Analisis Motivasi Gen Z Dalam Menjaga Kemanan Data Pribadi Di Media Sosial Menggunakan Protection Motivation Theory (Pmt)

Jesica Sampe Allo[1], Flourensia Sapty Rahayu[2], Generosa Lukhayu Pritalia[3], Elvania Pranisti[4], Aprillian Josua Marcelino*[5]

[1-5]Program Studi Sistem Informasi, Universitas Atma Jaya Yogyakarta

E-mail: 211711206@students.uajy.ac.id[1] , sapty.rahayu@uajy.ac.id[2], generosa.pritalia@uajy.ac.id[3], 231712660@students.uajy.ac.id[4], 231712227@students.uajy.ac.id[5]

Abstrak. Penelitian ini menganalisis motivasi Generasi Z dalam menjaga keamanan data pribadi di media sosial (Instagram dan TikTok) menggunakan Protection Motivation Theory (PMT). Permasalahan utama adalah kecenderungan Gen Z untuk oversharing dan kurangnya kesadaran privasi digital, yang meningkatkan kerentanan terhadap pencurian identitas dan penyalahgunaan data. Tujuan penelitian adalah menganalisis faktor-faktor PMT (Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy, dan Response Costs) yang memengaruhi motivasi perlindungan data pribadi Gen Z. Lima hipotesis diuji mengenai pengaruh langsung setiap faktor PMT. Metodologi yang digunakan adalah kuantitatif inferensial dengan survei daring (kuesioner) pada 100 responden Gen Z (13-28 tahun) pengguna aktif Instagram/TikTok, dipilih melalui purposive sampling. Data dianalisis dengan Structural Equation Modeling - Partial Least Squares (SEM-PLS). Hasil menunjukkan Perceived Severity, Perceived Vulnerability, dan Self-Efficacy berpengaruh positif dan signifikan terhadap motivasi perlindungan data. Namun, Response Efficacy berpengaruh negatif dan signifikan, mengindikasikan keyakinan berlebihan terhadap efektivitas tindakan perlindungan dapat menurunkan motivasi aktif. Response Costs tidak berpengaruh signifikan.

Kata kunci: generasi z, keamanan data pribadi, media sosial, *protection motivation theory*, privasi digital

Abstract. *This study analyzes Generation Z's motivation in maintaining personal data security on social media (Instagram and TikTok) using the Protection Motivation Theory (PMT). The main problem is Gen Z's tendency for oversharing and a lack of digital privacy awareness, which increases their vulnerability to identity theft and data misuse. The research aims to analyze PMT factors (Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy, and Response Costs) that influence Gen Z's personal data protection motivation. Five hypotheses were tested regarding the direct influence of each PMT factor. The methodology used is quantitative inferential with an online survey (questionnaire) on 100 Gen Z respondents (13-28 years old) active on Instagram/TikTok, selected through purposive sampling. Data were analyzed using Structural Equation Modeling - Partial Least Squares (SEM-PLS). The results show that Perceived Severity, Perceived Vulnerability, and Self-Efficacy have a positive and significant effect on data protection motivation. However, Response Efficacy has a negative and significant effect, indicating that overconfidence in the effectiveness of protection actions can decrease active motivation. Response Costs did not have a significant effect*.

Keywords: *generation z, personal data security, social media, protection motivation theory, digital privacy*.

Pendahuluan

Perkembangan teknologi digital yang sangat pesat telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, mulai dari cara berkomunikasi, bekerja, belajar, hingga membangun interaksi sosial melalui media sosial. Internet dan teknologi digital memberikan kemudahan berupa akses informasi yang luas serta komunikasi yang instan, namun di sisi lain juga memunculkan berbagai tantangan baru, khususnya terkait keamanan dan privasi data pribadi. Konsep Society 5.0 yang diperkenalkan oleh Jepang hadir sebagai pendekatan yang menekankan keseimbangan antara pemanfaatan teknologi canggih dan kesejahteraan manusia. Dalam konsep ini, teknologi seperti Artificial Intelligence (AI), Big Data, dan Internet of Things (IoT) dimanfaatkan untuk meningkatkan kualitas hidup masyarakat, termasuk melalui penggunaan platform media sosial sebagai sarana interaksi digital [1].

Media sosial merupakan sekumpulan aplikasi berbasis internet yang memungkinkan individu untuk berinteraksi, berbagi informasi, dan membangun jejaring sosial secara global. Platform seperti Facebook, TikTok, Twitter, dan Instagram saat ini menjadi media yang sangat populer di kalangan generasi muda untuk bersosialisasi dan memperoleh informasi [2]. Tingginya intensitas penggunaan media sosial turut memengaruhi perilaku pengguna dalam mengelola data pribadi. Dorongan untuk memperoleh popularitas, pengakuan sosial, atau validasi sering kali membuat pengguna membagikan informasi pribadi secara berlebihan tanpa mempertimbangkan risiko yang ada. Fenomena ini dikenal sebagai oversharing dan menjadi salah satu faktor utama meningkatnya ancaman terhadap privasi digital, seperti pencurian identitas dan penipuan daring. Selain itu, algoritma media sosial yang dirancang untuk meningkatkan keterlibatan pengguna dapat mendorong perilaku impulsif yang berpotensi membahayakan keamanan data pribadi [3].

Generasi Z merupakan kelompok yang lahir dan tumbuh di era digital, sehingga memiliki tingkat ketergantungan yang tinggi terhadap media sosial untuk berbagai keperluan, seperti berkomunikasi, mencari informasi, serta mengekspresikan identitas diri. Data menunjukkan bahwa lebih dari 92% Generasi Z aktif menggunakan media sosial, menjadikan mereka kelompok yang sangat terpapar pengaruh platform digital, baik yang bersifat positif maupun negatif [4]. Meskipun Generasi Z umumnya memiliki pengetahuan mengenai risiko keamanan data, sering kali terdapat ketidaksesuaian antara kesadaran tersebut dengan tindakan perlindungan yang dilakukan. Fenomena Fear of Missing Out (FOMO) turut memperkuat ketergantungan ini, di mana individu merasa terdorong untuk terus terhubung agar tidak tertinggal informasi atau tren terbaru di media sosial [5]. Selain itu, pengaruh media sosial juga meluas ke perilaku konsumsi Generasi Z, termasuk dalam keputusan berbelanja secara daring melalui platform seperti TikTok Shop [6].

Tingginya penggunaan media sosial membawa konsekuensi terhadap meningkatnya risiko keamanan data pribadi. Generasi Z cenderung kurang memperhatikan pengelolaan privasi digital, sehingga rentan terhadap ancaman seperti peretasan akun, pencurian identitas, serta penyalahgunaan data pribadi. Kasus kebocoran data yang terjadi di Indonesia menunjukkan bahwa perlindungan data pribadi masih menjadi isu yang serius. Penelitian sebelumnya mengungkapkan bahwa meskipun sebagian besar individu menyatakan peduli terhadap privasi, hanya sebagian kecil yang secara aktif melakukan pengaturan privasi pada akun media sosial mereka. Hal ini menunjukkan adanya kesenjangan antara kesadaran konseptual dan praktik nyata dalam melindungi privasi digital [7].

Di sisi lain, perusahaan media sosial sering mengumpulkan dan memanfaatkan data pribadi pengguna untuk kepentingan komersial, termasuk membagikannya kepada pihak ketiga tanpa pemahaman yang memadai dari pengguna. Kondisi ini semakin memperbesar risiko pelanggaran privasi. Perilaku *oversharing* pada Generasi Z juga dipengaruhi oleh minimnya pengawasan dan komunikasi dari lingkungan keluarga, sehingga batasan privasi dalam penggunaan media sosial menjadi kurang jelas. Akibatnya, Generasi Z cenderung mencari pengakuan sosial melalui media sosial dengan mengorbankan keamanan data pribadi mereka [8].

Pemahaman terhadap keamanan informasi dan privasi digital memiliki peran penting dalam membentuk perilaku perlindungan data. Pengetahuan mengenai potensi ancaman serta keyakinan individu terhadap kemampuannya dalam melindungi data pribadi dapat memengaruhi tingkat kecemasan dan motivasi dalam menjaga privasi di media sosial [9]. Salah satu pendekatan teoritis yang relevan untuk menjelaskan perilaku tersebut adalah *Protection Motivation Theory* (PMT). Teori

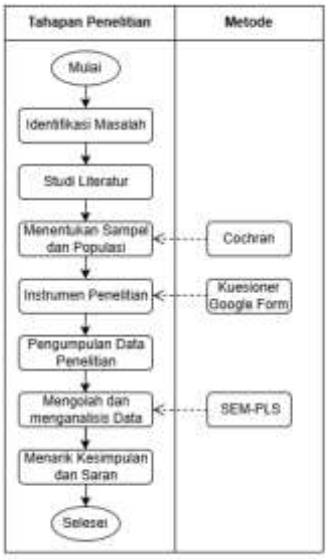
ini menjelaskan bahwa individu akan terdorong untuk melakukan tindakan perlindungan apabila mereka memandang ancaman sebagai serius, merasa rentan terhadap ancaman tersebut, serta meyakini bahwa tindakan perlindungan yang tersedia efektif dan dapat dilakukan [10].

Berdasarkan uraian tersebut, dapat disimpulkan bahwa tingginya penggunaan media sosial oleh Generasi Z memberikan manfaat sekaligus risiko terhadap keamanan data pribadi. Oleh karena itu, penelitian ini berfokus pada analisis motivasi Generasi Z dalam melindungi data pribadi di media sosial menggunakan *Protection Motivation Theory* (PMT), dengan meninjau faktor persepsi ancaman, kerentanan, efikasi respon, efikasi diri, dan biaya respon pada platform Instagram dan TikTok.

Metodologi Penelitian

2.1 Tahapan Penelitian

Penelitian ini disusun melalui beberapa tahapan yang saling berkaitan untuk memastikan proses penelitian berjalan secara sistematis dan terarah. Tahapan penelitian dimulai dari identifikasi masalah hingga analisis data menggunakan pendekatan statistik yang sesuai. Alur penelitian secara keseluruhan ditunjukkan pada Gambar 1.



Gambar 1. Tahap Penelitian

2.1.1 Identifikasi Masalah

Generasi Z dikenal sebagai kelompok yang memiliki tingkat ketergantungan tinggi terhadap media sosial dalam kehidupan sehari-hari. Namun, tingginya intensitas penggunaan tersebut tidak selalu diimbangi dengan kesadaran yang memadai terhadap risiko keamanan data pribadi. Perilaku *oversharing* serta keterbatasan pemahaman mengenai privasi digital menyebabkan Generasi Z rentan terhadap berbagai ancaman, seperti pencurian identitas dan penyalahgunaan data pribadi.

Meskipun berbagai teknologi dan fitur keamanan telah tersedia pada platform media sosial, motivasi Generasi Z dalam menerapkan langkah-langkah perlindungan data pribadi masih relatif rendah. Oleh karena itu, diperlukan kajian yang mendalam mengenai faktor-faktor yang memengaruhi motivasi Generasi Z dalam melindungi data pribadi mereka. Penelitian ini menggunakan pendekatan *Protection Motivation Theory* (PMT) untuk menganalisis bagaimana persepsi ancaman, kerentanan, serta kemampuan individu memengaruhi motivasi perlindungan data pribadi di media sosial.

2.1.2 Studi Literatur

Tahap studi literatur dilakukan untuk memperoleh landasan teoretis dan konseptual yang relevan dengan topik penelitian. Berdasarkan hasil tinjauan pustaka, *Protection Motivation Theory*

(PMT) dipilih sebagai kerangka utama dalam menganalisis motivasi Generasi Z dalam menjaga keamanan data pribadi di media sosial.

Beberapa penelitian terdahulu menunjukkan bahwa pengalaman negatif, seperti kebocoran data dan perundungan siber, dapat meningkatkan kesadaran individu terhadap pentingnya privasi digital. Namun, peningkatan kesadaran tersebut tidak selalu diikuti dengan tindakan perlindungan yang nyata. Selain itu, faktor *wishful thinking* sering kali menjadi penghambat individu dalam mengambil langkah preventif. Dalam konteks Generasi Z sebagai *digital native* dengan tingkat keterpaparan tinggi terhadap media sosial, pemahaman mengenai faktor psikologis yang memengaruhi perilaku perlindungan data menjadi sangat penting untuk diteliti lebih lanjut.

2.1.3 Penentuan Populasi dan Sampel

Populasi dalam penelitian ini didefinisikan sebagai seluruh individu yang memiliki karakteristik tertentu sesuai dengan tujuan penelitian. Populasi yang menjadi fokus penelitian ini adalah Generasi Z yang aktif menggunakan media sosial, khususnya platform Instagram dan TikTok.

Sampel penelitian merupakan bagian dari populasi yang dipilih untuk mewakili karakteristik populasi secara keseluruhan. Teknik pengambilan sampel yang digunakan adalah *purposive sampling*, yaitu metode pemilihan sampel berdasarkan kriteria tertentu yang telah ditetapkan oleh peneliti. Metode ini dipilih agar responden yang terlibat relevan dengan tujuan penelitian dan mampu memberikan data yang sesuai [22].

Kriteria responden dalam penelitian ini meliputi:
Berusia 13–28 tahun.
Aktif menggunakan media sosial dalam satu tahun terakhir.
Gen Z yang menggunakan platform Instagram atau TikTok.

Rentang usia 13–28 tahun dipilih karena berada pada fase remaja akhir hingga dewasa awal, di mana individu mulai memiliki kemandirian dalam pengambilan keputusan, termasuk dalam penggunaan media sosial dan pengelolaan privasi digital. Selain itu, kelompok usia ini merupakan pengguna aktif media sosial dengan tingkat interaksi digital yang tinggi.

Penentuan jumlah sampel dilakukan menggunakan rumus Cochran dengan tingkat kepercayaan 95% dan margin of error sebesar 10%. Berdasarkan perhitungan tersebut, diperoleh jumlah sampel minimum sebesar 96 responden. Untuk meningkatkan keandalan data, jumlah sampel kemudian dibulatkan menjadi 100 responden [23].

2.1.4 Instrumen Penelitian

Instrumen penelitian yang digunakan berupa kuesioner yang disusun berdasarkan konstruk berikut.

Tabel 1. Operasional Variabel

Variabel	Indikator
Perceived Severity	Ancaman serius terhadap data pribadi
Perceived Vulnerability	Kerentanan pengguna terhadap ancaman
Response Efficacy	Keyakinan efektivitas tindakan perlindungan
Self-Efficacy	Keyakinan individu dalam menjaga keamanan data
Response Costs	Hambatan dalam melakukan perlindungan data
Motivasi Perlindungan Data Pribadi Di Media Sosial	Niat untuk melakukan tindakan perlindungan

Tabel 2. Instrumen Penelitian

Variabel	Kode	Item Pernyataan
Perceived Severity (Seberapa serius	PS1	Saya merasa kehilangan data pribadi bisa menyebabkan masalah besar bagi saya.
	PS2	Saya takut kalau data pribadi saya bocor dan disalahgunakan.

Variabel	Kode	Item Pernyataan
ancaman terhadap data pribadi)	PS3	Saya khawatir jika orang lain bisa melihat dan memakai data pribadi saya tanpa izin.
	PS4	Saya merasa tidak nyaman jika informasi pribadi saya jatuh ke tangan orang yang tidak dikenal.
	PS5	Saya percaya bahwa pencurian data pribadi adalah masalah yang serius.
	PS6	Saya merasa ada risiko besar jika data pribadi saya tidak terlindungi dengan baik.
Perceived Vulnerability (Seberapa rentan terhadap ancaman)	PV1	Saya merasa data pribadi saya bisa dicuri kapan saja di media sosial.
	PV2	Saya sering mendengar orang mengalami pencurian data di media sosial.
	PV3	Saya merasa data pribadi saya mudah diakses oleh orang lain.
	PV4	Saya tidak yakin bahwa media sosial bisa benar-benar melindungi data saya.
	PV5	Saya kesulitan mengontrol siapa saja yang bisa melihat data pribadi saya.
	PV6	Saya sadar bahwa saya bisa menjadi korban pencurian data tanpa saya sadari.
Response Efficacy (Seberapa efektif tindakan perlindungan)	RE1	Saya percaya bahwa mengatur privasi akun bisa membantu melindungi data saya.
	RE2	Saya yakin menggunakan kata sandi yang kuat bisa mencegah akun saya diretas.
	RE3	Saya merasa menghindari membagikan informasi pribadi bisa meningkatkan keamanan saya.
	RE4	Saya percaya fitur keamanan media sosial bisa membantu menjaga data saya tetap aman.
	RE5	Saya yakin mengganti kata sandi secara rutin bisa mengurangi risiko pencurian akun.
	RE6	Saya percaya bahwa mengaktifkan verifikasi dua langkah bisa membuat akun lebih aman.
Self-Efficacy (Seberapa yakin dalam menjaga keamanan data)	EF1	Saya yakin bisa melindungi data pribadi saya di media sosial.
	EF2	Saya merasa tahu cara mengatur privasi akun saya dengan baik.
	EF3	Saya bisa mengenali tanda-tanda ancaman terhadap keamanan data saya.
	EF4	Saya bisa segera bertindak jika akun saya mengalami aktivitas mencurigakan.
	EF5	Saya yakin bisa menghindari pencurian data dengan langkah yang benar.
	EF6	Saya bisa menjaga keamanan akun saya dengan kebiasaan yang baik.
Response Costs (Hambatan dalam melindungi data)	RC1	Saya merasa mengatur privasi akun itu ribet.
	RC2	Saya kurang paham cara melindungi data pribadi saya di media sosial.
	RC3	Saya merasa fitur keamanan media sosial sulit digunakan.
	RC4	Saya malas mengganti kata sandi akun saya terlalu sering.
	RC5	Saya merasa mengamankan akun butuh waktu yang lama.
	RC6	Saya merasa membatasi privasi akun bisa mengurangi kenyamanan saya dalam bersosial di media.
Motivasi	MP1	Saya ingin meningkatkan keamanan data pribadi saya di media

Variabel	Kode	Item Pernyataan
Perlindungan Data Pribadi di Media Sosial (Niat untuk melindungi data)		sosial.
	MP2	Saya berencana mengubah pengaturan privasi akun saya agar lebih aman.
	MP3	Saya akan lebih berhati-hati saat membagikan informasi pribadi di media sosial.
	MP4	Saya akan menggunakan kata sandi yang lebih kuat untuk akun saya.
	MP5	Saya akan mengaktifkan fitur keamanan tambahan seperti verifikasi dua langkah.
	MP6	Saya ingin memastikan data pribadi saya tetap aman saat menggunakan media sosial.

2.1.5 Pengumpulan Data Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan landasan filsafat positivisme. Pendekatan kuantitatif dipilih karena penelitian bertujuan untuk menguji hubungan antar variabel secara empiris melalui data numerik dan analisis statistik [24].

Pengumpulan data dilakukan menggunakan survei daring melalui penyebaran kuesioner kepada responden yang memenuhi kriteria penelitian. Kuesioner digunakan sebagai instrumen utama untuk memperoleh data primer, dengan pertanyaan yang disusun berdasarkan kerangka *Protection Motivation Theory* (PMT) [25].

Variabel penelitian dikelompokkan ke dalam dua komponen utama PMT, yaitu:

Threat Appraisal, yang terdiri dari Perceived Severity dan Perceived Vulnerability.

Coping Appraisal, yang meliputi Response Efficacy, Self-Efficacy, dan Response Costs.

Seluruh item pernyataan diukur menggunakan skala Likert lima poin, mulai dari 1 (sangat tidak setuju) hingga 5 (sangat setuju). Skala ini digunakan untuk mengukur sikap, persepsi, dan pandangan responden terhadap isu perlindungan data pribadi di media sosial [26].

2.1.6 Pengolahan dan Analisis Data

Data yang telah terkumpul dianalisis menggunakan metode *Structural Equation Modeling–Partial Least Squares* (SEM-PLS). Metode SEM-PLS dipilih karena mampu menganalisis hubungan antar variabel laten secara simultan serta cocok digunakan pada penelitian dengan model yang kompleks dan ukuran sampel relatif moderat [27].

Tahapan analisis data meliputi evaluasi model pengukuran (*outer model*) dan evaluasi model struktural (*inner model*).

Evaluasi *outer model* dilakukan untuk menilai reliabilitas dan validitas konstruk. Reliabilitas internal diuji menggunakan nilai Cronbach's Alpha dan *Composite Reliability* (CR), dengan nilai CR di atas 0,70 menunjukkan tingkat reliabilitas yang baik. Selanjutnya, validitas konvergen dievaluasi melalui nilai *outer loading* dan *Average Variance Extracted* (AVE), di mana nilai AVE minimal sebesar 0,50 menunjukkan bahwa konstruk mampu menjelaskan lebih dari 50% varians indikatornya [28].

Validitas diskriminan diuji menggunakan beberapa pendekatan, yaitu *cross-loading*, kriteria Fornell–Larcker, dan rasio *Heterotrait-Monotrait* (HTMT). Nilai HTMT di bawah 0,90 menunjukkan bahwa konstruk dalam model memiliki perbedaan yang memadai satu sama lain.

Evaluasi *inner model* dilakukan untuk menilai hubungan antar variabel laten melalui koefisien determinasi (R^2), relevansi prediktif (Q^2), serta signifikansi koefisien jalur. Nilai R^2 digunakan untuk melihat kemampuan variabel independen dalam menjelaskan variabel dependen, sedangkan nilai Q^2 menunjukkan kemampuan prediktif model. Signifikansi hubungan antar variabel diuji menggunakan teknik *bootstrapping*, dengan nilai statistik-t lebih besar dari 1,96 menunjukkan hubungan yang signifikan pada tingkat signifikansi 5%.

Selain itu, ukuran efek f^2 dan q^2 digunakan untuk menilai besarnya pengaruh masing-masing variabel independen terhadap variabel dependen, baik dari sisi kekuatan pengaruh maupun kontribusi terhadap kemampuan prediksi model.

3. Hasil dan Pembahasan

3.1 Karakteristik Responden

Informasi mengenai karakteristik responden diperoleh melalui pengolahan data deskriptif yang dikumpulkan menggunakan kuesioner penelitian. Data ini bertujuan untuk memberikan gambaran umum mengenai profil responden yang terlibat dalam penelitian. Mengingat setiap responden memiliki pengalaman dan latar belakang yang berbeda dalam menggunakan media sosial, maka dilakukan pengelompokan berdasarkan variabel demografis, meliputi usia, jenis kelamin, tingkat pendidikan/pekerjaan, pengalaman menghadapi masalah keamanan, serta penggunaan fitur keamanan pada akun media sosial.

Tabel 3. Frekuensi Karakteristik Responden

Karakteristik Responden	Kriteria	Frekuensi	Persentase
Usia	13 – 16 Tahun	4	4%
	17 – 22 Tahun	88	88%
	23 – 28 Tahun	8	8%
Jenis Kelamin	Laki-laki	41	41%
	Perempuan	59	59%
Pekerjaan	SLTA/Sederajat	32	32%
	S1/Sederajat	60	60%
	S2/Sederajat	8	8%
Apakah Anda Pernah Mengalami Masalah Keamanan di Tiktok atau Instagram?	Ya, Instagram	45	45%
	Ya, Dikeduanya	34	34%
	Ya, Di Tiktok	21	21%
Apakah Anda Mengaktifkan Fitur Keamanan pada Saat Login di akun Tiktok atau Instagram?	Tidak, Di Instagram	2	2%
	Tidak, Dikeduanya	2	2%
	Tidak, Di Tiktok	3	3%%
	Ya, Di Instagram	84	84%
	Ya, Dikeduanya	6	6%
	Ya, Di Tiktok	3	3%
Total		**100**	**100%**

Sumber : Hasil Output SmartPLS 4.0.9.9 (2025)

Ringkasan distribusi karakteristik responden disajikan pada Tabel 2. Hasil analisis menunjukkan bahwa mayoritas responden berada pada rentang usia 17–22 tahun, yaitu sebanyak 88 orang (88%), diikuti oleh kelompok usia 23–28 tahun sebanyak 8 orang (8%), dan usia 13–16 tahun sebanyak 4 orang (4%). Berdasarkan jenis kelamin, responden perempuan mendominasi dengan persentase 59%, sementara responden laki-laki sebesar 41%.

Ditinjau dari latar belakang pendidikan, sebagian besar responden merupakan lulusan atau sedang menempuh pendidikan S1/sederajat sebanyak 60%, diikuti oleh SLTA/sederajat sebesar 32%, dan S2/sederajat sebesar 8%. Pada aspek pengalaman keamanan, sebagian besar responden mengaku pernah mengalami masalah keamanan pada Instagram (45%), baik pada kedua platform TikTok dan Instagram (34%), maupun hanya pada TikTok (21%). Sementara itu, mayoritas responden menyatakan telah mengaktifkan fitur keamanan saat login, khususnya pada Instagram (84%), yang menunjukkan adanya kesadaran awal terhadap pentingnya perlindungan akun.

3.2 Evaluasi Outer Model (Measurement Model)

Tahap awal analisis menggunakan metode Partial Least Square - Structural Equation Modeling (PLS-SEM) adalah melakukan evaluasi terhadap outer model atau model pengukuran. Evaluasi ini bertujuan untuk memastikan bahwa indikator yang digunakan mampu mengukur konstruk penelitian secara valid dan reliabel. Pengujian dilakukan melalui analisis validitas konvergen, reliabilitas internal, serta validitas diskriminan dengan bantuan perangkat lunak SmartPLS versi 4.0.9.9.

3.2.1 Validitas Konvergen

Tabel 4. Nilai Loading Factor Setelah Eliminasi

Variabel	Indikator	Loading Factor	Tanda	Batas	Hasil Uji
Perceived Severity	X1.1	0.825	>	0.70	Valid
	X1.2	0.842	>	0.70	Valid
	X1.3	0.889	>	0.70	Valid
	X1.4	0.795	>	0.70	Valid
	X1.5	0.808	>	0.70	Valid
	X1.6	0.796	>	0.70	Valid
Perceived Vulnerability	X2.1	0.785	>	0.70	Valid
	X2.2	0.844	>	0.70	Valid
	X2.3	0.803	>	0.70	Valid
	X2.4	0.899	>	0.70	Valid
	X2.5	0.905	>	0.70	Valid
	X2.6	0.852	>	0.70	Valid
Respon Efficacy	X3.1	0.729	>	0.70	Valid
	X3.2	0.797	>	0.70	Valid
	X3.3	0.814	>	0.70	Valid
	X3.4	0.738	>	0.70	Valid
	X3.5	0.789	>	0.70	Valid
	X3.6	0.705	>	0.70	Valid

Variabel	Indikator	Loading Factor	Tanda	Batas	Hasil Uji
Self-Efficacy	X4.1	0.761	>	0.70	Valid
	X4.2	0.850	>	0.70	Valid
	X4.3	0.799	>	0.70	Valid
	X4.4	0.804	>	0.70	Valid
	X4.5	0.818	>	0.70	Valid
	X4.6	0.836	>	0.70	Valid
Response Cost	X5.2	0.828	>	0.70	Valid
	X5.3	0.810	>	0.70	Valid
	X5.4	0.819	>	0.70	Valid
	X5.5	0.794	>	0.70	Valid
	X5.6	0.817	>	0.70	Valid
Motivasi Perlindungan Data Pribadi Di Media Sosial	Y1	0.818	>	0.70	Valid
	Y2	0.925	>	0.70	Valid
	Y3	0.931	>	0.70	Valid
	Y4	0.891	>	0.70	Valid
	Y5	0.910	>	0.70	Valid
	Y6	0.924	>	0.70	Valid

Sumber : Hasil Output SmartPLS 4.0.9.9 (2025)

Tabel 5. Nilai Average Variance Extracted (AVE)

Variabel	AVE	Tanda	Batas	Hasil Uji
Perceived Severity	0.683	>	0.50	Valid
Perceived Vulnerability	0.721	>	0.50	Valid
Respon Efficacy	0.582	>	0.50	Valid
Self-Efficacy	0.659	>	0.50	Valid
Response Cost	0.662	>	0.50	Valid
Motivasi Perlindungan Data Prubadi Di Media Sosial	0.811	>	0.50	Valid

Sumber : Hasil Output SmartPLS 4.0.9.9 (2025)

Validitas konvergen dievaluasi berdasarkan nilai outer loading dan Average Variance Extracted (AVE). Suatu indikator dinyatakan valid apabila memiliki nilai outer loading ≥ 0,70. Hasil pengujian awal menunjukkan bahwa seluruh indikator memenuhi kriteria tersebut, kecuali indikator X5.1 pada variabel Response Cost yang memiliki nilai loading sebesar 0,583. Oleh karena itu, indikator tersebut dieliminasi dari model pengukuran.

Setelah proses eliminasi, seluruh indikator menunjukkan nilai outer loading di atas batas minimum yang ditetapkan, sehingga seluruh indikator dinyatakan valid. Selain itu, hasil pengujian AVE pada masing-masing konstruk menunjukkan nilai di atas 0,50, yang mengindikasikan bahwa seluruh variabel laten telah memenuhi kriteria validitas konvergen dengan baik.

3.2.2 Reliabilitas Internal

Uji reliabilitas dilakukan untuk menilai konsistensi internal indikator dalam mengukur konstruk laten. Reliabilitas dinyatakan terpenuhi apabila nilai Cronbach's Alpha dan Composite Reliability berada di atas 0,70. Berdasarkan hasil pengujian, seluruh variabel penelitian memiliki nilai Cronbach's Alpha dan Composite Reliability yang melebihi batas tersebut. Dengan demikian, dapat disimpulkan bahwa seluruh konstruk dalam penelitian ini bersifat reliabel dan mampu merepresentasikan variabel yang diukur secara konsisten.

3.2.3 Validitas Diskriminan

Validitas diskriminan diuji menggunakan tiga pendekatan, yaitu cross loading, kriteria Fornell-Larcker, dan Heterotrait-Monotrait Ratio (HTMT). Hasil pengujian cross loading menunjukkan bahwa setiap indikator memiliki nilai loading tertinggi pada konstruk yang diukur dibandingkan dengan konstruk lainnya. Selanjutnya, hasil uji Fornell-Larcker memperlihatkan bahwa nilai akar AVE setiap konstruk lebih besar dibandingkan korelasi antar konstruk lain. Sementara itu, nilai HTMT seluruh variabel berada di bawah ambang batas 0,90. Berdasarkan ketiga pengujian tersebut, dapat disimpulkan bahwa model telah memenuhi kriteria validitas diskriminan dan layak untuk dilanjutkan ke tahap evaluasi inner model.

Tabel 6. Fornell Larcker

	Motivasi Perlindungan Data Pribadi Di Media Sosial	**Perceived Severity**	**Perceived Vulnerability**	**Response Costs**	**Respon Efficacy**	**Self Efficacy**
Motivasi Perlindungan Data Pribadi Di Media Sosial	**0.901**					
Perceived Severity	0. 813	**0.826**				
Perceived Vulnerability	0.822	0.733	**0.849**			
Response Costs	0.180	0.137	0.238	**0.814**		
Respon Efficacy	0.486	0.516	0.706	0.125	**0.763**	
Self Efficacy	0.822	0.775	0.754	0.214	0.567	**0.812**

Tabel 7. Uji Heterotrait Monotrait Ratio

	Motivasi Perlindungan Data Pribadi Di Media Sosial	**Perceived Severity**	**Perceived Vulnerability**	**Response Costs**	**Respon Efficacy**	**Self Efficacy**
Motivasi Perlindungan Data Pribadi Di Media Sosial						
Perceived Severity	0.872					
Perceived Vulnerability	0.864	0.799				
Response Costs	0.164	0.145	0.228			
Respon Efficacy	0.526	0.579	0.789	0.151		
Self Efficacy	0.886	0.858	0.826	0.225	0.634	

3.3 Evaluasi Inner Model (Structural Model)

Evaluasi inner model bertujuan untuk menguji hubungan kausal antar variabel laten dalam model struktural. Pengujian dilakukan dengan menganalisis nilai koefisien determinasi (R^2), predictive relevance (Q^2), pengujian hipotesis, serta ukuran efek (f^2 dan q^2).

3.3.1 Koefisien Determinasi (R^2)

Nilai R^2 digunakan untuk mengukur sejauh mana variabel independen mampu menjelaskan variasi pada variabel dependen. Hasil analisis menunjukkan bahwa nilai R^2 untuk variabel Motivasi Perlindungan Data Pribadi di Media Sosial sebesar 0,826. Artinya, sebesar 82,6% variasi motivasi perlindungan data pribadi dapat dijelaskan oleh variabel Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy, dan Response Cost, sedangkan sisanya sebesar 17,4% dipengaruhi oleh faktor lain di luar model penelitian. Nilai ini menunjukkan bahwa model memiliki kemampuan prediktif yang sangat kuat.

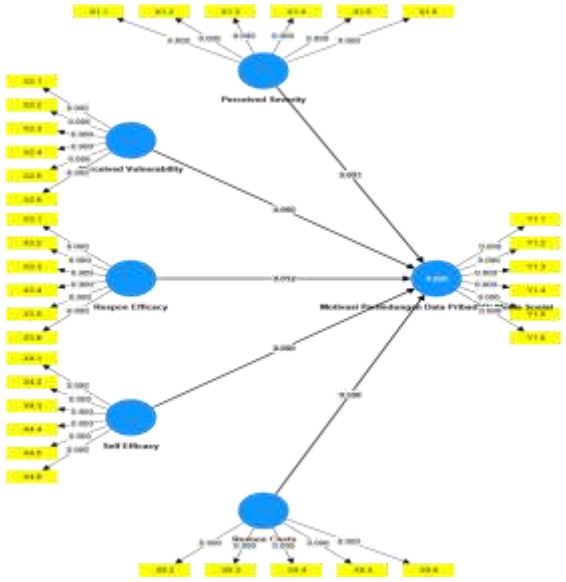
3.3.2 Predictive Relevance (Q^2)

Tabel 8. Nilai Q^2 Predict

Variabel	**Q^2 *Predict***	**Hasil Uji**
Motivasi Perlindungan Data Pribadi Di Media Sosial	0.633	Relevan

Uji Q^2 dilakukan menggunakan teknik blindfolding untuk menilai kemampuan prediktif model. Hasil pengujian menunjukkan nilai Q^2 sebesar 0,633, yang lebih besar dari nol. Hal ini menandakan bahwa model memiliki relevansi prediktif yang baik dalam menjelaskan motivasi perlindungan data pribadi di media sosial.

3.3.3 Uji Hipotesis



Gambar 2. Bootstrapping

Pengujian hipotesis dilakukan melalui teknik bootstrapping dengan memperhatikan nilai original sample, T-statistics, dan P-value. Hasil analisis menunjukkan bahwa Perceived Severity, Perceived Vulnerability, dan Self-Efficacy memiliki pengaruh positif dan signifikan terhadap motivasi perlindungan data pribadi. Sebaliknya, Response Efficacy menunjukkan pengaruh negatif yang signifikan, sementara Response Cost tidak memberikan pengaruh signifikan terhadap motivasi perlindungan data pribadi di media sosial.

3.3.4 Ukuran Efek (f^2)

Analisis ukuran efek menunjukkan bahwa variabel Perceived Severity, Perceived Vulnerability, dan Self-Efficacy memiliki pengaruh besar terhadap variabel dependen. Variabel Response Efficacy memiliki pengaruh sedang, sedangkan Response Cost memiliki pengaruh yang sangat kecil. Hal ini mengindikasikan bahwa faktor persepsi ancaman dan keyakinan diri berperan dominan dalam mendorong motivasi perlindungan data pribadi.

Tabel 9. Uji F Square

Variabel	F Square	Kriteria
Perceived Severity terhadap Motivasi Perlindungan Data Pribadi Di Media Sosial	0.162	Besar
Perceived Vulnerability terhadap Motivasi Perlindungan Data Pribadi Di Media Sosial	0.413	Besar
Respon Efficacy terhadap Motivasi Perlindungan Data Pribadi Di Media	0.129	Sedang

Sosial		
Self-Efficacy terhadap Motivasi Perlindungan Data Pribadi Di Media Sosial	0.213	Besar
Response Cost terhadap Motivasi Perlindungan Data Pribadi Di Media Sosial	0.004	Kecil

3.3.5 Ukuran Efek Prediktif (q^2)

Tabel 10. Nilai Q^2 Predict

Variabel	Q^2 *Predict*	Hasil Uji
Motivasi Perlindungan Data Pribadi Di Media Sosial	0.633	Relevan

Hasil pengujian q^2 menunjukkan bahwa variabel motivasi perlindungan data pribadi memiliki nilai q^2 sebesar 0,633, yang termasuk dalam kategori efek besar. Hal ini memperkuat temuan bahwa model penelitian memiliki kemampuan prediktif yang tinggi.

3.4 Pembahasan

3.4.1 Pengaruh Perceived Severity terhadap Motivasi Perlindungan Data Pribadi

Hasil penelitian menunjukkan bahwa persepsi keparahan ancaman berpengaruh positif dan signifikan terhadap motivasi perlindungan data pribadi. Temuan ini mengindikasikan bahwa semakin besar risiko yang dirasakan akibat kebocoran data, semakin tinggi dorongan individu untuk melindungi informasi pribadinya. Hasil ini sejalan dengan Protection Motivation Theory (PMT) yang menyatakan bahwa penilaian ancaman merupakan faktor penting dalam memicu perilaku protektif.

3.4.2 Pengaruh Perceived Vulnerability terhadap Motivasi Perlindungan Data Pribadi

Perceived Vulnerability terbukti memiliki pengaruh positif dan signifikan terhadap motivasi perlindungan data pribadi. Hal ini menunjukkan bahwa individu yang merasa dirinya rentan terhadap ancaman keamanan cenderung lebih terdorong untuk mengambil langkah perlindungan. Temuan ini konsisten dengan teori PMT dan penelitian sebelumnya yang menekankan peran kerentanan yang dirasakan dalam membentuk perilaku protektif.

3.4.3 Pengaruh Response Efficacy terhadap Motivasi Perlindungan Data Pribadi

Hasil penelitian menunjukkan bahwa Response Efficacy berpengaruh negatif dan signifikan terhadap motivasi perlindungan data pribadi. Temuan ini mengindikasikan adanya fenomena false sense of security, di mana individu yang terlalu percaya pada efektivitas sistem keamanan justru menjadi kurang termotivasi untuk melakukan perlindungan secara aktif.

3.4.4 Pengaruh Self-Efficacy terhadap Motivasi Perlindungan Data Pribadi

Self-Efficacy terbukti memiliki pengaruh positif dan signifikan terhadap motivasi perlindungan data pribadi. Individu yang memiliki keyakinan tinggi terhadap kemampuannya dalam melindungi data cenderung lebih aktif dalam menerapkan langkah-langkah keamanan. Temuan ini memperkuat konsep PMT yang menempatkan self-efficacy sebagai faktor kunci dalam penilaian penanganan ancaman.

3.4.5 Pengaruh Response Cost terhadap Motivasi Perlindungan Data Pribadi

Response Cost tidak menunjukkan pengaruh signifikan terhadap motivasi perlindungan data pribadi. Hal ini mengindikasikan bahwa bagi responden yang didominasi oleh Generasi Z, biaya atau pengorbanan dalam melindungi data pribadi tidak dianggap sebagai hambatan utama. Tingginya literasi digital dan kebiasaan menggunakan teknologi sejak dini membuat tindakan perlindungan data dipersepsikan sebagai sesuatu yang mudah dan tidak memberatkan.

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa Protection Motivation Theory (PMT) secara umum mampu menjelaskan faktor-faktor yang memengaruhi motivasi Generasi Z dalam melindungi data pribadi di media sosial. Dari lima hipotesis yang diuji, sebagian besar variabel dalam kerangka PMT menunjukkan pengaruh yang signifikan terhadap motivasi perlindungan data pribadi. Perceived severity, perceived vulnerability, dan self-efficacy terbukti berpengaruh positif dan signifikan, yang menandakan bahwa persepsi terhadap tingkat keparahan ancaman, kerentanan terhadap risiko digital, serta keyakinan individu terhadap kemampuan dirinya menjadi pendorong utama munculnya perilaku protektif. Sebaliknya, response efficacy menunjukkan pengaruh negatif yang signifikan, mengindikasikan adanya kecenderungan rasa aman semu ketika individu terlalu bergantung pada efektivitas sistem keamanan yang tersedia, sehingga menurunkan inisiatif perlindungan secara aktif. Sementara itu, response costs tidak memberikan pengaruh yang signifikan, yang menunjukkan bahwa upaya perlindungan data tidak dipersepsikan sebagai beban oleh Generasi Z karena tingginya literasi digital dan kebiasaan penggunaan teknologi. Dengan demikian, hasil penelitian ini menegaskan bahwa motivasi perlindungan data pribadi pada Generasi Z lebih dipengaruhi oleh faktor persepsi ancaman dan keyakinan diri dibandingkan oleh pertimbangan biaya atau pengorbanan dalam melakukan perlindungan.

Referensi

[1] M. Dkk., "Mengamati Perkembangan Teknologi dan Bisnis Digital dalam Transisi Menuju Era Industri 5 . 0," *Wawasan J. Ilmu Manajemen, Ekon. dan Kewirausahan*, vol. 2, no. 3, pp. 175–187, 2024.

[2] S. Widiani, "Generasi Z Dalam Memanfaatkan Media Sosial," *Kaisa J. Pendidik. dan Pembelajaran*, vol. 2, no. 1, pp. 1–9, 2023.

[3] N. Chris, "Pengaruh Kesadaran Keamanan Informasi dan Privasi Jaringan Sosial Terhadap Perilaku Perlindungan Privasi pada Para Pengguna Jaringan Sosial," *SOURCE J. Ilmu Komun.*, vol. 7, no. 2, p. 170, 2021.

[4] Y. F. Nafisah, "Penggunaan Media Sosial pada Generasi Z Use of Social Media in Generation Z Abstrak," *Character J. Penelit. Psikol.*, vol. 11, no. 02, pp. 705–713, 2024.

[5] S. N. F. Jannah and T. S. Rosyiidiani, "Gejala Fear of Missing Out dan Adiksi Media Sosial Remaja Putri di Era Pandemi Covid-19," *J. Paradig. J. Multidisipliner Mhs. Pascasarj. Indones.*, vol. 3, no. 1, pp. 1–14, 2022.

[6] V. Kumalasari and S. Sumiyana, "Faktor-Faktor yang Memengaruhi Behavioral Intention untuk Menggunakan Tiktok Shop pada Gen Z," *ABIS Account. Bus. Inf. Syst.*, vol. 15, no. 1, pp. 37–48, 2024.

[7] A. C. Kusuma and A. D. Rahmani, "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)," *SUPREMASI J. Huk.*, vol. 5, no. 1, pp. 46–63, 2022.

[8] E. Yosida, "Persepsi Gen Z Mengenai Perilaku Oversharing di Media Sosial," *DOI 10.37817/ikraith-humaniora*, vol. 9, no. 1, pp. 1–9, 2025.

[9] A. Dkk., "Pentingnya Mewujudkan Pertahanan dan Keamanan Bagi Generasi Z di Era Media Sosial," *JIHAD J. Ilmu Huk. dan Adm.*, vol. 6, no. 2, pp. 2746–3842, 2024.

[10] C. Dkk., "Research on the influence mechanism of privacy invasion experiences with privacy protection intentions in social media contexts: Regulatory focus as the moderator," *Front. Psychol.*, vol. 13, 2023.

[11] M. P. C. Randana and R. A. Syakurah, "Review of social media intervention in adult population during COVID-19 pandemic based on protection motivation theory," *Int. J. Public Heal. Sci.*, vol. 10, no. 4, pp. 843–849, 2021.

[12] M. B. Yel and M. K. M. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022.

[13] N. Dkk., "Protecting Privacy on Social Media: Mitigating Cyberbullying and Data Heist Through Regulated Use and Detox, with a Mediating Role of Privacy Safety Motivations," *Soc.*

Media Soc., vol. 10, no. 4, 2024.
[14] R. Dkk., "Adoption of identity theft protection services in social media: A PMT investigation," *Sustain. Eng. Innov.*, vol. 6, no. 1, pp. 87–102, 2024.
[15] M. P. Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]," *J. Polit. Din. Masal. Polit. Dalam Negeri dan Hub. Int.*, vol. 13, no. 2, pp. 222–238, 2023.
[16] N. Dkk., "Dinamika Perilaku Gen Z Sebagai Generasi Internet," *Konsensus J. Ilmu Pertahanan, Huk. dan Ilmu Komun.*, vol. 1, no. 1, pp. 95–102, 2024.
[17] M. A. D. Septianto, D. Priharsari, and ..., "Analisis Kesediaan Berbagi Identitas Digital berdasarkan PMT: Perceived Severity, Perceived Vulnerability, Response Efficacy, dan Usia," *... Teknol. Inf. dan ...*, vol. 6, no. 11, pp. 5532–5540, 2022.
[18] Y. A. L. Sari, A. Kusyanti, and R. I. Rokhmawati, "Analisis Faktor-Faktor yang Memengaruhi Perilaku Pengguna Sistem Informasi Akademik Mahasiswa dalam Penciptaan Kata Sandi Kuat dengan Menggunakan Protection Motivation Theory (Studi pada XYZ)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 4, pp. 1348–1357, 2018.
[19] F. D. Pawestri and J. Jumino, "Analisis Hubungan Information Privacy Concern dan Perilaku Perlindungan Privasi Pengguna Twitter di Indonesia," *Anuva J. Kaji. Budaya, Perpustakaan, dan Inf.*, vol. 5, no. 2, pp. 221–236, 2021.
[20] S. R. Winarto and R. Bisma, "Studi Literatur: Analisis Persepsi UMKM Di Indonesia Terhadap Cyber Security Menggunakan Model Protection Motivation Theory (PMT)," *J. Informatics Comput. Sci.*, vol. 3, no. 01, pp. 20–28, 2021.
[21] A. T. Susena, A. Wigraha, and R. Dantes, "ROLLER TERHADAP TORQUE DAN RPM PADA MOTOR GANESHA ELECTRIC VEHICLES 1 . 0 BASE CONTINOUS VARIABLE TRANSMISION (CVT) Singaraja , Indonesia," *J. Jur. Tek. Mesin*, vol. 7, no. 1, 2017.
[22] P. G. Subhaktiyasa, "Menentukan Populasi dan Sampel : Pendekatan Metodologi Penelitian Kuantitatif dan Kualitatif," *J. Ilm. Profesi Pendidik.*, vol. 9, no. 1, pp. 2721–2731, 2024.
[23] S. K. Ahmed, "How to choose a sampling technique and determine sample size for research: A simplified guide for researchers," *Oral Oncol. Reports*, vol. 12, no. September, p. 100662, 2024.
[24] A. Dkk., "Metodologi Penelitian Kuantitatif dan Penerapannya dalam Penelitian," *Educ. Journal.2022*, vol. 2, no. 2, pp. 1–6, 2022.
[25] gunawan Siti, junista, "Teknik Pengumpulan Data," *JISOSEPOL J. ILMU Sos. Ekon. DAN Polit.*, vol. 3, no. 1, pp. 39–47, 2024.
[26] B. Simamora, "Skala Likert, Bias Penggunaan dan Jalan Keluarnya," *J. Manaj.*, vol. 12, no. 1, pp. 84–93, 2022.
[27] Rensya Siwalette dkk, "Analisi Faktor-Faktor Yang Berpengaruh Terhadap Pembelian Secara Online Di Kota Ambon Menggunakan Metode Structural Equation Modeling - Partial Least Square (SEM-PLS) (Analysis Of Factors That Influence Online Shopping in The City of Ambon Using Struc," *J. Stat. its Appl.*, vol. 4, pp. 57–64, 2022.
[28] D. J. Ketchen, *A Primer on Partial Least Squares Structural Equation Modeling*, vol. 46, no. 1–2. 2013.
[29] K. Dkk., "Analisis Kesediaan Berbagi Identitas Digital berdasarkan Faktor Self-Efficacy, Perceived Severity dan Gender," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 11, pp. 5380–5389, 2022.
[30] D. Fujs, "Social network self-protection model: What motivates users to self-protect?," *J. Cyber Secur. Mobil.*, vol. 8, no. 4, pp. 467–492, 2019.
[31] D. Yang, "A Replication Study of User Motivation in Protecting Information Security using Protection Motivation Theory and Self-Determination Theory," *AIS Trans. Replication Res.*, vol. 7, pp. 1–22, 2021.
[32] D. Sedek, "Motivational Factors in Privacy Protection Behaviour Model for Social Networking," *MATEC Web Conf.*, vol. 150, pp. 1–5, 2018.
[33] R. C. Eklund and G. Tenenbaum, "Protection Motivation Theory," in *Encyclopedia of Sport*

and Exercise Psychology, 2014. doi: 10.4135/9781483332222.n225.
[34] D. Alkire, "Triggers and motivators of privacy protection behavior on Facebook," *J. Serv. Mark.*, vol. 33, no. 1, pp. 57–72, 2019.