pornografi/0/sorotan_media.
[17] Iskandar, "LinkedIn Ungkap Informasi Akun dari 700 Juta Data Pengguna yang Bocor, Ini Detailnya," Liputan 6, 30 June 2021. [Online]. Available: https://www.liputan6.com/tekno/read/4594797/linkedin-ungkap-informasi-akun-dari-700-juta-data-pengguna-yang-bocor-ini-detailnya. [Accessed 3 June 2023].
[18] R. K. Hastuti, "500 Juta Data Pengguna LinkedIn Dikabarkan Bocor, Faktanya?," *CNBC Indonesia*. 2021, [Online]. Available: https://www.cnbcindonesia.com/tech/20210410175034-37-236852/500-juta-data-pengguna-linkedin-dikabarkan-bocor-faktanya.
[19] F. Fahusni, "Instagram Mendapatkan Denda Besar Gara-gara Data Privasi," Selular.id, 7 September 2022. [Online]. Available: https://selular.id/2022/09/instagram-mendapatkan-denda-besar-gara-gara-data-privasi/. [Accessed 10 July 2023].
[20] N. Ridhwan, "Kabar Terbaru TikTok: Dilarang di Perangkat Pemerintah Australia, Didenda Rp236 Miliar di Inggris," Tempo.co, 5 April 2023. [Online]. Available: https://dunia.tempo.co/read/1711370/kabar-terbaru-tiktok-dilarang-di-perangkat-pemerintah-australia-didenda-rp236-miliar-di-inggris. [Accessed 10 July 2023].
[21] H. P. Yuwinanto, "Privasi online dan keamanan data," *Palimpsest (Iowa. City).*, no. 031, p. 11, 2015
[22] D. Puspa, A. Soegiharto, A. Nizar Hidayanto, and Q. Munajat, "Data Privacy: What Still Needs Consideration in Online Application Systems?" Jurnal Sistem Informasi, vol. 16, no. 1, pp. 49-63, 2020. [Online]. Available: https://doi.org/10.21609/jsi.v16i1.941.
[23] Y. Liu, W. K. Tse, P. Y. Kwok, and Y. H. Chiu, "Impact of Social Media Behavior on Privacy Information Security Based on Analytic Hierarchy Process," Inf., vol. 13, no. 6, 2022, doi: 10.3390/info13060280.

[24] H. Gunawan, "PENGUKURAN KESADARAN KEAMANAN INFORMASI DAN PRIVASI DALAM SOSIAL MEDIA," J. Muara Sains, Teknologi, Kedokteran, dan Ilmu Kesehatan, vol. 5, no. 1, pp. 1-8, 2021. DOI: 10.24912/jmstkik.v5i1.3456.
[25] J. R. Batmetan, B. Kariso, M. Moningkey, and A. Tumembow, "Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi," p. 4, 2018, doi: 10.31219/OSF.IO/CAHZR.