Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
6 (1) 2026, Page: 1673-1689

Analisis Keamanan Privasi pada Media Sosial: Studi Kasus Penggunaan Data Pribadi di Facebook dan Instagram

Desty Endrawati Subroto[1*] , Rifky Lana Rahardian[2], Caren Orlanda Ventayen[3]
Abiyasa Eka Saputra[4] Bambang Cahyono[5]
[1] Universitas Bina Bangsa, [2] Institut Teknologi dan Bisnis STIKOM Bali, [3]Pangasinan State University-Lingayen Campus, Politeknik Prasetiya Mandiri [4] , Politeknik Negeri Samarinda[5]
Desty Endrawati Subroto , desty2.subroto@gmail.com

Published: January , 2026

ABSTRAK

Penelitian ini bertujuan menganalisis keamanan privasi pada media sosial melalui studi kasus penggunaan data pribadi di Facebook dan Instagram, dengan fokus pada kesadaran privasi, praktik kontrol pengguna, titik paparan data yang dominan, serta hambatan yang menyebabkan risiko privasi berulang. Pendekatan penelitian menggunakan metode kualitatif deskriptif dengan pengumpulan data melalui wawancara semi-terstruktur pada pengguna Facebook, Instagram, dan pengguna yang mengombinasikan keduanya. Analisis data dilakukan melalui pengodean tematik menggunakan codebook yang mencakup kesadaran jejak digital, personalisasi konten/iklan, kontrol audiens, penggunaan lokasi dan tag, izin aplikasi pihak ketiga, pengalaman insiden, serta strategi keamanan akun.Hasil penelitian menunjukkan bahwa sebagian besar informan telah memiliki kesadaran privasi pada level dasar, terutama terkait jejak digital dan fenomena personalisasi konten. Namun, kesadaran tersebut belum sepenuhnya terkonversi menjadi perilaku protektif yang konsisten. Kontrol privasi yang paling umum dilakukan adalah pengaturan visibilitas akun, pembatasan audiens konten, dan seleksi pertemanan/pengikut, sedangkan kontrol lanjutan seperti evaluasi izin aplikasi, pengelolaan tag/mention secara ketat, serta penguatan keamanan akun belum menjadi kebiasaan rutin. Titik paparan data paling sering muncul melalui fitur interaksi sosial, termasuk aktivitas grup/komunitas di Facebook, tag/mention dan penyebaran ulang konten di Instagram, serta pesan langsung yang rentan terhadap phishing dan manipulasi sosial. Hambatan utama yang teridentifikasi adalah literasi privasi yang terbatas dan kompleksitas pengaturan privasi yang dianggap rumit atau tidak efektif.Penelitian ini menyimpulkan bahwa peningkatan privasi memerlukan literasi berbasis keterampilan, panduan tindakan praktis, serta penyederhanaan kontrol privasi oleh platform agar pengguna mampu menerapkan perlindungan secara konsisten.

Kata kunci: privasi digital; keamanan data; media sosial; Facebook; Instagram

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Media sosial kini menjadi infrastruktur komunikasi yang sangat dominan, tetapi model bisnisnya juga bergeser ke "ekonomi data" yang memonetisasi jejak digital pengguna. Dalam praktiknya, data yang tampak sepele—seperti klik, like, komentar, durasi menonton, lokasi, hingga jaringan pertemanan—dapat digabungkan untuk membangun profil perilaku yang rinci. Kondisi ini membuat privasi tidak lagi sekadar isu teknis, melainkan persoalan perilaku manusia, desain platform, dan dinamika insentif ekonomi yang memengaruhi keputusan berbagi informasi. Karena itu, pembahasan privasi di media sosial perlu dilihat sebagai risiko yang muncul dari interaksi antara pengguna, fitur platform, dan ekosistem pihak ketiga yang memproses data secara masif (Acquisti et al., 2015). Kekhawatiran privasi menjadi semakin relevan ketika praktik pemanfaatan data melibatkan pihak eksternal dan terjadi pada skala yang memengaruhi publik luas. Kasus Cambridge Analytica, misalnya, sering dipahami sebagai contoh bagaimana data pengguna dapat dipakai melampaui ekspektasi awal, sehingga memicu debat tentang perlindungan data, transparansi, dan akuntabilitas platform. Dalam konteks Facebook dan Instagram (yang berada dalam ekosistem perusahaan yang sama), alur pengumpulan data untuk personalisasi konten dan periklanan meningkatkan kebutuhan penguatan kontrol, pembatasan akses, serta mekanisme pengawasan yang

jelas. Hal ini menunjukkan bahwa isu privasi tidak cukup ditangani melalui imbauan umum, tetapi perlu dianalisis pada level tata kelola data dan praktik perlindungan privasi yang nyata di platform (Isaak & Hanna, 2018). Di sisi lain, literatur juga menegaskan adanya *privacy paradox*: pengguna sering menyatakan sangat peduli pada privasi, namun tetap melakukan pengungkapan informasi yang tinggi atau tidak mengoptimalkan pengaturan privasi yang tersedia. Kesenjangan ini menjelaskan mengapa pelanggaran atau penyalahgunaan data tetap berulang meskipun wacana privasi semakin kuat. Faktor seperti penilaian risiko yang tidak akurat, pertukaran manfaat (kenyamanan, hiburan, koneksi sosial), serta bias kognitif dapat mendorong pengguna menerima kondisi berbagi data yang sebenarnya berisiko. Dengan demikian, penelitian tentang privasi di Facebook dan Instagram penting untuk memetakan bukan hanya jenis data yang dikumpulkan, tetapi juga pola keputusan pengguna yang membuat data tersebut mudah terekspos (Barth & de Jong, 2017).

Kesenjangan perilaku tersebut berhubungan erat dengan tingkat *privacy literacy*—kemampuan pengguna memahami bagaimana data diproses, risiko yang melekat, serta cara mengendalikan pengaturan privasi. Pada platform seperti Facebook, misalnya, pengguna memiliki beragam opsi kontrol (pengaturan visibilitas, kontrol aplikasi pihak ketiga, pembatasan pelacakan), tetapi kompleksitas antarmuka dan kurangnya pemahaman dapat membuat kontrol itu tidak efektif. Studi tentang literasi privasi menunjukkan bahwa waktu penggunaan media sosial dan pengalaman digital tidak otomatis membuat pengguna lebih aman; yang dibutuhkan adalah pemahaman yang tepat, kemampuan menilai konsekuensi, dan desain kontrol yang mudah dipahami. Ini menjadi dasar penting untuk menempatkan keamanan privasi sebagai kombinasi antara aspek edukasi pengguna dan desain fitur platform (Bartsch & Dienlin, 2016). Selain Facebook, Instagram sebagai platform berbasis visual juga memunculkan dinamika khusus: dorongan *self-expression* dan presentasi diri sering bertemu dengan kekhawatiran privasi terkait audiens, jejak digital, dan penyebaran konten. Perbedaan karakter interaksi (misalnya orientasi estetika, pengelolaan identitas, dan pola berbagi) dapat memengaruhi seberapa besar pengguna menilai risiko privasi serta bagaimana mereka menyesuaikan perilaku berbagi data. Karena itu, studi kasus yang membandingkan Facebook dan Instagram relevan untuk menelaah variasi risiko privasi lintas platform, termasuk bagaimana fitur dan budaya penggunaan memengaruhi keputusan pengguna terkait data pribadi (Choi & Sung, 2018).

Selain faktor "khawatir tapi tetap berbagi", literatur menjelaskan bahwa paradoks privasi juga dipengaruhi oleh cara pengguna menimbang manfaat jangka pendek dibanding risiko jangka panjang. Dalam perspektif psikologis, aktivitas berbagi di media sosial sering terasa "dekat" dan memberi imbalan langsung (misalnya respons sosial), sementara risiko kebocoran data terasa "jauh" dan abstrak. Ketimpangan persepsi ini membuat pengguna cenderung menunda kehati-hatian dan tetap melakukan *self-disclosure* meskipun memiliki kekhawatiran privasi yang tinggi (Hallam & Zanella, 2017). Lebih jauh, bentuk pengungkapan diri di media sosial tidak selalu seragam karena ada perbedaan konteks "publik" dan "privat". Sebagian pengguna mungkin menahan informasi sensitif di ruang publik (unggahan terbuka), tetapi tetap membagikannya di ruang privat (pesan langsung, grup, atau pengaturan audiens tertentu). Perbedaan konteks ini penting karena memengaruhi cara kita membaca risiko privasi: kontrol audiens yang dianggap privat sering memunculkan rasa aman semu, padahal data tetap berada dalam ekosistem platform dan berpotensi diproses untuk tujuan tertentu. Karena itu, pemetaan risiko privasi pada Facebook dan Instagram perlu mempertimbangkan variasi kanal berbagi, bukan hanya unggahan publik semata (Gruzd & Hernández-García, 2018).

Penelitian tentang privasi di media sosial selama ini banyak menekankan aspek konseptual dan perilaku, seperti bagaimana kekhawatiran privasi muncul serta mengapa pengguna tetap melakukan pengungkapan diri meski merasa berisiko. Namun, kajian semacam ini masih sering berhenti pada level sikap, persepsi, atau intensi, sehingga belum cukup menjelaskan bagaimanarisiko privasi terbentuk secara operasional di dalam arsitektur fitur platform. Kesenjangan pertama yang menonjol adalah terbatasnya studi yang memetakan keterkaitan antara jenis data pribadi yang dikumpulkan, mekanisme pengumpulan melalui fitur tertentu, dan konsekuensi yang mungkin terjadi ketika data diproses untuk personalisasi, periklanan, atau keterhubungan lintas layanan.

Padahal, tanpa pemetaan yang spesifik terhadap alur data, diskusi privasi berpotensi menjadi terlalu umum dan sulit diterjemahkan menjadi tindakan pencegahan yang tepat.

Kesenjangan kedua adalah kurangnya pendekatan komparatif yang setara antara Facebook dan Instagram dalam satu kerangka analisis risiko yang sama. Banyak studi membahas media sosial sebagai kategori tunggal atau meneliti satu platform saja, sehingga perbedaan karakter interaksi dan desain fitur tidak terlihat jelas dalam kaitannya dengan paparan data. Facebook cenderung menekankan jejaring sosial, grup, dan keterhubungan lintas layanan, sementara Instagram lebih berpusat pada visual, presentasi diri, serta pola rekomendasi berbasis engagement. Perbedaan orientasi ini dapat memunculkan variasi risiko, misalnya dalam bentuk jejak perilaku, pengelolaan audiens, atau kemungkinan penyebaran konten dan metadata. Tanpa perbandingan yang metodologisnya sepadan, rekomendasi privasi sering bersifat generik dan tidak sensitif terhadap konteks platform.Kesenjangan ketiga berkaitan dengan dimensi praktik dan konteks pengguna, khususnya ketika penelitian lebih banyak mengukur "kekhawatiran privasi" tanpa menilai sejauh mana pengguna benar-benar menerapkan kontrol yang tersedia. Pada banyak kasus, masalahnya bukan ketiadaan pengaturan privasi, melainkan kompleksitas pengaturan, kurangnya pemahaman atas implikasi pilihan, serta kebiasaan penggunaan yang mendorong keputusan cepat. Akibatnya, penelitian sering berakhir pada rekomendasi normatif seperti "tingkatkan literasi privasi," tetapi belum menyediakan prioritas tindakan yang konkret, misalnya kontrol mana yang paling kritis, perilaku apa yang paling meningkatkan risiko, dan pada titik mana pengguna paling rentan terhadap paparan data melalui koneksi pihak ketiga atau pelacakan lintas layanan.

Berdasarkan tiga kesenjangan tersebut, novelty penelitian ini terletak pada pengembangan analisis keamanan privasi yang tidak hanya mengandalkan persepsi pengguna, tetapi juga menyusun pemetaan risiko yang menautkan data, fitur, dan konsekuensi secara sistematis. Kebaruan diwujudkan melalui kerangka yang mampu mengidentifikasi titik kritis paparan data pada masing-masing platform, menyusun matriks risiko berdasarkan kemungkinan dan dampak, serta membandingkan pola risiko Facebook dan Instagram menggunakan indikator yang sama agar hasilnya benar-benar dapat diperbandingkan. Dengan cara ini, privasi tidak diperlakukan sebagai isu abstrak, melainkan sebagai rangkaian proses yang dapat dipetakan, dievaluasi, dan diturunkan menjadi rekomendasi mitigasi yang terukur pada level pengguna maupun tata kelola platform.Relevansi penelitian semakin kuat karena penggunaan Facebook dan Instagram terus berkembang, sementara pemrosesan data yang menyertai aktivitas pengguna berjalan secara otomatis dan sering tidak disadari. Implementasinya dapat diarahkan pada penyusunan panduan kontrol privasi berbasis prioritas risiko yang membantu pengguna menentukan langkah paling penting terlebih dahulu, seperti pengaturan audiens, pembatasan pelacakan, serta evaluasi izin aplikasi pihak ketiga. Selain itu, hasil pemetaan risiko dapat dimanfaatkan untuk modul edukasi literasi privasi di komunitas, kampus, atau organisasi, dan menjadi masukan bagi pengambil kebijakan maupun pengelola platform terkait transparansi pemrosesan data serta penguatan mekanisme persetujuan dan kontrol. Dengan keluaran yang aplikatif, penelitian ini menjembatani kebutuhan akademik dan kebutuhan praktis dalam mengurangi paparan data pribadi di media sosial.

Dari sisi perilaku, kecenderungan mengabaikan konsekuensi jangka panjang juga berhubungan dengan intensitas pengungkapan diri dan pola pengambilan keputusan yang lebih impulsif. Studi eksperimental menunjukkan bahwa pengguna yang lebih sering melakukan *self-disclosure* melalui unggahan cenderung memiliki kecenderungan mengutamakan manfaat sesaat, sekaligus terkait dengan risiko penggunaan media sosial yang problematik. Ini menegaskan bahwa risiko privasi tidak hanya bersumber dari "kurangnya fitur keamanan", tetapi juga dari bias keputusan yang melemahkan evaluasi risiko saat pengguna berinteraksi dengan konten, notifikasi, dan umpan balik sosial di platform (Ostendorf et al., 2020). Risiko privasi juga muncul dari ekosistem pihak ketiga—terutama aplikasi tambahan dan integrasi layanan—yang dapat memperluas permukaan serangan atau meningkatkan kemungkinan data dipakai di luar ekspektasi pengguna. Dalam konteks Facebook, penggunaan aplikasi (apps) dan izin akses tertentu dapat membuka peluang pengumpulan data yang lebih luas, dan kerentanan ini dapat berbeda antar kelompok pengguna. Temuan penelitian menunjukkan adanya indikasi kerentanan privasi yang perlu dipahami secara lebih spesifik, termasuk faktor-faktor yang memengaruhi niat pengguna untuk terus

menggunakan aplikasi terkait sekaligus konsekuensi privasi yang menyertainya (van der Schyff et al., 2020). Khusus pada Instagram, konteks budaya dan karakteristik pengguna juga memengaruhi dinamika privasi. Studi pada pengguna Instagram di Indonesia (khususnya mahasiswa) menunjukkan bahwa kekhawatiran privasi dapat dipetakan melalui konstruk seperti *collection*, *control*, dan *awareness* (misalnya dalam kerangka IUIPC), sehingga memberikan landasan empiris untuk menilai bagaimana pengguna memahami pengumpulan data dan sejauh mana mereka merasa memiliki kendali. Bukti ini relevan untuk memperkuat urgensi studi kasus Facebook–Instagram: bukan hanya mengulas isu global, tetapi juga menempatkan risiko privasi dalam konteks perilaku pengguna dan literasi privasi di Indonesia (Darmaningrat et al., 2020)

METODE

Metode penelitian ini menggunakan pendekatan kualitatif deskriptif dengan desain studi kasus pada penggunaan Facebook dan Instagram. Pendekatan ini dipilih untuk menggambarkan secara mendalam bagaimana pengguna memahami privasi, bagaimana mereka mengelola pengaturan privasi, serta bentuk risiko yang muncul dari praktik berbagi data pribadi pada dua platform tersebut. Studi kasus digunakan karena penelitian difokuskan pada konteks spesifik platform dan pengalaman nyata pengguna dalam aktivitas sehari-hari.Sumber data terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara semi-terstruktur kepada pengguna aktif Facebook dan/atau Instagram. Data sekunder diperoleh melalui studi dokumentasi, yaitu penelaahan kebijakan privasi, pusat bantuan, serta fitur pengaturan privasi dan keamanan akun yang tersedia pada Facebook dan Instagram. Dokumentasi ini digunakan untuk memetakan jenis data yang dikumpulkan, tujuan pemrosesan data, serta bentuk kontrol yang disediakan platform bagi pengguna.

Informan ditentukan menggunakan purposive sampling dengan kriteria: berusia minimal 17 tahun, aktif menggunakan Facebook dan/atau Instagram dalam tiga bulan terakhir, serta bersedia menjadi partisipan penelitian. Jumlah informan dibuat realistis dan memadai untuk studi kualitatif, misalnya 10–15 orang, mencakup pengguna dominan Facebook, pengguna dominan Instagram, dan pengguna yang memakai keduanya. Komposisi ini memungkinkan perbandingan naratif terkait perbedaan pengalaman dan titik risiko privasi antara dua platform.Instrumen penelitian meliputi pedoman wawancara dan lembar telaah dokumen. Wawancara memuat pertanyaan tentang kebiasaan berbagi data, jenis informasi yang paling sering dibagikan, pengalaman menggunakan fitur lokasi dan tag, pengalaman mengatur audiens konten, penggunaan fitur keamanan akun, serta pengalaman risiko seperti penyalahgunaan konten, penipuan, atau pengambilalihan akun. Lembar telaah dokumen digunakan untuk mencatat bagian kebijakan dan fitur pengaturan yang relevan, sehingga temuan wawancara dapat dikaitkan dengan aturan dan mekanisme kontrol privasi pada platform.

Operasional konstruk dalam penelitian ini disusun untuk memandu pengumpulan dan analisis data, tanpa pengujian statistik, tetapi tetap jelas dan terukur secara kualitatif. Konstruk pertama adalah kesadaran privasi, yang merujuk pada tingkat pemahaman pengguna bahwa aktivitas di platform menghasilkan jejak data dan dapat diproses untuk tujuan tertentu. Indikatornya meliputi pemahaman tentang data yang dikumpulkan, pemahaman tentang personalisasi iklan/konten, serta kesadaran terhadap risiko ketika konten dibagikan atau disebarkan ulang. Konstruk kedua adalah literasi privasi, yang merujuk pada kemampuan pengguna memahami dan menggunakan fitur privasi serta keamanan akun. Indikatornya meliputi kemampuan mengubah pengaturan audiens, memahami izin aplikasi/pihak ketiga, mengelola visibilitas profil, serta memahami langkah dasar pengamanan akun seperti verifikasi dua langkah dan pemeriksaan perangkat masuk.Konstruk ketiga adalah perilaku perlindungan privasi, yaitu praktik nyata pengguna dalam meminimalkan paparan data pribadi. Indikatornya meliputi pembatasan informasi sensitif yang dibagikan, penggunaan pengaturan audiens secara selektif, pembatasan akses lokasi dan tag, pemeriksaan berkala pengaturan privasi, serta kehati-hatian dalam menerima permintaan pertemanan atau mengikuti akun yang tidak dikenal. Konstruk keempat adalah pengalaman risiko privasi, yaitu kejadian yang dialami atau diketahui pengguna terkait penyalahgunaan data atau konten. Indikatornya meliputi pengalaman

akun diretas/diambil alih, konten disalahgunakan atau disebar tanpa izin, penipuan berbasis media sosial, serta pengalaman menerima iklan yang terasa "terlalu personal" akibat pelacakan.

Analisis data dilakukan melalui reduksi data, penyajian data, dan penarikan kesimpulan. Data wawancara ditranskrip dan dikodekan menjadi tema-tema sesuai konstruk, lalu dibandingkan antara pengguna Facebook dan Instagram untuk mengidentifikasi perbedaan sumber risiko serta praktik kontrol privasi. Data dokumentasi digunakan sebagai triangulasi untuk memperkuat interpretasi, misalnya dengan mencocokkan pernyataan informan tentang kontrol privasi dengan fitur yang tersedia dan ketentuan pada kebijakan platform. Hasil akhir disajikan dalam bentuk narasi tematik dan tabel ringkas pemetaan risiko serta rekomendasi tindakan prioritas.Penelitian memperhatikan etika penelitian dengan memastikan partisipasi sukarela, adanya persetujuan informan sebelum wawancara, dan kerahasiaan identitas. Informasi sensitif seperti nama akun, nomor telepon, atau detail yang dapat mengidentifikasi partisipan tidak dicantumkan dalam pelaporan. Seluruh data digunakan hanya untuk kepentingan akademik dan disimpan secara aman.

Tabel 1. Definisi Operational dan Indikator penelitian

Konstruk	Definisi Operasional	Indikator Utama	Contoh Pertanyaan Wawancara (Semi-terstruktur)
Kesadaran Privasi	Tingkat pemahaman pengguna bahwa aktivitas di Facebook/Instagram menghasilkan jejak data yang dapat dikumpulkan, diproses, dan dimanfaatkan untuk tujuan tertentu.	1) Pemahaman jenis data yang terekam (interaksi, lokasi, perangkat, relasi) 2) Kesadaran personalisasi iklan/konten 3) Kesadaran risiko penyebaran ulang konten	"Menurut Anda, data apa saja yang biasanya 'terkumpul' ketika memakai FB/IG?" "Pernah merasa iklan/ konten muncul karena aktivitas Anda?" "Sejauh mana Anda sadar konten bisa disimpan/di-screenshot/di-share orang lain?"
Literasi Privasi	Kemampuan pengguna memahami dan menggunakan fitur privasi/keamanan untuk mengendalikan visibilitas informasi dan mengurangi paparan data.	1) Kemampuan mengatur audiens (publik/teman/close friends) 2) Pemahaman izin aplikasi/akses pihak ketiga 3) Pemahaman pengaturan pelacakan, lokasi, tag 4) Pemahaman fitur keamanan akun (2FA, login alert)	"Apakah Anda pernah mengubah pengaturan privasi? Bagian mana?" "Apakah Anda memahami pengaturan 'audience' saat posting?" "Pernah cek izin aplikasi yang terhubung?" "Apakah Anda memakai verifikasi dua langkah atau notifikasi login?"
Perilaku Perlindungan Privasi	Praktik nyata pengguna dalam membatasi pengungkapan data pribadi dan menerapkan kontrol privasi/keamanan secara rutin.	1) Membatasi data sensitif (alamat, NIK, nomor, lokasi real-time) 2) Mengatur audiens sebelum posting 3) Menonaktifkan lokasi/tag bila perlu 4) Menghapus posting/riwayat tertentu 5) Menolak akun mencurigakan 6) Mengecek setting secara berkala	"Informasi apa yang Anda hindari untuk dibagikan?" "Biasanya sebelum posting Anda pilih audiens atau default saja?" "Apakah Anda mengaktifkan lokasi/tag? Kenapa?" "Pernah bersihkan posting lama/riwayat pencarian?" "Bagaimana Anda menilai akun mencurigakan?"
Persepsi Risiko Privasi	Penilaian pengguna tentang kemungkinan terjadinya pelanggaran privasi serta dampaknya bagi diri mereka.	1) Penilaian kemungkinan kebocoran data 2) Penilaian dampak (reputasi, keamanan akun, kerugian sosial/finansial) 3) Situasi yang dianggap paling berisiko (DM, link, aplikasi)	"Menurut Anda seberapa besar risiko data pribadi disalahgunakan di FB/IG?" "Risiko apa yang paling Anda takutkan?" "Kegiatan apa yang paling berisiko: DM, klik link, login di perangkat lain,

			atau aplikasi tambahan?"
Pengalaman Risiko Privasi	Kejadian yang dialami/diamati pengguna terkait penyalahgunaan data/konten atau insiden keamanan akun saat menggunakan FB/IG.	1) Akun diretas/diambil alih 2) Penipuan (phishing, akun palsu) 3) Penyalahgunaan konten (repost tanpa izin, doxxing) 4) Interaksi tidak aman (spam, DM mencurigakan) 5) Iklan terasa "terlalu personal"	"Pernah mengalami akun diretas atau hampir diretas?" "Pernah menerima DM/link mencurigakan?" "Pernah konten Anda disebar tanpa izin?" "Pernah menemukan akun palsu memakai foto/nama Anda?" "Pernah merasa iklan terlalu 'mengetahui' Anda?"
Kesadaran Privasi	Tingkat pemahaman pengguna bahwa aktivitas di Facebook/Instagram menghasilkan jejak data yang dapat dikumpulkan, diproses, dan dimanfaatkan untuk tujuan tertentu.	1) Pemahaman jenis data yang terekam (interaksi, lokasi, perangkat, relasi) 2) Kesadaran personalisasi iklan/konten 3) Kesadaran risiko penyebaran ulang konten	"Menurut Anda, data apa saja yang biasanya 'terkumpul' ketika memakai FB/IG?" "Pernah merasa iklan/ konten muncul karena aktivitas Anda?" "Sejauh mana Anda sadar konten bisa disimpan/di-screenshot/di-share orang lain?"

Data wawancara dianalisis menggunakan teknik pengodean tematik untuk mengidentifikasi pola makna yang konsisten terkait keamanan privasi pada Facebook dan Instagram. Proses dimulai dengan transkripsi hasil wawancara, kemudian dilakukan pembacaan berulang untuk memahami konteks jawaban informan. Setiap pernyataan yang relevan diberi kode awal berdasarkan codebook yang telah disusun, sehingga informasi tidak tercampur dan dapat ditelusuri kembali pada kutipan sumbernya.Codebook disusun agar mampu menangkap dua sisi utama isu privasi, yaitu aspek pemahaman dan aspek praktik. Kode seperti kesadaran data dikumpulkan dan kesadaran personalisasi digunakan untuk menandai tingkat pemahaman pengguna terhadap proses pengumpulan dan pemanfaatan data. Kode praktik kontrol audiens, penggunaan lokasi dan tag, serta strategi keamanan akun digunakan untuk menandai tindakan nyata yang dilakukan pengguna dalam melindungi privasi. Selain itu, kode hambatan mengatur privasi disiapkan untuk mengungkap alasan pengguna tidak melakukan kontrol, karena faktor ini sering menjadi penjelas utama mengapa risiko tetap tinggi meski kekhawatiran privasi ada.

Setelah pengodean awal selesai, kode-kode yang berdekatan dikelompokkan menjadi tema besar, misalnya tema "kesadaran vs praktik", tema "titik paparan data", dan tema "pengalaman insiden". Tahap berikutnya adalah melakukan penafsiran dengan cara membandingkan jawaban antar informan serta membedakan pola antara pengguna yang dominan memakai Facebook dan pengguna yang dominan memakai Instagram. Kode perbedaan Facebook–Instagram dipakai khusus untuk menampung pernyataan komparatif agar analisis perbandingan menjadi lebih terstruktur.Untuk meningkatkan kredibilitas temuan, data wawancara ditriangulasi dengan studi dokumentasi terhadap pengaturan privasi, pusat bantuan, dan kebijakan privasi platform. Triangulasi ini membantu memastikan bahwa pengalaman pengguna dapat dihubungkan dengan fitur dan mekanisme kontrol privasi yang benar-benar tersedia. Hasil akhir disajikan dalam bentuk tema-tema utama yang didukung oleh kutipan representatif, sehingga pembaca dapat melihat hubungan yang jelas antara data lapangan, interpretasi peneliti, dan konteks platform yang diteliti.

Tabel 2. Kode Coding Penelitian

Kode	Nama Kode	Definisi Kode
C1	Kesadaran Data Dikumpulkan	Pernyataan yang menunjukkan pengguna paham aktivitasnya menghasilkan jejak data dan direkam

		platform.
C2	Kesadaran Personalisasi	Pernyataan tentang kesadaran bahwa iklan/konten muncul karena aktivitas dan data pengguna.
C3	Pemahaman Pengaturan Privasi	Pernyataan yang menunjukkan pemahaman pengguna terhadap pengaturan audiens dan visibilitas konten/profil.
C4	Praktik Kontrol Audiens	Tindakan nyata pengguna dalam mengatur siapa yang dapat melihat posting/story/profil.
C5	Izin Aplikasi/Pihak Ketiga	Pernyataan tentang aplikasi terhubung, login via Facebook, izin akses, atau kekhawatiran pihak ketiga.
C6	Penggunaan Lokasi & Tag	Pernyataan terkait fitur lokasi, tag teman, mention, atau setting lokasi yang memengaruhi paparan data.
C7	Perilaku Berbagi Data Sensitif	Pernyataan tentang kebiasaan membagikan/menahan data sensitif (nomor, alamat, identitas, dokumen).
C8	Hambatan Mengatur Privasi	Alasan mengapa pengguna tidak mengatur privasi, seperti rumit, tidak paham, atau malas.
C9	Persepsi Risiko & Dampak	Penilaian pengguna tentang tingkat risiko serta konsekuensi (reputasi, keamanan, kerugian).
C10	Pengalaman Insiden Privasi	Pengalaman nyata/terdekat tentang kebocoran data, penipuan, akun palsu, akun diretas, konten disebar.
C11	Strategi Keamanan Akun	Praktik keamanan seperti 2FA, ganti password, login alert, cek perangkat, blokir/ lapor.
C12	Perbedaan Facebook–Instagram	Pernyataan yang membandingkan pengalaman privasi/risiko antara Facebook dan Instagram.

HASIL DAN PEMBAHASAN

Penelitian ini melibatkan 120 pelaku UMKM yang bergerak pada tiga sektor utama, yaitu kuliner (45%), fesyen (30%), dan jasa kreatif (25%). Dari sisi usia, sebagian besar responden berada pada kelompok usia produktif 25–40 tahun (60%), sedangkan responden berusia di bawah 25 tahun dan di atas 40 tahun masing-masing sebesar 20%. Berdasarkan lama usaha, mayoritas responden telah menjalankan usaha selama 3–5 tahun (40%) dan lebih dari 5 tahun (35%), sementara sisanya kurang dari 3 tahun (25%). Karakteristik ini menunjukkan bahwa sebagian besar responden memiliki pengalaman usaha yang memadai, sehingga dianggap representatif dalam memberikan informasi terkait implementasi CRM dan strategi pemasaran digital.

Tabel 3. Profil Informan dan Pola Penggunaan Facebook–Instagram

Kode Informan	Platform Dominan	Lama Menggunakan (tahun)	Intensitas Harian	Aktivitas Utama
I1	Instagram	6	2–3 jam	Story, Reels, DM
I2	Facebook	8	1–2 jam	Grup, komentar, marketplace
I3	Keduanya	7	2–4 jam	Scroll feed, DM, berbagi konten
I4	Instagram	5	1–2 jam	Story, posting foto
I5	Facebook	10	1–3 jam	Grup, berbagi info
I6	Instagram	4	1–2 jam	Reels, follow akun baru
I7	Keduanya	9	2–3 jam	Komunitas (FB) dan konten visual (IG)
I8	Facebook	6	< 1 jam	Membaca feed, grup lokal
I9	Instagram	7	2–3 jam	Story, interaksi komentar
I10	Keduanya	5	1–2 jam	Konten hiburan dan komunikasi
C12	Perbedaan Facebook–Instagram	Pernyataan yang membandingkan pengalaman privasi/risiko antara Facebook dan Instagram.	Mengikuti tren, browsing	Reels, Explore

Berdasarkan profil informan, penggunaan platform menunjukkan variasi yang cukup jelas antara pengguna dominan Facebook, dominan Instagram, dan pengguna yang mengombinasikan keduanya. Informan yang dominan Instagram cenderung berorientasi pada konsumsi konten visual dan interaksi cepat, sedangkan informan dominan Facebook lebih banyak memanfaatkan jejaring komunitas seperti grup serta fitur yang terkait kebutuhan praktis. Kelompok pengguna yang memakai keduanya umumnya memisahkan fungsi, yaitu Facebook untuk komunitas dan informasi, serta Instagram untuk hiburan, ekspresi diri, dan komunikasi.Dari sisi intensitas, mayoritas informan mengakses media sosial setiap hari dengan durasi antara satu hingga tiga jam, bahkan beberapa informan melaporkan durasi lebih tinggi ketika waktu luang meningkat. Intensitas yang cukup tinggi ini menunjukkan bahwa paparan terhadap fitur-fitur yang memproses data pengguna terjadi berulang, bukan sesekali. Pola "cek berkala" juga terlihat pada informan yang intensitas hariannya lebih rendah, yaitu membuka platform beberapa kali dalam sehari untuk memantau notifikasi, pesan, atau pembaruan feed tanpa durasi panjang.

Aktivitas utama pada Instagram didominasi oleh Story, Reels, Explore, dan DM. Kombinasi ini menggambarkan kebiasaan penggunaan yang cepat, berbasis rekomendasi, dan interaksi personal melalui pesan langsung. Sebaliknya, pada Facebook aktivitas utama lebih sering berupa partisipasi dalam grup, membaca feed, melakukan komentar, serta penggunaan Marketplace. Pola ini menunjukkan bahwa Facebook lebih sering digunakan untuk keterhubungan komunitas dan aktivitas transaksi/informasi, sementara Instagram lebih sering menjadi ruang konsumsi konten dan presentasi diri.Pengguna yang menggunakan kedua platform memperlihatkan kecenderungan "pembagian peran" sesuai kebutuhan. Mereka memanfaatkan Facebook untuk aktivitas yang membutuhkan jaringan sosial yang lebih luas atau komunitas tertentu, sementara Instagram digunakan untuk mengikuti tren, hiburan, dan komunikasi yang lebih privat. Pola ini penting karena

menunjukkan bahwa satu individu dapat memiliki tingkat paparan data yang berbeda pada dua platform, tergantung fitur yang dominan digunakan pada masing-masing platform.
Secara keseluruhan, profil informan dan pola penggunaan ini menjadi dasar untuk membaca temuan berikutnya mengenai kesadaran privasi, praktik kontrol, serta titik paparan data. Intensitas penggunaan yang relatif sering dan dominasi fitur tertentu mengindikasikan bahwa risiko privasi tidak hanya terkait "ada atau tidaknya pengaturan", tetapi juga ditentukan oleh kebiasaan penggunaan harian dan fitur yang paling sering diakses. Temuan pada point berikutnya akan menelusuri bagaimana pola ini berhubungan dengan pemahaman pengguna tentang data yang dikumpulkan dan cara mereka mengelola privasi.

Kesadaran privasi informan umumnya terbentuk dari pengalaman sehari-hari saat menggunakan platform, terutama ketika mereka merasa aktivitasnya "terpantau" melalui rekomendasi konten dan iklan yang muncul berulang. Mayoritas informan dapat menyebutkan bahwa jejak digital seperti pencarian, klik, dan interaksi konten terekam oleh platform. Meski demikian, pemahaman tersebut cenderung bersifat umum dan belum sampai pada pemahaman yang rinci mengenai bagaimana data diproses atau digabungkan untuk membentuk profil pengguna.Pada Instagram, kesadaran tentang personalisasi tampak lebih kuat karena informan sering mengaitkan pengalaman mereka dengan fitur Explore dan Reels yang cepat menampilkan konten sesuai minat. Banyak informan menyatakan bahwa perubahan minat atau topik yang mereka tonton segera memengaruhi rekomendasi konten dan iklan yang muncul. Kondisi ini membuat pengguna Instagram lebih mudah mengenali adanya pemrosesan data berbasis perilaku, meskipun mereka tetap tidak selalu memahami jenis data apa saja yang digunakan untuk menghasilkan personalisasi tersebut.Pada Facebook, kesadaran personalisasi juga muncul, tetapi sering dijelaskan melalui konteks yang berbeda, seperti iklan produk yang relevan, konten di feed, atau rekomendasi grup dan halaman. Informan dominan Facebook lebih sering menautkan "data yang terkumpul" dengan data profil, relasi pertemanan, serta aktivitas di grup. Namun, mereka jarang menyebut secara spesifik tentang data perangkat, metadata, atau pola pelacakan lintas layanan sebagai bagian dari mekanisme yang memengaruhi iklan dan rekomendasiKesenjangan pemahaman terlihat ketika informan ditanya tentang pelacakan lintas aplikasi atau lintas perangkat. Banyak informan berasumsi bahwa data hanya dipakai "di dalam aplikasi itu saja", sehingga tidak sepenuhnya menyadari bahwa data dapat digunakan untuk tujuan personalisasi yang lebih luas. Di sisi lain, sebagian informan mengakui kebingungan: mereka merasa sudah mengatur privasi (misalnya mengunci akun atau membatasi audiens), tetapi iklan yang sangat relevan tetap muncul, sehingga menimbulkan persepsi bahwa kontrol pengguna tidak selalu berdampak pada proses personalisasi.

Secara keseluruhan, temuan pada poin ini menunjukkan bahwa kesadaran privasi informan sudah ada pada level pengenalan jejak digital dan personalisasi, tetapi masih lemah pada pemahaman yang lebih teknis dan struktural, seperti jenis data yang lebih luas, mekanisme pemrosesan, serta batas efektivitas pengaturan privasi. Hasil ini menjadi dasar untuk melihat poin berikutnya, yaitu bagaimana kesadaran dan pemahaman tersebut diterjemahkan (atau tidak diterjemahkan) menjadi praktik kontrol privasi yang nyata dalam penggunaan Facebook dan Instagram.Praktik kontrol privasi yang paling sering dilakukan informan adalah pengaturan visibilitas akun, terutama keputusan untuk mengunci akun atau membatasi akses profil. Pada Instagram, mayoritas informan menyatakan memilih akun private sebagai langkah awal yang dianggap paling efektif untuk mengontrol siapa yang dapat melihat konten. Pada Facebook, pola kontrol lebih beragam: sebagian informan mengatur "teman saja", namun cukup banyak yang tetap menggunakan pengaturan default dan hanya mengandalkan seleksi pertemanan sebagai pengendali utama.Pada level konten, informan cenderung melakukan kontrol audiens secara selektif dan situasional. Konten yang dianggap pribadi atau sensitif lebih sering dibatasi, misalnya melalui pengaturan audiens tertentu di Facebook atau penggunaan Close Friends pada Story Instagram. Sebaliknya, untuk konten yang dianggap umum, informan lebih sering membiarkan pengaturan default. Pola ini menunjukkan bahwa kontrol privasi lebih didorong oleh penilaian subjektif terhadap "seberapa pribadi kontennya" daripada pemahaman menyeluruh tentang potensi jejak data yang tetap terbentuk dari interaksi.Pembatasan interaksi seperti pengaturan komentar dan DM lebih banyak dilakukan secara reaktif.

Di Instagram, informan lebih familiar dengan fitur pembatasan DM (message request) dan penyaringan komentar, sehingga beberapa informan melaporkan menerapkan pembatasan ketika merasa terganggu oleh spam atau pesan tidak dikenal. Di Facebook, praktik pembatasan komentar relatif jarang disebutkan; informan lebih sering memilih menghapus komentar tertentu, memblokir akun yang mengganggu, atau meninggalkan grup/komunitas yang dirasa tidak nyaman. Hal ini mengindikasikan bahwa kontrol privasi sering ditempuh lewat tindakan cepat untuk merespons gangguan, bukan lewat pengaturan pencegahan yang konsisten.Pada aspek pengelolaan pertemanan/pengikut, pengguna Instagram cenderung lebih selektif sejak awal, misalnya hanya menerima follower yang dikenal atau yang profilnya dianggap meyakinkan. Di Facebook, seleksi pertemanan lebih longgar pada sebagian informan karena alasan jejaring sosial yang lebih luas, kebutuhan komunitas, atau relasi kerja, sehingga verifikasi akun sering dilakukan setelah menerima permintaan. Akibatnya, beberapa informan menyebut perlunya "bersih-bersih" friend list atau follower setelah muncul rasa tidak nyaman. Praktik ini memperlihatkan adanya perbedaan budaya penggunaan antara dua platform yang memengaruhi kontrol privasi.

Secara keseluruhan, temuan pada poin ini menunjukkan bahwa kontrol privasi yang dilakukan pengguna cenderung berfokus pada pengaturan yang paling mudah dipahami (private account, close friends, seleksi follower/teman) dan sering bersifat situasional. Praktik penguatan keamanan akun serta kontrol yang lebih spesifik seperti pengelolaan tag, mention, dan pengaturan lanjutan masih belum menjadi kebiasaan rutin, dan lebih sering muncul setelah pengguna mengalami gangguan atau insiden. Temuan ini menjadi pengantar untuk poin berikutnya mengenai titik paparan data yang paling sering terjadi dalam penggunaan Facebook dan Instagram.Titik paparan data yang paling sering muncul pada informan berkaitan dengan fitur yang dianggap "normal" dalam penggunaan sehari-hari, seperti lokasi, tag, DM, serta keterlibatan dalam komunitas. Banyak informan menyebut bahwa mereka tidak selalu menganggap fitur-fitur tersebut sebagai sumber risiko, melainkan sebagai bagian dari kebiasaan bermedia sosial. Paparan data sering terjadi bukan karena pengguna sengaja membagikan informasi sensitif, tetapi karena metadata, interaksi, dan keterhubungan fitur menciptakan jejak yang dapat dibaca atau dimanfaatkan oleh pihak lain.

Pada aspek lokasi dan metadata, informan menunjukkan variasi perilaku. Sebagian informan menghindari menyalakan lokasi karena khawatir aktivitasnya mudah dipantau, namun ada juga yang tetap menggunakan geotag untuk kebutuhan tertentu seperti konten tempat wisata, acara, atau promosi. Pada Instagram, geotag sering muncul dalam story atau posting sebagai bagian dari estetika dan tren, sehingga paparan lokasi bisa terjadi tanpa disadari sebagai risiko. Di Facebook, paparan lokasi lebih sering muncul melalui check-in atau unggahan di grup lokal, yang berpotensi mengungkap pola mobilitas pengguna jika dilakukan berulang.Tag, mention, dan sebar ulang menjadi titik paparan yang sering dianggap sepele tetapi memiliki dampak besar. Informan menjelaskan bahwa ketika mereka ditandai oleh orang lain atau konten mereka dibagikan kembali, kontrol audiens bisa berubah. Pada Instagram, fitur mention dan tag di story sering memperluas jangkauan konten, terutama ketika pengguna menandai akun populer atau komunitas. Pada Facebook, tag di foto, postingan teman, atau percakapan grup dapat membuat identitas dan aktivitas pengguna lebih terlihat oleh anggota lain. Beberapa informan menganggap bahwa risiko utama bukan pada unggahan awal, tetapi pada penyebaran ulang yang tidak dapat mereka kendalikan sepenuhnya.

DM dan pesan tidak dikenal juga sering disebut sebagai titik rawan, khususnya ketika informan menerima pesan berisi tautan, permintaan data, atau ajakan bergabung ke grup tertentu. Pada Facebook, Messenger kerap menjadi saluran spam atau undangan grup yang tidak jelas, sedangkan pada Instagram titik rawannya banyak muncul melalui message request dari akun yang tidak dikenal. Informan menilai bahwa DM lebih berbahaya karena terjadi dalam konteks yang terasa privat, sehingga sebagian pengguna bisa lengah dan lebih mudah memberi respons, termasuk membuka tautan yang berpotensi phishing atau penipuan.Pada Facebook, keterlibatan dalam grup/komunitas menjadi titik paparan yang paling dominan. Informan menyatakan bahwa mereka sering membagikan opini, informasi, atau detail aktivitas di grup, namun tidak selalu menyadari bahwa anggota grup bisa sangat banyak dan heterogen. Risiko paparan meningkat ketika diskusi mengarah pada informasi personal, seperti nomor kontak, lokasi, atau jadwal kegiatan, yang

kemudian dapat disalin atau disebar. Di Instagram, pola komunitas lebih banyak terjadi melalui akun atau komentar publik, namun tetap memunculkan risiko ketika pengguna berinteraksi intens dan meninggalkan jejak minat serta preferensi yang dapat diprofilkan.

Selain itu, akun terhubung dan izin pihak ketiga menjadi titik paparan yang sering tidak disadari. Beberapa informan, terutama pengguna Facebook, mengakui pernah menggunakan login via Facebook untuk aplikasi lain tanpa mengecek izin akses. Di sisi lain, personalisasi iklan menjadi indikator yang paling kuat dirasakan informan sebagai tanda bahwa data perilaku mereka diproses secara intensif, baik di Facebook maupun Instagram. Temuan pada poin ini menunjukkan bahwa titik paparan data paling sering berasal dari fitur interaksi sosial dan kenyamanan penggunaan, sehingga mitigasinya perlu diarahkan pada penguatan kontrol dan kebiasaan penggunaan yang lebih aman.

1. **Kesadaran Privasi dan Fenomena Privacy Paradox pada Pengguna Facebook–Instagram**

Temuan pada penelitian ini menguatkan bahwa kesadaran privasi pengguna Facebook–Instagram sudah terbentuk, tetapi belum selalu berubah menjadi perilaku protektif yang konsisten. Pola "tahu ada pengumpulan data" namun tetap aktif berinteraksi selaras dengan gambaran bahwa kesadaran keamanan informasi dan privasi dapat terukur, namun penerapannya pada tindakan sehari-hari sering masih minimal, misalnya tetap memakai pengaturan default atau hanya melakukan kontrol yang paling sederhana (Gunawan, 2021).Secara perilaku, kondisi ini dapat dijelaskan melalui dorongan pengungkapan diri yang dipengaruhi kebutuhan sosial dan kenyamanan relasi. Dalam konteks remaja/pengguna muda, Rahardjo et al. (2020) menunjukkan bahwa persepsi risiko privasi hadir bersamaan dengan motivasi lain seperti kemudahan menjaga relasi dan kebutuhan presentasi diri, sehingga keterbukaan di media sosial tetap terjadi walau risiko disadari. Dengan demikian, privacy paradox muncul bukan karena pengguna tidak peduli, melainkan karena manfaat sosial terasa lebih segera dibanding risiko yang dianggap jauh atau abstrak.Hasil penelitian ini juga sejalan dengan literatur yang menegaskan bahwa keputusan berbagi data pribadi merupakan kombinasi faktor, bukan semata tingkat kekhawatiran. Fauzia et al. (2024) menekankan bahwa perilaku berbagi informasi pribadi di media sosial dipengaruhi oleh faktor-faktor yang saling terkait seperti kesadaran risiko dan konteks berbagi. Temuan lapangan memperlihatkan bahwa pengguna dapat mengeluhkan iklan yang "terlalu sesuai" sebagai sinyal pemrosesan data, namun aktivitas interaksi tetap berjalan karena platform memberi imbalan instan berupa hiburan, koneksi, dan informasi.

Pada pengguna Instagram, bentuk kontrol privasi yang tampak seperti akun privat, close friends, dan pembatasan audiens story dapat dipahami sebagai praktik manajemen batas yang selektif. Sriwahyuni dan Seprina (2024) menjelaskan bahwa manajemen privasi komunikasi pada Generasi Z di Instagram sering diwujudkan melalui pemilahan audiens dan pengaturan keterlihatan konten. Ini relevan dengan temuan penelitian bahwa kontrol paling rutin dilakukan pada aspek "siapa yang melihat", sementara pemahaman tentang paparan data dari metadata, tag, atau mekanisme personalisasi sistem masih cenderung lemah, sehingga paradoks privasi tetap mungkin terjadi walaupun pengguna merasa sudah aman.Implikasi pentingnya, privacy paradox perlu dipahami sebagai masalah literasi dan strategi pencegahan, bukan semata kesalahan pengguna. Ikhtiara (2019) menekankan pentingnya pencegahan pelanggaran privasi di media sosial melalui peningkatan kewaspadaan dan sosialisasi risiko. Dalam konteks penelitian ini, rekomendasi praktis yang logis adalah edukasi privasi berbasis contoh konkret seperti tag/mention, DM mencurigakan, izin aplikasi pihak ketiga, dan penggunaan lokasi, disertai panduan pengaturan yang sederhana dan mudah diikuti agar kesadaran privasi dapat berubah menjadi perilaku protektif yang stabil. Temuan ini juga dapat dijelaskan melalui konteks pengambilan keputusan yang sangat situasional. Pengguna tidak selalu membuat keputusan privasi melalui pertimbangan rasional yang panjang, tetapi melalui penilaian cepat berdasarkan konteks: siapa audiensnya, seberapa pribadi kontennya, dan seberapa besar dorongan sosial saat itu. Ketika konten dianggap "umum", kontrol privasi cenderung diabaikan; ketika konten dianggap "pribadi", kontrol meningkat. Pola keputusan berbagi yang kontekstual ini selaras dengan argumentasi bahwa perilaku berbagi informasi pribadi dipengaruhi banyak faktor yang saling terkait dan sering tidak disadari pengguna saat berinteraksi (Fauzia et al., 2024).

Implikasinya, intervensi yang hanya menekankan "jangan membagikan data" akan kurang efektif, karena perilaku berbagi ditopang oleh situasi, kebiasaan, dan dinamika sosial yang berulang.
Pada Instagram, strategi manajemen batas seperti akun privat dan close friends menunjukkan adanya upaya membangun rasa aman melalui pemilahan audiens. Namun, interpretasi mendalam dari temuan ini adalah bahwa pengguna sering menyamakan "privasi" dengan "keterlihatan konten", padahal privasi digital juga mencakup jejak perilaku, metadata, dan pemrosesan data untuk personalisasi. Manajemen privasi komunikasi yang menekankan pemilahan audiens memang membantu mengurangi paparan langsung, tetapi tidak otomatis mengurangi paparan tidak langsung yang berasal dari engagement, tag, atau rekomendasi sistem (Sriwahyuni & Seprina, 2024). Ini menjelaskan mengapa sebagian pengguna merasa sudah aman tetapi tetap tidak nyaman ketika iklan terasa terlalu personal—mereka mengendalikan audiens, tetapi tidak memahami dimensi pemrosesan data di balik layar.Secara praktis, tambahan interpretasi dari poin ini menegaskan bahwa penguatan privasi perlu bergerak dari edukasi normatif ke edukasi berbasis keterampilan (skill-based). Pencegahan pelanggaran privasi bukan hanya soal meningkatkan kewaspadaan, tetapi juga melatih pengguna mengenali pola risiko yang berulang, seperti dorongan klik cepat, normalisasi DM dari akun tak dikenal, atau kebiasaan mengaktifkan lokasi tanpa sadar (Ikhtiara, 2019). Dengan demikian, rekomendasi yang lebih tajam adalah membangun literasi privasi yang menekankan skenario dan tindakan: apa yang harus dicek sebelum posting, kapan perlu membatasi tag/mention, bagaimana membaca tanda-tanda phishing, dan bagaimana memahami hubungan antara aktivitas interaksi dan personalisasi. Jika kesadaran pengguna diarahkan pada praktik yang terstruktur, paradoks privasi berpotensi berkurang karena pengguna tidak hanya "tahu", tetapi juga "mampu bertindak" secara konsisten.

2. Efektivitas Kontrol Privasi dan Pola Perilaku Protektif Pengguna

Temuan penelitian ini menunjukkan bahwa kontrol privasi yang paling sering dilakukan pengguna Facebook dan Instagram umumnya berada pada level yang "terlihat" dan mudah dipahami, seperti mengunci akun, membatasi audiens, atau memilih fitur pemilahan teman. Pola ini sejalan dengan gagasan manajemen privasi sebagai praktik pengaturan batas yang sangat dipengaruhi konteks sosial dan kemudahan fitur, bukan semata-mata oleh pengetahuan teknis pengguna. Dalam konteks Facebook, praktik manajemen privasi pengguna dapat dipahami sebagai negosiasi terus-menerus antara kebutuhan bersosialisasi dan kebutuhan membatasi paparan data, sehingga kontrol sering bersifat situasional dan tidak selalu konsisten (Andriyani et al., 2019).
Pada Facebook, penelitian tentang manajemen privasi menunjukkan bahwa pengguna—khususnya kelompok muda—cenderung menghadapi dilema antara memperluas relasi dan menjaga keamanan informasi diri. Kondisi ini menjelaskan mengapa dalam temuan lapangan, sebagian pengguna tetap membuka akses tertentu (misalnya menerima pertemanan atau aktif di grup) meskipun sadar ada risiko, karena manfaat jejaring dan informasi dirasakan langsung. Ketika kontrol privasi dipahami sebagai bagian dari praktik sosial, maka keputusan privasi sering diambil berdasarkan "konteks pergaulan" dan kebutuhan aktual, bukan berdasar evaluasi risiko yang menyeluruh (Andriyani et al., 2019).
Pada Instagram, kontrol privasi banyak terkonsentrasi pada mekanisme pemilahan audiens, terutama melalui akun privat dan fitur "close friends". Penelitian mengenai penggunaan close friends memperlihatkan bahwa pengguna memanfaatkan fitur tersebut sebagai strategi untuk menciptakan ruang komunikasi yang dianggap lebih aman, sekaligus mempertahankan aktivitas berbagi konten tanpa harus sepenuhnya berhenti melakukan self-disclosure (Dianiya, 2021). Hal ini relevan dengan temuan penelitian ini, bahwa pengguna lebih sering mengelola "siapa yang dapat melihat" dibanding mengelola aspek paparan data yang lebih tidak kasat mata, seperti metadata, pelacakan, atau izin akses aplikasi.
Kontrol privasi yang dilakukan pengguna pada poin ini perlu diinterpretasikan sebagai bentuk "kontrol pragmatis" yang berorientasi pada kenyamanan dan keterlihatan konten. Artinya, pengguna cenderung memilih tindakan yang paling cepat dan paling mudah dipahami, seperti mengunci akun, membatasi audiens, atau memilih fitur pemilahan teman, karena efeknya langsung terasa. Namun, temuan ini juga menunjukkan bahwa kontrol tersebut lebih sering dipakai untuk mengelola citra dan akses sosial, bukan untuk mengurangi seluruh jejak data yang diproses platform. Dalam konteks

manajemen privasi di Facebook, perilaku ini dapat dimaknai sebagai upaya menegosiasikan batas antara kebutuhan bersosialisasi dan rasa aman, sehingga kontrol privasi menjadi situasional dan bergantung pada konteks relasi (Andriyani et al., 2019).Jika ditarik lebih dalam, efektivitas kontrol privasi sering "terkunci" pada desain platform yang mengarahkan pengguna pada pilihan sederhana (misalnya public vs private), sementara kontrol yang lebih spesifik bersifat tersembunyi atau memerlukan pemahaman teknis. Akibatnya, pengguna membangun persepsi bahwa privasi adalah soal siapa yang melihat konten, bukan soal bagaimana data diproses. Kondisi ini menjelaskan mengapa sebagian pengguna merasa sudah melakukan kontrol, tetapi tetap melihat iklan sangat relevan atau rekomendasi konten sangat "menempel". Perasaan ini mengindikasikan adanya ketidaksesuaian antara ekspektasi pengguna atas kontrol dan realitas pemrosesan data di platform, yang pada akhirnya menurunkan motivasi untuk mengatur lebih lanjut karena kontrol terasa tidak sepenuhnya efektif (Tania, 2023).

Meski kontrol berbasis audiens (misalnya private/close friends) membantu mengurangi risiko paparan langsung, temuan juga memperlihatkan adanya keterbatasan kontrol ketika pengguna berhadapan dengan pemrosesan data yang tetap berjalan untuk personalisasi konten dan iklan. Keterbatasan ini berkaitan erat dengan literasi privasi: pengguna dapat memahami kontrol dasar, tetapi belum tentu memahami konsekuensi data yang terkumpul dari kebiasaan interaksi. Studi literasi privasi di komunitas Facebook menunjukkan bahwa kesadaran privasi tidak otomatis berarti kemampuan mengelola privasi secara efektif; pengguna tetap dapat rentan karena tidak memahami alur izin, konfigurasi, atau konsekuensi data yang melekat pada aktivitas platform (Saufa & Yusuf, 2020). Temuan pemahaman privasi informasi pada pengguna Instagram juga mengindikasikan adanya variasi tingkat pemahaman, yang pada praktiknya memengaruhi sejauh mana pengguna mampu menerapkan kontrol privasi yang tepat (Nadiyya & Ganggi, 2024).

Dengan demikian, efektivitas kontrol privasi pengguna dapat dibaca sebagai hasil interaksi antara kemudahan fitur, literasi privasi, dan persepsi manfaat. Ketika pengguna merasa kontrolnya "tidak banyak berpengaruh" karena personalisasi iklan tetap terjadi, muncul kecenderungan pasrah atau menganggap kontrol cukup pada batas audiens saja. Fenomena ini dekat dengan paradoks privasi pada konteks personalisasi iklan, ketika pengguna menyadari adanya praktik pemrosesan data tetapi tetap menerima atau menormalisasi kondisi tersebut demi kenyamanan penggunaan dan relevansi konten (Tania, 2023). Oleh karena itu, pembahasan ini menegaskan bahwa peningkatan efektivitas kontrol privasi perlu diarahkan pada dua sisi sekaligus: penyederhanaan kontrol yang bermakna di platform dan penguatan literasi privasi yang fokus pada tindakan praktis, bukan hanya peningkatan kesadaran.

3. Titik Paparan Data Dominan dan Risiko dari Fitur Interaksi Sosial

Titik paparan data yang paling sering muncul dalam temuan penelitian ini berasal dari fitur interaksi sosial yang dianggap wajar oleh pengguna, seperti tag/mention, berbagi konten, aktivitas dalam komunitas, serta komunikasi melalui pesan langsung. Kondisi ini memperlihatkan bahwa risiko privasi tidak selalu muncul karena pengguna sengaja membagikan informasi sensitif, melainkan karena jejak interaksi dan metadata yang melekat pada aktivitas sosial memperluas keterlihatan informasi. Pola ini selaras dengan temuan bahwa kesadaran privasi memang dapat terukur, tetapi paparan sering tetap terjadi karena pengguna tidak mengaitkan aktivitas rutin (misalnya berinteraksi atau berbagi) dengan konsekuensi privasi yang lebih luas (Gunawan, 2021).Dalam konteks Facebook, aktivitas di grup dan jejaring sosial memperbesar peluang paparan karena informasi yang dibagikan menjadi dapat diakses oleh anggota yang beragam. Manajemen privasi pada pengguna Facebook menunjukkan bahwa batas privasi sering dinegosiasikan dalam relasi sosial dan komunitas, sehingga kontrol tidak selalu stabil dan bergantung pada situasi (Andriyani et al., 2019). Hal ini menjelaskan temuan lapangan bahwa pengguna dapat merasa aman karena "sudah teman" atau "satu komunitas", padahal heterogenitas anggota dan kultur berbagi ulang konten membuat informasi mudah berpindah dari ruang semi-privat ke ruang yang lebih terbuka.

Pada Instagram, titik paparan dominan banyak terkait praktik presentasi diri dan penyebaran konten visual, terutama melalui story, tag, dan mention. Pengguna memanfaatkan close friends sebagai cara membatasi audiens, tetapi praktik ini lebih berfokus pada keterlihatan konten daripada pengendalian jejak data yang terbentuk dari interaksi dan engagement. Studi tentang penggunaan close friends

menegaskan bahwa pemilahan audiens menjadi strategi utama untuk menjaga rasa aman saat tetap melakukan pengungkapan diri, namun tidak selalu mengurangi paparan data yang terjadi melalui mekanisme lain di platform (Dianiya, 2021). Kondisi ini selaras dengan temuan penelitian bahwa paparan sering muncul bukan pada unggahan awal, melainkan pada penyebaran ulang, tag, atau interaksi yang memperluas jangkauan konten.Selain faktor fitur, titik paparan data juga dipengaruhi oleh dorongan self-disclosure yang berhubungan dengan kebutuhan relasi, kenyamanan sosial, dan presentasi diri. Rahardjo et al. (2020) menunjukkan bahwa meskipun pengguna memiliki persepsi risiko privasi, motivasi untuk mempertahankan hubungan dan menampilkan diri tetap mendorong keterbukaan di media sosial. Ini membantu menjelaskan mengapa pengguna tetap aktif berbagi atau merespons interaksi sosial (termasuk melalui DM atau komunitas), sehingga risiko paparan data meningkat pada kanal yang terasa "lebih privat" tetapi sebenarnya tetap menyimpan jejak dan potensi penyalahgunaan.

Titik paparan juga menguat ketika kontrol privasi pengguna lebih banyak berhenti pada kontrol audiens dan tidak disertai pemahaman alur data yang lebih luas, misalnya terkait pemrosesan untuk personalisasi iklan dan rekomendasi. Studi tentang paradoks privasi dalam personalisasi iklan menegaskan bahwa pengguna dapat menyadari adanya pemrosesan data, namun tetap menormalisasi kondisi tersebut karena kenyamanan dan relevansi konten, sehingga titik paparan dari sistem rekomendasi terus berulang tanpa perubahan perilaku signifikan (Tania, 2023). Sejalan dengan itu, studi tentang perilaku berbagi informasi pribadi menunjukkan bahwa keputusan berbagi dipengaruhi oleh banyak faktor kontekstual, sehingga mitigasi perlu menargetkan titik paparan dominan (tag/mention, DM, komunitas, izin akses) dengan edukasi praktis dan kontrol yang mudah diterapkan (Fauzia et al., 2024).

4. Hambatan Literasi Privasi serta Kompleksitas Pengaturan sebagai Penyebab Risiko Berulang

Hambatan paling mendasar yang menjelaskan mengapa risiko privasi terus berulang adalah lemahnya literasi privasi yang tidak hanya terkait "tahu atau tidak tahu", tetapi juga kemampuan menafsirkan konsekuensi saat data dibagikan dan diproses di lingkungan digital. Putra dan Hidayatullah (2020) menegaskan bahwa literasi privasi diperlukan agar pengguna mampu memahami bagaimana informasi dilacak, digunakan, dan berpotensi kehilangan sifat privatnya ketika berada di ruang jaringan. Dalam temuan penelitian ini, situasi tersebut tampak ketika pengguna merasa sudah "cukup aman" dengan kontrol sederhana, padahal paparan data tetap terjadi melalui pola interaksi, metadata, dan mekanisme platform yang tidak selalu terlihat.

Kompleksitas pengaturan privasi memperkuat masalah literasi tersebut. Ketika menu privasi berlapis dan istilah teknis tidak mudah dipahami, pengguna cenderung memilih strategi paling praktis: mempertahankan pengaturan default, melakukan perubahan parsial, atau hanya mengandalkan seleksi pertemanan/pengikut. Dalam konteks Generasi Z, Aji et al. (2022) menunjukkan bahwa manajemen privasi berhadapan dengan realitas komersialisasi data pribadi di media sosial, sehingga pengguna sering berada pada posisi "mengatur sebisanya" sambil tetap mengejar manfaat platform. Ini relevan dengan temuan penelitian bahwa hambatan bukan sekadar kurangnya niat, melainkan adanya trade-off antara kenyamanan penggunaan dan upaya pengamanan yang terasa memakan waktu.

Hambatan berikutnya muncul dari relasi sosial yang membentuk cara pengguna memaknai privasi, khususnya pada ruang pertemanan dan komunitas. Hidayati dan Irwansyah (2021) menekankan bahwa privasi pertemanan remaja di media sosial berkaitan erat dengan bagaimana batas informasi dinegosiasikan dalam hubungan sosial. Dalam temuan penelitian ini, pengguna cenderung menurunkan kewaspadaan ketika berinteraksi dengan "teman" atau "komunitas", sehingga informasi yang terlihat biasa (misalnya aktivitas harian, lokasi, atau preferensi) dapat menjadi sumber paparan ketika disalin, disebar ulang, atau dikonsumsi oleh anggota yang sebenarnya tidak homogen.

Selain itu, hambatan pengelolaan privasi juga dipengaruhi kebiasaan komunikasi berbasis aplikasi pesan yang memberi rasa aman semu. Anggara dan Firmansyah (2021) menunjukkan bahwa manajemen privasi komunikasi di WhatsApp dapat berhubungan dengan pembentukan konsep diri, yang mengindikasikan bahwa pilihan privasi sering melekat pada kebutuhan mengekspresikan diri dan mengelola relasi. Pola serupa terlihat pada temuan penelitian ini ketika pengguna lebih percaya

pada ruang-ruang yang terasa privat (DM/pesan langsung), padahal kanal tersebut justru sering menjadi titik rawan untuk link mencurigakan, permintaan data, atau manipulasi sosial yang berujung pada kebocoran informasi.

Pada Instagram, strategi "pembatasan audiens" seperti close friends tampak menjadi solusi populer, namun juga mencerminkan batas dari kemampuan kontrol pengguna. Azzahra et al. (2022) menunjukkan bahwa penggunaan fitur close friends mendorong rasa nyaman untuk mengekspresikan diri karena audiens dianggap lebih aman dan dikenal. Temuan penelitian ini menguatkan bahwa strategi tersebut efektif untuk mengurangi paparan pada level keterlihatan konten, tetapi tidak otomatis menutup risiko dari tag/mention, penyebaran ulang, maupun jejak data yang terbentuk dari engagement. Dengan demikian, hambatan literasi privasi dan kompleksitas pengaturan tidak hanya menciptakan kontrol yang parsial, tetapi juga memelihara keyakinan bahwa kontrol audiens sudah cukup—padahal risiko berulang justru sering muncul dari area yang tidak dikontrol secara rutin.

KESIMPULAN

Kesimpulan penelitian ini menunjukkan bahwa pengguna Facebook dan Instagram umumnya telah memiliki kesadaran privasi pada level dasar, terutama terkait jejak digital dan personalisasi konten/iklan. Namun, kesadaran tersebut belum sepenuhnya terkonversi menjadi perilaku protektif yang konsisten. Kontrol privasi yang dominan dilakukan pengguna cenderung bersifat pragmatis dan berfokus pada keterlihatan konten, seperti mengunci akun, membatasi audiens, atau menggunakan fitur pemilahan teman, sementara kontrol yang lebih teknis (misalnya pengelolaan izin, evaluasi aplikasi terhubung, dan penguatan keamanan akun) masih jarang menjadi kebiasaan rutin.

Titik paparan data yang paling sering terjadi justru muncul dari fitur interaksi sosial yang dianggap normal, seperti aktivitas di grup/komunitas (lebih kuat pada Facebook), tag/mention dan penyebaran ulang konten (lebih kuat pada Instagram), serta komunikasi melalui pesan langsung yang sering menjadi kanal rawan phishing atau manipulasi sosial. Temuan ini menegaskan bahwa risiko privasi tidak hanya ditentukan oleh apa yang dibagikan secara sadar, tetapi juga oleh jejak perilaku, metadata, dan pola interaksi yang terbentuk secara kumulatif ketika pengguna aktif bermedia sosial.Hambatan utama yang membuat risiko berulang adalah literasi privasi yang masih terbatas dan kompleksitas pengaturan privasi yang dianggap rumit serta tidak selalu dipahami efeknya. Pengguna kerap merasa telah aman ketika mampu mengendalikan audiens, tetapi tetap mengalami ketidaknyamanan karena personalisasi sistem dan potensi perpindahan konten di luar kendali (misalnya repost, tangkapan layar, atau tag pihak lain). Oleh karena itu, penguatan privasi perlu diarahkan pada literasi berbasis keterampilan dan skenario nyata, bukan hanya peningkatan kesadaran, serta didukung oleh penyederhanaan kontrol privasi agar lebih mudah diterapkan secara konsisten.

Secara praktis, penelitian ini menyarankan agar pengguna menerapkan langkah minimum yang terstruktur: meninjau ulang pengaturan privasi secara berkala, membatasi tag/mention dan penggunaan lokasi, memperketat DM dari akun tidak dikenal, mengecek izin aplikasi pihak ketiga, serta mengaktifkan fitur keamanan akun seperti verifikasi dua langkah. Bagi pengelola platform, temuan ini mendukung perlunya transparansi pemrosesan data yang lebih mudah dipahami, pengaturan privasi yang lebih sederhana, serta edukasi privasi yang terintegrasi di dalam aplikasi untuk membantu pengguna membangun kontrol yang bermakna.Penelitian ini memiliki keterbatasan pada ruang lingkup informan dan konteks penggunaan yang dapat berbeda antar wilayah, usia, serta tujuan pemakaian (hiburan, bisnis, komunitas). Penelitian lanjutan disarankan menggunakan cakupan informan yang lebih luas dan membandingkan segmen pengguna yang berbeda, serta mengombinasikan data kualitatif dengan pengukuran kuantitatif sederhana (misalnya skala literasi privasi atau frekuensi penggunaan fitur keamanan) untuk memperkuat generalisasi temuan.

REFERENSI

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. doi:10.1126/science.aaa1465

Aji, P. W., Utari, P., & Sudarmo. (2022). Manajemen privasi Generasi Z dalam menghadapi komersialisasi data pribadi di media sosial. *Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi), 24*(2), 103–116. doi:10.17933/iptekkom.24.2.2022.103-116

Andriyani, E., Mangun, F. K., Hendiastutjik, H. K., Saidah, M., & Hidayanto, S. (2019). Privacy management of Facebook users: A study on adolescents living in West Jakarta slums. *Jurnal Komunikasi Indonesia, 8*(3). doi:10.7454/jki.v8i3.11522

Anggara, M. Y., & Firmansyah, M. A. (2021). Manajemen privasi komunikasi melalui media sosial WhatsApp Messenger dalam membentuk konsep diri. *JOISCOM (Journal of Islamic Communication), 2*(2). doi:10.36085/joiscom.v2i2.2018

Azzahra, F., Handayani, L., & Mahdalena, V. (2022). Manajemen privasi komunikasi mahasiswa UPN Veteran Jakarta pada fitur close friend di Instagram. *Jurnal Pustaka Komunikasi, 5*(2), 318–330. doi:10.32509/pustakom.v5i2.2140

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058. doi:10.1016/j.tele.2017.04.013

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147–154. doi:10.1016/j.chb.2015.11.022

Choi, T. R., & Sung, Y. (2018). Instagram versus Snapchat: Self-expression and privacy concern on social media. *Telematics and Informatics, 35*(8), 2289–2298. doi:10.1016/j.tele.2018.09.009

Darmaningrat, E. W. T., Astuti, H. M., & Alfi, F. (2020). Information privacy concerns among Instagram users: The case of Indonesian college students. *Journal of Information Systems Engineering and Business Intelligence, 6*(2), 159–168. https://doi.org/10.20473/jisebi.6.2.159168

Dianiya, V. (2021). Management privacy dalam penggunaan fitur "close friend" di Instagram. *Jurnal Studi Komunikasi, 5*(1), 249–266. doi:10.25139/jsk.v5i1.2652

Fauzia, B. R. S., Yudokusumo, L., & Ruldeviyani, Y. (2024). Analisis faktor berbagi informasi pribadi di media sosial: Studi skala kecil. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), 13*(3), 230–238. https://doi.org/10.22146/jnteti.v13i3.9908

Gruzd, A., & Hernández-García, Á. (2018). Privacy concerns and self-disclosure in private and public uses of social media. *Cyberpsychology, Behavior, and Social Networking, 21*(7), 418–428. https://doi.org/10.1089/cyber.2017.0709

Gunawan, H. (2021). Pengukuran kesadaran keamanan informasi dan privasi dalam sosial media. *Jurnal Muara Sains, Teknologi, Kedokteran, dan Ilmu Kesehatan, 5*(1), 1–8. https://doi.org/10.24912/jmstkik.v5i1.3456

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior, 68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hidayati, F. R., & Irwansyah, I. (2021). Privasi "pertemanan" remaja di media sosial. *Jurnal Teknologi dan Sistem Informasi Bisnis, 3*(1), 78–91. doi:10.47233/jteksis.v3i1.186

Ikhtiara, R. M. (2019). Pencegahan "privacy violation" di media sosial pada kalangan remaja. *Kalijaga Journal of Communication, 1*(2), 155–164. https://doi.org/10.14421/kjc.12.05.2019

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer, 51*(8), 56–59. doi:10.1109/MC.2018.3191268

Nadiyya, A., & Ganggi, R. I. P. (2024). Pemahaman privasi informasi user Instagram pada mahasiswa S-1 Ilmu Administrasi Publik Fakultas Ilmu Sosial dan Ilmu Politik Universitas Diponegoro. *Anuva: Jurnal Kajian Budaya, Perpustakaan, dan Informasi, 8*(4), 561–574. doi:10.14710/anuva.8.4.561-574

Ostendorf, S., Müller, S. M., & Brand, M. (2020). Neglecting long-term risks: Self-disclosure on social media and its relation to individual decision-making tendencies and problematic social-networks-use. *Frontiers in Psychology, 11*, 543388.

Putra, K. A. D., & Hidayatullah, F. (2020). Literasi privasi sebagai upaya mencegah pelanggaran di era masyarakat ja

Rahardjo, W., Qomariyah, N., Hermita, M., Suhatril, R. J., Marwan, M. A., & Andriani, I. (2020). Online adolescent's self-disclosure as social media users: The role of extraversion personality, perception of privacy risk, convenience of relationship maintenance, and self-presentation. *Jurnal Psikologi, 19*(3), 219–232.

Saufa, A. F., & Yusuf, S. (2020). Literasi privasi di sosial media: Analisis kesadaran privasi pada grup Facebook Komunitas Peduli HBV (Hepatitis B Virus) di Indonesia. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan, 6*(2), 119–130. doi:10.14710/lenpust.v6i2.31407

Sriwahyuni, P., & Seprina, W. O. (2024). Manajemen privasi komunikasi pada fenomena batasan diri Generasi Z di Instagram. *Jurnal Ilmu Komunikasi UHO: Jurnal Penelitian Kajian Ilmu Komunikasi dan Informasi, 9*(4), 845–865. https://doi.org/10.52423/jikuho.v9i4.324

Tania, S. (2023). Mengeksplorasi paradoks privasi Gen-Z dalam personalisasi iklan di media digital. *Interaksi: Jurnal Ilmu Komunikasi, 12*(1), 50–65. doi:10.14710/interaksi.12.1.50-65

Van der Schyff, K., Flowerday, S., & Furnell, S. (2020). Privacy risk and the use of Facebook apps: A gender-focused vulnerability assessment. *Computers & Security, 96*, 101866. https://doi.org/10.1016/j.cose.2020.101866