E-ISSN : 2988-1986
https://ejournal.cahayailmubangsa.institute/index.php/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 10 No 8 Tahun 2026

KESADARAN KEAMANAN SIBER DALAM PERLINDUNGAN DATA PRIBADI PENGGUNA FACEBOOK DI KALANGAN GENERASI Z

Adit Nasruloh Rakasiwi[1], Joshua Dwi Putra[2], Muhammad Ari Permana[3]
[1,2,3] Program Studi Sistem Informasi, Universitas Pamulang
E-mail: adit.nasruloh@gmail.com[1], putrajoshua193@gmail.com[2]
aripermana991@gmail.com[3]

ABSTRACT

The widespread use of Facebook among Generation Z provides various benefits in communication and information sharing; however, it also increases the risk of personal data security breaches. Cybersecurity awareness plays a crucial role in protecting users' personal data, particularly for Generation Z, who are considered digital natives but do not always possess adequate digital security literacy. This study aims to explore and understand cybersecurity awareness in the protection of personal data among Generation Z Facebook users. This study employs a qualitative approach using a descriptive method. Data were collected through in-depth interviews with Generation Z informants who actively use Facebook. The collected data were analyzed through data reduction, data display, and conclusion drawing to obtain a comprehensive understanding of participants' perceptions, interpretations, and practices regarding personal data protection. Data validity was ensured through source triangulation. The findings indicate that most informants demonstrate a basic awareness of cybersecurity threats, such as account hacking, identity theft, and misuse of personal information. However, this awareness has not been fully translated into practical protective behaviors, including the effective management of privacy settings, the use of strong passwords, and the utilization of additional security features provided by Facebook. Habitual behavior, convenience, and a low perception of potential risks were identified as the main factors hindering optimal personal data protection. This study concludes that cybersecurity awareness among Generation Z Facebook users remains largely conceptual and has not been fully internalized into everyday practices. Therefore, continuous cybersecurity education and digital literacy initiatives are necessary to encourage more responsible personal data protection behaviors among Generation Z.

Keywords: cybersecurity awareness, personal data protection, Facebook, Generation Z, qualitative study

ABSTRAK

Penggunaan media sosial Facebook yang masif di kalangan Generasi Z menghadirkan berbagai kemudahan dalam berkomunikasi dan berbagi informasi, namun di sisi lain juga meningkatkan risiko terhadap keamanan dan penyalahgunaan data pribadi. Kesadaran

Article History
Received: Januari 2026
Reviewed: Januari 2026
Published: Januari 2026

Plagiarism Checker No 235
Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

keamanan siber menjadi aspek penting dalam melindungi data pribadi pengguna, terutama bagi Generasi Z yang tergolong sebagai digital native tetapi tidak selalu memiliki literasi keamanan digital yang memadai. Penelitian ini bertujuan untuk menggali dan memahami kesadaran keamanan siber dalam perlindungan data pribadi pengguna Facebook di kalangan Generasi Z. Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif. Teknik pengumpulan data dilakukan melalui wawancara mendalam terhadap informan Generasi Z yang aktif menggunakan Facebook. Data yang diperoleh dianalisis menggunakan teknik reduksi data, penyajian data, serta penarikan kesimpulan untuk memperoleh pemahaman yang komprehensif mengenai persepsi, pemaknaan, dan praktik perlindungan data pribadi yang dilakukan oleh informan. Keabsahan data dijaga melalui triangulasi sumber. Hasil penelitian menunjukkan bahwa sebagian besar informan telah memiliki kesadaran dasar mengenai ancaman keamanan siber, seperti risiko peretasan akun, pencurian identitas, dan penyalahgunaan informasi pribadi. Namun, kesadaran tersebut belum sepenuhnya diimplementasikan dalam perilaku nyata, seperti pengelolaan pengaturan privasi akun, penggunaan kata sandi yang kuat, dan pemanfaatan fitur keamanan tambahan yang disediakan oleh Facebook. Faktor kebiasaan, kenyamanan penggunaan, serta rendahnya persepsi terhadap potensi dampak risiko menjadi penghambat utama dalam penerapan perlindungan data pribadi secara optimal. Penelitian ini menyimpulkan bahwa kesadaran keamanan siber Generasi Z dalam perlindungan data pribadi pengguna Facebook masih berada pada tingkat konseptual dan belum sepenuhnya terinternalisasi dalam praktik sehari-hari. Oleh karena itu, diperlukan upaya peningkatan literasi dan edukasi keamanan siber yang berkelanjutan untuk mendorong perilaku perlindungan data pribadi yang lebih bertanggung jawab di kalangan Generasi Z.
Kata Kunci: kesadaran keamanan siber, perlindungan data pribadi, Facebook, Generasi Z, penelitian kualitatif

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam pola interaksi sosial masyarakat. Media sosial menjadi salah satu produk utama dari perkembangan tersebut yang memungkinkan individu untuk berkomunikasi, berbagi informasi, dan membangun jejaring sosial secara cepat dan luas. Salah satu platform media sosial yang masih banyak digunakan hingga saat ini adalah Facebook. Platform ini tidak hanya berfungsi sebagai sarana komunikasi, tetapi juga sebagai ruang berbagi identitas, ekspresi diri, dan aktivitas sosial secara digital. Namun, intensitas penggunaan media sosial yang tinggi juga diiringi dengan meningkatnya risiko terhadap keamanan dan penyalahgunaan data pribadi.

Data pribadi merupakan informasi yang dapat mengidentifikasi seseorang secara langsung maupun tidak langsung, seperti nama, alamat, nomor telepon, alamat *email*, foto pribadi, hingga aktivitas daring. Dalam konteks media sosial, data pribadi sering kali dibagikan secara sadar maupun tidak sadar oleh pengguna. Kondisi ini membuka peluang terjadinya berbagai ancaman keamanan siber, seperti *account hacking*, *identity theft*, *phishing*, dan penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Oleh karena itu, perlindungan data pribadi menjadi isu penting dalam era digital, terutama bagi pengguna media sosial.

Generasi Z merupakan kelompok generasi yang lahir dan tumbuh di tengah pesatnya perkembangan teknologi digital. Generasi ini sering disebut sebagai *digital natives* karena terbiasa menggunakan perangkat digital dan internet sejak usia dini. Meskipun memiliki kemampuan adaptasi teknologi yang tinggi, Generasi Z tidak selalu memiliki tingkat kesadaran keamanan siber yang memadai. Kemudahan akses, kebiasaan berbagi informasi, serta persepsi bahwa risiko keamanan siber jarang terjadi sering kali menyebabkan Generasi Z mengabaikan aspek perlindungan data pribadi dalam penggunaan media sosial.

Kesadaran keamanan siber (*cybersecurity awareness*) merujuk pada pemahaman, sikap, dan perilaku individu dalam mengenali serta mengantisipasi berbagai ancaman di ruang digital. Kesadaran ini mencakup pengetahuan mengenai risiko keamanan, kemampuan mengelola pengaturan privasi, penggunaan kata sandi yang kuat, serta pemanfaatan fitur keamanan tambahan yang disediakan oleh platform digital. Tingkat kesadaran keamanan siber yang rendah dapat meningkatkan kerentanan pengguna terhadap pelanggaran data pribadi dan kejahatan siber.

Facebook sebagai platform media sosial menyediakan berbagai fitur perlindungan, seperti pengaturan privasi akun, autentikasi dua faktor (*two-factor authentication*), serta kontrol terhadap informasi yang dibagikan. Namun, efektivitas fitur-fitur tersebut sangat bergantung pada kesadaran dan perilaku pengguna dalam menggunakannya. Tanpa pemahaman dan kesadaran yang memadai, keberadaan fitur keamanan tidak secara otomatis menjamin perlindungan data pribadi pengguna.

Sejumlah penelitian sebelumnya menunjukkan bahwa rendahnya literasi keamanan digital menjadi salah satu faktor utama penyebab terjadinya pelanggaran data pribadi di kalangan generasi muda. Edukasi dan peningkatan kesadaran keamanan siber dinilai penting untuk membangun budaya digital yang aman dan bertanggung jawab. Penelitian yang dilakukan oleh Aksayeth et al. (2025) serta Nardiono dan Fuadi (2025) menegaskan bahwa kesadaran keamanan data pribadi pada generasi muda masih perlu ditingkatkan melalui edukasi yang berkelanjutan dan kontekstual, terutama dalam penggunaan media sosial.

Berdasarkan latar belakang tersebut, penelitian ini penting untuk dilakukan guna menggali secara mendalam bagaimana kesadaran keamanan siber dalam perlindungan data pribadi pengguna Facebook di kalangan Generasi Z. Pendekatan kualitatif dipilih untuk memahami secara komprehensif persepsi, pemaknaan, dan pengalaman Generasi Z dalam menghadapi risiko keamanan siber. Hasil penelitian ini diharapkan dapat memberikan kontribusi teoretis dalam kajian keamanan siber serta menjadi bahan pertimbangan praktis bagi upaya peningkatan literasi dan edukasi keamanan digital di kalangan generasi muda.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan **kualitatif** dengan metode **deskriptif kualitatif**. Pendekatan kualitatif dipilih untuk memperoleh pemahaman yang mendalam mengenai kesadaran keamanan siber dalam perlindungan data pribadi pengguna Facebook di kalangan Generasi Z. Metode deskriptif digunakan untuk menggambarkan secara sistematis persepsi, pemaknaan, serta pengalaman subjek penelitian terkait praktik perlindungan data pribadi dalam penggunaan media sosial.

2.1 Subjek dan Objek Penelitian

Subjek penelitian adalah Generasi Z yang aktif menggunakan Facebook. Generasi Z dalam penelitian ini dibatasi pada individu yang berusia 18–25 tahun. Objek penelitian adalah kesadaran keamanan siber (*cybersecurity awareness*) dalam perlindungan data pribadi (*personal data protection*) pengguna Facebook.

2.2 Kriteria Informan

Pemilihan informan dilakukan secara *purposive sampling*, dengan kriteria sebagai berikut:

1. Berusia antara 18–25 tahun dan termasuk dalam kategori Generasi Z.
2. Memiliki akun Facebook yang aktif digunakan.
3. Pernah melakukan aktivitas berbagi informasi pribadi di Facebook.
4. Bersedia menjadi informan dan memberikan data secara terbuka melalui wawancara.

Jumlah informan ditentukan berdasarkan prinsip *data saturation*, yaitu proses pengumpulan data dihentikan ketika informasi yang diperoleh telah berulang dan tidak ditemukan temuan baru yang signifikan.

2.3 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini meliputi:

1. Wawancara Mendalam

   Wawancara dilakukan secara semi-terstruktur untuk menggali persepsi, pengalaman, dan pemahaman informan terkait keamanan siber dan perlindungan data pribadi di Facebook. Panduan wawancara disusun secara fleksibel agar memungkinkan eksplorasi mendalam terhadap jawaban informan.
2. Observasi

   Observasi dilakukan secara terbatas terhadap perilaku penggunaan Facebook, khususnya terkait pengaturan privasi dan kebiasaan berbagi informasi pribadi, untuk mendukung data hasil wawancara.
3. Dokumentasi

   Dokumentasi digunakan sebagai data pendukung berupa catatan wawancara, tangkapan layar (*screenshot*) pengaturan privasi akun (dengan persetujuan informan), serta dokumen pendukung lainnya yang relevan dengan penelitian.

2.4 Teknik Analisis Data

Analisis data dilakukan secara kualitatif dengan mengacu pada model analisis interaktif yang meliputi:

1. Reduksi Data

   Proses pemilihan, pemusatan perhatian, dan penyederhanaan data mentah yang diperoleh dari wawancara, observasi, dan dokumentasi.
2. Penyajian Data

   Data yang telah direduksi disajikan dalam bentuk narasi deskriptif untuk memudahkan pemahaman pola dan hubungan antar data.
3. Penarikan Kesimpulan dan Verifikasi

   Kesimpulan ditarik berdasarkan temuan yang konsisten dan diverifikasi secara berulang selama proses penelitian berlangsung.

2.5 Keabsahan Data

Keabsahan data dijaga melalui teknik triangulasi sumber, yaitu membandingkan data yang diperoleh dari wawancara, observasi, dan dokumentasi. Selain itu, dilakukan *member checking* dengan mengonfirmasi kembali hasil wawancara kepada informan untuk memastikan kesesuaian antara data yang diperoleh dan maksud informan.

3. HASIL DAN PEMBAHASAN

3.1 Pemahaman Generasi Z terhadap Keamanan Siber dan Data Pribadi

Berdasarkan hasil wawancara mendalam, pemahaman Generasi Z terhadap keamanan siber dan data pribadi menunjukkan variasi tingkat pengetahuan yang cukup beragam. Secara umum, informan memahami keamanan siber sebagai upaya untuk melindungi akun dan informasi pribadi dari akses pihak lain yang tidak berwenang. Pemahaman ini muncul dari pengalaman penggunaan media sosial sehari-hari serta paparan informasi melalui media daring dan pemberitaan mengenai kasus kebocoran data.

Sebagian besar informan mengartikan data pribadi sebagai informasi identitas yang bersifat personal, seperti nama lengkap, foto pribadi, nomor telepon, alamat *email*, tanggal lahir, dan lokasi tempat tinggal. Informan juga menyebutkan aktivitas digital seperti riwayat unggahan, komentar, dan *likes* sebagai bagian dari jejak digital yang perlu dijaga. Namun, pemahaman mengenai data pribadi yang bersifat sensitif, seperti metadata akun, riwayat aktivitas daring, serta data yang dikumpulkan oleh pihak ketiga melalui aplikasi terhubung (*third-party applications*), masih tergolong rendah.

Dalam memahami keamanan siber, sebagian informan cenderung memusatkan perhatian pada ancaman yang bersifat langsung dan kasat mata, terutama pembajakan akun (*account hacking*). Ancaman lain seperti *phishing*, *social engineering*, *identity theft*, dan penyalahgunaan data untuk kepentingan komersial belum sepenuhnya dipahami secara komprehensif. Hal ini menunjukkan bahwa pemahaman Generasi Z terhadap keamanan siber masih terbatas pada pengalaman personal dan belum mencakup dimensi risiko yang lebih luas.

Selain itu, penelitian ini menemukan bahwa sebagian informan memiliki pemahaman normatif mengenai pentingnya menjaga privasi, namun belum disertai dengan pengetahuan teknis yang memadai. Misalnya, informan mengetahui bahwa penggunaan kata sandi yang kuat penting untuk keamanan akun, tetapi tidak memahami prinsip pembuatan kata sandi yang aman, seperti kombinasi huruf, angka, dan simbol, serta pentingnya pembaruan kata sandi secara berkala. Hal serupa juga terlihat pada pemahaman mengenai fitur autentikasi dua faktor (*two-factor authentication*), yang dikenal oleh sebagian informan, namun jarang digunakan karena dianggap merepotkan.

Pemahaman Generasi Z terhadap keamanan siber juga dipengaruhi oleh persepsi bahwa platform media sosial telah menyediakan sistem keamanan yang cukup andal. Beberapa informan beranggapan bahwa tanggung jawab perlindungan data pribadi sepenuhnya berada pada pihak platform, sehingga pengguna tidak perlu melakukan pengaturan keamanan secara

mendalam. Persepsi ini menunjukkan adanya ketergantungan berlebihan pada sistem teknologi dan rendahnya kesadaran terhadap peran individu dalam menjaga keamanan data pribadi.

Temuan ini mengindikasikan bahwa pemahaman keamanan siber di kalangan Generasi Z masih berada pada tingkat konseptual dan parsial. Informan cenderung mengetahui istilah dan risiko secara umum, tetapi belum memiliki pemahaman yang mendalam mengenai mekanisme perlindungan data pribadi serta implikasi jangka panjang dari kebocoran data. Kondisi ini memperlihatkan adanya kesenjangan antara literasi teknologi dan literasi keamanan siber, di mana kemampuan menggunakan teknologi tidak selalu diikuti dengan kemampuan melindungi diri di ruang digital.

Dengan demikian, pemahaman Generasi Z terhadap keamanan siber dan data pribadi perlu dipandang sebagai fondasi awal yang masih memerlukan penguatan melalui edukasi yang sistematis dan berkelanjutan. Pendekatan edukatif yang menekankan pemahaman risiko nyata, praktik perlindungan data, serta tanggung jawab individu dalam menjaga privasi digital menjadi penting untuk meningkatkan kesadaran keamanan siber secara menyeluruh.

3.2 Kesadaran terhadap Risiko Keamanan Siber di Facebook

Hasil penelitian menunjukkan bahwa Generasi Z pengguna Facebook memiliki tingkat kesadaran yang cukup beragam terhadap risiko keamanan siber yang melekat pada penggunaan platform media sosial. Secara umum, informan menyadari bahwa Facebook dapat menjadi ruang yang rentan terhadap berbagai ancaman keamanan, terutama yang berkaitan dengan kebocoran dan penyalahgunaan data pribadi. Kesadaran ini umumnya terbentuk dari pengalaman pribadi, informasi yang diperoleh melalui media daring, serta pemberitaan mengenai kasus pelanggaran data yang melibatkan media sosial.

Risiko keamanan siber yang paling banyak dikenali oleh informan adalah pembajakan akun (*account hacking*). Informan memahami bahwa akun Facebook dapat diambil alih oleh pihak lain melalui teknik tertentu, seperti pencurian kata sandi atau akses tidak sah. Selain itu, beberapa informan juga menyadari risiko penyalahgunaan foto dan informasi pribadi yang diunggah ke Facebook, seperti penggunaan foto tanpa izin atau penyebaran informasi pribadi ke pihak lain.

Meskipun demikian, kesadaran terhadap risiko keamanan siber lainnya masih terbatas. Ancaman seperti *phishing*, *social engineering*, pencurian identitas (*identity theft*), serta pengumpulan data oleh aplikasi pihak ketiga (*third-party applications*) belum sepenuhnya dipahami oleh seluruh informan. Sebagian informan menganggap ancaman tersebut bersifat teknis dan hanya mungkin terjadi pada pengguna dengan tingkat aktivitas digital yang sangat

tinggi atau pada individu tertentu saja.

Penelitian ini juga menemukan bahwa kesadaran terhadap risiko keamanan siber sering kali bersifat situasional. Informan cenderung meningkatkan kewaspadaan setelah mendengar atau menyaksikan kasus kebocoran data, baik yang dialami oleh orang terdekat maupun yang diberitakan secara luas. Namun, kewaspadaan tersebut bersifat sementara dan tidak selalu diikuti dengan perubahan perilaku jangka panjang dalam penggunaan Facebook. Setelah beberapa waktu, perhatian terhadap risiko keamanan kembali menurun seiring dengan rutinitas penggunaan media sosial.

Selain itu, persepsi risiko (*risk perception*) yang rendah menjadi faktor penting yang memengaruhi tingkat kesadaran informan. Banyak informan merasa bahwa kemungkinan mereka menjadi korban pelanggaran keamanan siber relatif kecil. Pandangan ini diperkuat oleh anggapan bahwa akun mereka tidak menyimpan informasi yang dianggap penting atau bernilai tinggi. Akibatnya, informan cenderung menyepelekan risiko kebocoran data pribadi dan menganggap perlindungan keamanan sebagai hal yang tidak mendesak.

Kesadaran terhadap risiko keamanan siber di Facebook juga dipengaruhi oleh tingkat kepercayaan terhadap platform. Sebagian informan beranggapan bahwa Facebook sebagai perusahaan teknologi besar telah memiliki sistem keamanan yang kuat, sehingga risiko kebocoran data dapat diminimalkan secara otomatis. Kepercayaan yang tinggi terhadap platform ini menyebabkan informan kurang aktif dalam memanfaatkan fitur keamanan yang tersedia dan cenderung menyerahkan tanggung jawab perlindungan data kepada pihak penyedia layanan.

Temuan penelitian ini menunjukkan bahwa kesadaran Generasi Z terhadap risiko keamanan siber di Facebook belum bersifat menyeluruh dan berkelanjutan. Kesadaran yang ada masih terfokus pada risiko yang mudah dikenali dan sering diberitakan, sementara ancaman yang lebih kompleks dan bersifat tidak langsung kurang mendapatkan perhatian. Kondisi ini mengindikasikan perlunya pendekatan edukatif yang tidak hanya meningkatkan pengetahuan tentang jenis-jenis risiko keamanan siber, tetapi juga membangun pemahaman mengenai dampak jangka panjang dari kebocoran data pribadi.

Dengan demikian, kesadaran terhadap risiko keamanan siber di Facebook di kalangan Generasi Z perlu diperkuat melalui literasi digital yang menekankan pemahaman risiko secara holistik. Upaya ini penting agar Generasi Z tidak hanya menyadari adanya ancaman, tetapi juga mampu mengantisipasi dan memitigasi risiko tersebut melalui perilaku penggunaan media sosial yang lebih aman dan bertanggung jawab.

3.3 Praktik Perlindungan Data Pribadi Pengguna Facebook

Hasil penelitian menunjukkan bahwa praktik perlindungan data pribadi yang dilakukan oleh Generasi Z pengguna Facebook masih berada pada tingkat dasar dan belum diterapkan secara konsisten. Meskipun sebagian informan telah menyadari pentingnya menjaga keamanan data pribadi, kesadaran tersebut belum sepenuhnya terwujud dalam perilaku perlindungan yang komprehensif dan berkelanjutan.

Sebagian besar informan menyatakan bahwa bentuk perlindungan data pribadi yang paling umum dilakukan adalah pengaturan visibilitas unggahan, seperti membatasi siapa saja yang dapat melihat unggahan mereka menjadi *friends only*. Langkah ini dipersepsikan sebagai upaya yang cukup untuk menjaga privasi, terutama dalam membatasi akses orang yang tidak dikenal. Namun, praktik ini sering kali tidak disertai dengan evaluasi terhadap informasi pribadi lain yang tercantum dalam profil akun, seperti nomor telepon, alamat *email*, dan informasi lokasi, yang masih dibiarkan terbuka atau tidak diperbarui secara berkala.

Dalam hal pengelolaan akun, sebagian informan menggunakan kata sandi yang dianggap aman, tetapi tidak memahami sepenuhnya prinsip keamanan kata sandi (*password security*). Beberapa informan mengakui menggunakan kata sandi yang sama untuk beberapa akun media sosial atau jarang melakukan pembaruan kata sandi. Praktik ini menunjukkan adanya kerentanan terhadap risiko keamanan siber, meskipun informan merasa bahwa akun mereka relatif aman.

Pemanfaatan fitur keamanan lanjutan yang disediakan oleh Facebook, seperti autentikasi dua faktor (*two-factor authentication*), masih tergolong rendah. Sebagian informan menyatakan telah mengetahui fitur tersebut, tetapi memilih untuk tidak mengaktifkannya karena dianggap merepotkan atau mengganggu kenyamanan penggunaan. Faktor kenyamanan (*convenience*) menjadi pertimbangan utama dalam keputusan informan untuk mengabaikan fitur keamanan tambahan, meskipun mereka memahami manfaatnya dalam meningkatkan perlindungan akun.

Selain itu, penelitian ini menemukan bahwa pengelolaan izin aplikasi pihak ketiga (*third-party applications*) belum menjadi perhatian utama bagi informan. Banyak informan yang mengizinkan aplikasi lain terhubung dengan akun Facebook tanpa memahami data apa saja yang diakses dan bagaimana data tersebut digunakan. Minimnya pemahaman mengenai mekanisme pengumpulan data oleh pihak ketiga menunjukkan adanya celah dalam praktik perlindungan data pribadi yang berpotensi menimbulkan risiko keamanan.

Praktik perlindungan data pribadi juga dipengaruhi oleh kebiasaan berbagi informasi di media sosial. Informan cenderung membagikan aktivitas sehari-hari, foto, dan lokasi secara

rutin tanpa mempertimbangkan implikasi jangka panjang terhadap privasi. Kebiasaan ini menunjukkan bahwa kebutuhan akan eksistensi sosial dan interaksi digital sering kali lebih diutamakan dibandingkan pertimbangan keamanan data pribadi.

Temuan penelitian ini menunjukkan bahwa praktik perlindungan data pribadi di kalangan Generasi Z masih bersifat reaktif, yaitu dilakukan setelah muncul kekhawatiran atau pengalaman negatif terkait keamanan siber. Perlindungan yang bersifat preventif dan berkelanjutan belum menjadi bagian dari kebiasaan penggunaan Facebook. Kondisi ini menegaskan bahwa perlindungan data pribadi tidak hanya bergantung pada pengetahuan dan kesadaran, tetapi juga pada pembentukan perilaku yang konsisten dan bertanggung jawab.

Dengan demikian, praktik perlindungan data pribadi pengguna Facebook di kalangan Generasi Z masih memerlukan penguatan melalui edukasi keamanan siber yang bersifat praktis dan aplikatif. Pendekatan edukatif yang menekankan pembiasaan penggunaan fitur keamanan, pemahaman risiko nyata, serta pengelolaan informasi pribadi secara sadar diharapkan dapat meningkatkan kualitas perlindungan data pribadi secara menyeluruh.

3.4 Pembahasan

Hasil penelitian ini menunjukkan bahwa kesadaran keamanan siber di kalangan Generasi Z pengguna Facebook masih berada pada tingkat dasar dan belum sepenuhnya terinternalisasi dalam perilaku perlindungan data pribadi. Temuan ini mengindikasikan adanya kesenjangan antara pengetahuan (*knowledge*) dan tindakan (*behavior*) dalam praktik keamanan siber. Generasi Z sebagai *digital natives* memiliki kemampuan adaptasi teknologi yang tinggi, namun kemampuan tersebut tidak selalu diiringi dengan literasi keamanan digital yang memadai.

Pemahaman Generasi Z terhadap keamanan siber cenderung bersifat konseptual dan terbatas pada ancaman yang bersifat langsung, seperti pembajakan akun (*account hacking*). Ancaman yang lebih kompleks dan tidak kasat mata, seperti *phishing*, *social engineering*, serta penyalahgunaan data oleh pihak ketiga, kurang mendapat perhatian. Kondisi ini menunjukkan bahwa kesadaran keamanan siber belum mencakup pemahaman holistik mengenai ekosistem risiko digital yang melekat pada penggunaan media sosial.

Temuan ini sejalan dengan konsep *cybersecurity awareness* yang menekankan bahwa kesadaran tidak hanya mencakup pengetahuan, tetapi juga sikap dan perilaku preventif. Rendahnya pemanfaatan fitur keamanan lanjutan seperti autentikasi dua faktor (*two-factor authentication*) memperlihatkan bahwa kenyamanan penggunaan (*convenience*) sering kali lebih diprioritaskan dibandingkan aspek keamanan. Hal ini memperkuat pandangan bahwa

faktor manusia (*human factor*) menjadi elemen krusial dalam keberhasilan perlindungan data pribadi.

Selain itu, persepsi risiko (*risk perception*) yang rendah turut memengaruhi tingkat kesadaran Generasi Z terhadap keamanan siber. Banyak informan merasa bahwa kemungkinan mereka menjadi korban kejahatan siber relatif kecil, terutama karena mereka menganggap informasi yang dibagikan tidak bernilai penting. Persepsi ini berkontribusi pada sikap abai terhadap pengelolaan privasi dan keamanan akun. Padahal, dalam konteks keamanan digital, data yang tampak sepele sekalipun dapat dimanfaatkan untuk berbagai bentuk penyalahgunaan, termasuk pencurian identitas (*identity theft*).

Kepercayaan yang tinggi terhadap platform Facebook juga memengaruhi perilaku pengguna dalam melindungi data pribadi. Sebagian informan beranggapan bahwa tanggung jawab utama perlindungan data berada pada penyedia platform, bukan pada pengguna. Pandangan ini mencerminkan adanya ketergantungan berlebihan terhadap sistem teknologi dan kurangnya kesadaran akan peran individu dalam menjaga keamanan digital. Temuan ini menguatkan argumen bahwa perlindungan data pribadi merupakan tanggung jawab bersama antara penyedia layanan dan pengguna.

Dari sisi praktik, penelitian ini menunjukkan bahwa perlindungan data pribadi yang dilakukan oleh Generasi Z masih bersifat reaktif. Pengguna cenderung meningkatkan kewaspadaan setelah terpapar kasus kebocoran data, namun kewaspadaan tersebut tidak berlanjut menjadi kebiasaan jangka panjang. Hal ini menunjukkan bahwa kesadaran keamanan siber belum menjadi bagian dari budaya digital (*digital culture*) yang melekat dalam kehidupan sehari-hari Generasi Z.

Temuan penelitian ini sejalan dengan hasil penelitian Aksayeth et al. (2025), Nardiono dan Fuadi (2025), serta Janova et al. (2024) yang menegaskan pentingnya edukasi keamanan data pribadi bagi generasi muda. Edukasi yang bersifat informatif saja dinilai belum cukup untuk mendorong perubahan perilaku. Diperlukan pendekatan edukatif yang menekankan aspek praktis, kontekstual, dan berkelanjutan agar kesadaran keamanan siber dapat diterapkan secara konsisten dalam penggunaan media sosial.

Dengan demikian, pembahasan ini menegaskan bahwa kesadaran keamanan siber di kalangan Generasi Z tidak dapat dipahami hanya sebagai persoalan pengetahuan teknologi, tetapi juga sebagai persoalan sikap, kebiasaan, dan tanggung jawab individu dalam ruang digital. Upaya peningkatan kesadaran keamanan siber perlu diarahkan pada pembentukan perilaku preventif, penguatan literasi keamanan digital, serta peningkatan pemahaman mengenai risiko dan dampak jangka panjang dari kebocoran data pribadi.

KESIMPULAN

Penelitian ini menunjukkan bahwa kesadaran keamanan siber (*cybersecurity awareness*) dalam perlindungan data pribadi pengguna Facebook di kalangan Generasi Z masih berada pada tingkat dasar dan belum sepenuhnya terinternalisasi dalam perilaku penggunaan media sosial. Generasi Z memiliki pemahaman konseptual mengenai keamanan siber dan data pribadi, namun pemahaman tersebut belum secara konsisten diwujudkan dalam praktik perlindungan data pribadi yang komprehensif dan berkelanjutan.

Hasil penelitian mengungkap bahwa Generasi Z cenderung lebih menyadari risiko keamanan siber yang bersifat langsung dan kasat mata, seperti pembajakan akun (*account hacking*), dibandingkan ancaman yang bersifat kompleks dan tidak langsung, seperti *phishing*, *social engineering*, dan penyalahgunaan data oleh pihak ketiga. Rendahnya persepsi risiko (*risk perception*), tingginya orientasi pada kenyamanan penggunaan (*convenience*), serta kepercayaan berlebihan terhadap sistem keamanan platform media sosial menjadi faktor utama yang memengaruhi rendahnya penerapan perlindungan data pribadi secara optimal.

Praktik perlindungan data pribadi yang dilakukan oleh Generasi Z pengguna Facebook masih bersifat reaktif dan terbatas pada pengaturan privasi dasar. Pemanfaatan fitur keamanan lanjutan, seperti autentikasi dua faktor (*two-factor authentication*) dan pengelolaan izin aplikasi pihak ketiga, belum menjadi kebiasaan yang melekat dalam penggunaan sehari-hari. Temuan ini menegaskan bahwa perlindungan data pribadi tidak hanya bergantung pada ketersediaan teknologi, tetapi juga sangat dipengaruhi oleh faktor manusia (*human factor*).

Berdasarkan temuan tersebut, penelitian ini menyimpulkan bahwa peningkatan kesadaran keamanan siber di kalangan Generasi Z memerlukan pendekatan edukatif yang bersifat berkelanjutan, praktis, dan kontekstual. Upaya peningkatan literasi keamanan digital perlu diarahkan tidak hanya pada peningkatan pengetahuan, tetapi juga pada pembentukan sikap dan perilaku preventif dalam penggunaan media sosial. Dengan demikian, Generasi Z diharapkan mampu menjadi pengguna media sosial yang lebih bijak, aman, dan bertanggung jawab dalam melindungi data pribadi di era digital.

DAFTAR PUSTAKA

[1] Aksayeth, M. B., Yahya, H., Faga, D. A., Fahmi, D., Aliyafasya, F. M., Mustaqiim, M., Zannah, M., Rahmawati, R., Mooy, S. G., Pontoh, Y. R., & Purnama, O. A. A. (2025). Membangun kesadaran keamanan data pribadi di era digital. *APPA: Jurnal Pengabdian kepada Masyarakat, 2*(5), 523–527.

[2] Janova, B. G., dkk. (2024). Edukasi keamanan data bagi pelajar dan remaja dalam dunia digital. *APPA: Jurnal Pengabdian kepada Masyarakat*. Universitas Pamulang.

[3] Nardiono, & Fuadi, A. L. (2025). Sosialisasi keamanan siber dalam bermedia sosial pada SMK Panti Karya 3. *KOMMAS: Jurnal Pengabdian kepada Masyarakat*. Universitas Pamulang.

[4] Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

[5] Cahyono, A. S. (2016). Pengaruh media sosial terhadap perubahan sosial masyarakat di Indonesia. *Jurnal Ilmu Sosial*, 9(1), 140–157.

[6] Creswell, J. W. (2016). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

[7] Floridi, L. (2018). *Information ethics: On the philosophical foundation of computer ethics*. Oxford University Press.

[8] Kaspersky. (2021). *Cybersecurity awareness report*. Kaspersky Lab.

[9] Livingstone, S. (2019). Privacy, data protection, and children's digital rights. *Journal of Media Ethics*, 34(2), 76–89.

[10] Miles, M. B., & Huberman, A. M. (2014). *Qualitative data analysis: A methods sourcebook*. Sage Publications.

[11] NIST. (2020). *Framework for improving critical infrastructure cybersecurity*. National Institute of Standards and Technology.

[12] OECD. (2019). *Digital security risk management*. OECD Publishing.

[13] Pratama, D. (2019). Penggunaan metode interaktif dalam edukasi keamanan data pada pelajar. *Jurnal Pendidikan dan Teknologi, 7*(1), 45–59.

[14] Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon, 9*(5), 1–6.

[15] Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal HAM, 11*(2), 285–299.

[16] Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.

[17] Statista. (2022). *Facebook users statistics report*. Statista Research Department.

[18] Sugiyono. (2019). *Metode penelitian kualitatif*. Alfabeta.

[19] UNESCO. (2021). *Media and information literacy: Policy and strategy guidelines*. UNESCO Publishing.

[20] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

[21] Van Dijk, J. (2020). *The network society*. Sage Publications.

[22] We Are Social. (2022). *Digital 2022: Indonesia*. We Are Social & Hootsuite.

[23] Yin, R. K. (2018). *Case study research and applications: Design and methods*. Sage Publications.