

BAB II

TINJAUAN PUSTAKA

2.1 Studi Sebelumnya

Penelitian sebelumnya oleh Randana dan Syakurah [24] *menggunakan metode Protection Motivation Theory* (PMT) untuk meneliti dampak intervensi media sosial terhadap orang dewasa selama epidemi COVID-19. Analisis meta ini didasarkan pada lima studi cross-sectional yang dilakukan pada tahun 2020 dengan total partisipan sebanyak 2.448 orang, dan menggunakan pendekatan *Preferred Reporting Items for Systematic Reviews and Meta-Analysis* (PRISMA) untuk menarik kesimpulan. Hasilnya menunjukkan bahwa cyberchondria, persepsi terhadap tingkat keparahan, serta persepsi kerentanan merupakan faktor prediktif utama dalam penggunaan media sosial selama masa pandemi. Reaksi perilaku individu selama pandemi secara signifikan dipengaruhi oleh *Cyberchondria*, yang didefinisikan sebagai kekhawatiran berlebihan yang disebabkan oleh paparan informasi kesehatan di internet. Reaksi seseorang terhadap informasi yang dibagikan di media sosial tentang suatu penyakit dipengaruhi oleh keyakinan mereka tentang tingkat keparahan dan kerentanannya.

Seiring dengan meningkatnya penggunaan media sosial, keamanan informasi dan privasi data pribadi menjadi perhatian utama dalam dunia digital. Penelitian yang dilakukan oleh Yel dan Nasution [25] mengkaji berbagai aspek yang memengaruhi perlindungan data pengguna di media sosial dengan menggunakan metode *blended*, yang mencakup analisis literatur dan penelitian pustaka. Temuan penelitian mengungkapkan bahwa keamanan informasi dipengaruhi secara signifikan oleh enam elemen kunci, yaitu perlindungan terhadap data, tingkat kesadaran pengguna, pengendalian akses, pengelolaan risiko, keterbukaan informasi, serta prinsip etika dalam pengelolaan data digital. Studi ini menekankan pentingnya desain sistem yang memungkinkan pengguna memiliki kendali atas data pribadi mereka untuk mencegah kebocoran informasi yang tidak diinginkan.

Penelitian sebelumnya oleh Niu dkk, [26] meneliti bagaimana kesadaran terhadap pengungkapan informasi daring dan masalah privasi memengaruhi tindakan perlindungan pengguna media sosial. Penelitian ini berfokus pada perilaku protektif, seperti pengaturan penggunaan media sosial dan detoksifikasi digital, yang muncul

sebagai respons terhadap pengalaman negatif seperti pencurian data dan perundungan siber. Dengan menggunakan metode survei, penelitian ini menemukan bahwa kesadaran akan pengungkapan informasi daring berperan sebagai mediator dalam hubungan antara pencurian data dan penggunaan media sosial yang diatur. Sementara itu, masalah privasi terbukti memediasi hubungan antara pengalaman perundungan siber dan kecenderungan pengguna untuk melakukan detoksifikasi media sosial. Hasil ini konsisten dengan Teori Motivasi Perlindungan (PMT), yang menunjukkan bahwa pengalaman negatif di dunia digital dapat memicu perilaku perlindungan terhadap privasi. Selain itu, penelitian ini mengungkap bahwa tidak semua individu yang menyadari ancaman privasi akan langsung mengambil tindakan perlindungan. Oleh karena itu, memahami hubungan kompleks antara pengalaman negatif daring, persepsi risiko, dan tindakan protektif menjadi hal yang krusial dalam meningkatkan kesadaran serta keamanan digital pengguna media sosial.

Penelitian sebelumnya oleh Chen dkk, [23], mengembangkan model mediasi rantai yang dimoderasi berdasarkan Teori Motivasi Perlindungan (PMT) dan Teori Fokus Regulasi untuk memahami bagaimana pengalaman pelanggaran privasi memengaruhi niat perlindungan privasi pengguna media sosial. Penelitian ini juga memperkenalkan kelelahan privasi sebagai variabel emosional yang berperan dalam proses pengambilan keputusan terkait perlindungan privasi. Melalui pendekatan kuantitatif, hasil studi menunjukkan bahwa pengalaman terkait pelanggaran privasi memiliki pengaruh terhadap meningkatnya keinginan pengguna untuk menjaga dan melindungi privasi mereka. Namun, efek ini dimediasi oleh dua faktor utama: biaya respons dan kelelahan privasi. Kelelahan privasi, yang muncul akibat paparan berulang terhadap ancaman privasi, justru dapat menurunkan niat perlindungan, meskipun pengguna telah mengalami pelanggaran sebelumnya. Penelitian ini juga menemukan bahwa perbedaan dalam fokus regulasi individu memengaruhi tingkat kelelahan privasi. Individu dengan fokus regulasi promosi yang lebih berorientasi pada pencapaian dan pertumbuhan cenderung lebih tahan terhadap kelelahan privasi dan tetap mempertahankan perilaku protektif. Sebaliknya, individu dengan fokus regulasi pencegahan yang lebih berhati-hati dan berorientasi pada keamanan lebih rentan mengalami kelelahan privasi, sehingga berpotensi mengabaikan tindakan perlindungan. Temuan ini menyoroti bahwa kelelahan privasi menjadi faktor kunci dalam menurunnya kesadaran perlindungan privasi di media

sosial. Namun, strategi berbasis fokus regulasi dapat menjadi solusi untuk mengurangi dampak negatif kelelahan privasi, sehingga pengguna tetap terdorong untuk menjaga keamanan data pribadi mereka secara optimal.

Penelitian sebelumnya oleh Rahman dkk [27], meneliti niat adopsi layanan perlindungan pencurian identitas di media sosial dalam konteks negara tertentu dengan menggunakan kerangka Teori Motivasi Perlindungan (PMT). Penelitian ini bertujuan untuk memahami sejauh mana individu terdorong untuk mengadopsi layanan perlindungan identitas dibandingkan dengan sekadar memiliki *wishful thinking* keinginan tanpa tindakan nyata terhadap perlindungan privasi mereka. berdasarkan pendekatan *Protection Motivation Theory* (PMT), hasil penelitian mengindikasikan bahwa faktor-faktor dalam teori tersebut memberikan kontribusi sebesar 47% terhadap keputusan pengguna dalam mengadopsi layanan perlindungan terhadap pencurian identitas di platform media sosial. Sementara itu, pengaruh PMT terhadap *wishful thinking* tercatat sebesar 35%. Temuan ini mengindikasikan bahwa sebagian besar individu menyadari ancaman pencurian identitas sebagai masalah serius dan memiliki kecenderungan lebih tinggi untuk mengambil tindakan protektif dibandingkan hanya berharap atau berangan-angan tentang perlindungan identitas. Dibandingkan dengan penelitian Saya, terdapat beberapa perbedaan utama. Penelitian Rahman dkk, berfokus pada adopsi layanan perlindungan pencurian identitas di media sosial secara umum, sementara penelitian saya secara spesifik meneliti motivasi Generasi Z dalam melindungi data pribadi di Instagram dan TikTok berdasarkan PMT. Selain itu, metode penelitian berbeda, di mana penelitian Rahman dkk, menguji 10 hipotesis dengan model statistik, sementara penelitian Saya menggunakan pendekatan kuantitatif inferensia. Perbedaan lainnya terletak pada aspek yang ditekankan: penelitian Rahman dkk, menyoroti peran *wishful thinking* dalam keputusan perlindungan identitas, sedangkan penelitian ini lebih berfokus pada faktor-faktor motivasi perlindungan yang memengaruhi perilaku pengguna media sosial dalam menjaga data pribadi mereka.

Penelitian oleh Mehdy dkk, yang berjudul *Privacy as a Planned Behavior: Effects of Situational Factors on Privacy Perceptions and Plans* menggunakan teori *Theory of Planned Behavior* (TPB) untuk menganalisis bagaimana faktor situasional mempengaruhi persepsi privasi dan niat individu untuk mengungkapkan informasi pribadi. Melalui survei terhadap 401 peserta, penelitian ini menemukan bahwa norma

subjektif dan kontrol perilaku yang dirasakan memiliki hubungan positif dengan sikap privasi situasional, yang pada gilirannya mempengaruhi niat untuk mengungkapkan informasi. Hasil ini menunjukkan bahwa faktor-faktor psikologis dan situasional berperan penting dalam pengambilan keputusan terkait privasi di media sosial.

Sementara itu, studi oleh Kuo-Cheng dkk, yang berjudul *Social Media Privacy Management Strategies: A SEM Analysis of User Privacy Behaviors* mengadopsi teori *Communication Privacy Management* (CPM) dan menggunakan metode Structural Equation Modeling (SEM) untuk mengeksplorasi strategi manajemen privasi pengguna media sosial. Penelitian ini menunjukkan bahwa kesadaran keamanan dan kontrol privasi yang dirasakan berpengaruh signifikan terhadap bagaimana pengguna mengelola privasi dan seberapa banyak mereka mengungkapkan diri di platform media sosial. Temuan ini menyoroti pentingnya pemahaman individu terhadap kontrol privasi dan kesadaran akan risiko dalam pengambilan keputusan terkait privasi di media sosial.

Penelitian Erlangga menggunakan pendekatan *Technology Acceptance Model* (TAM) untuk menganalisis pengaruh persepsi kemudahan penggunaan terhadap sikap individu dalam menggunakan media sosial. Hasil penelitiannya menunjukkan bahwa semua hipotesis yang diajukan didukung, sehingga menegaskan relevansi model TAM dalam menjelaskan keterlibatan pengguna serta pentingnya variabel tambahan untuk memahami penerimaan teknologi di platform media sosial. Sementara itu, penelitian ini mengambil pendekatan berbeda dengan menggunakan *Protection Motivation Theory* (PMT) untuk menganalisis motivasi generasi Z dalam menjaga keamanan data pribadi di media sosial. Fokus utama diarahkan pada bagaimana persepsi ancaman dan penilaian kemampuan menghadapi risiko memengaruhi perilaku protektif terhadap data pribadi. Dengan demikian, perbedaan utama terletak pada pendekatan teoritis dan fokus kajian: jika penelitian sebelumnya lebih menekankan pada penerimaan dan penggunaan media sosial, maka penelitian ini berorientasi pada aspek perlindungan dan keamanan data pribadi dalam konteks penggunaan media sosial oleh generasi Z.

Penelitian ini menyoroti peran Teori Motivasi Perlindungan (PMT) dalam memahami bagaimana Generasi Z melindungi data pribadi di media sosial. Studi sebelumnya menunjukkan bahwa persepsi ancaman, kerentanan, dan efikasi diri memengaruhi perilaku protektif, namun faktor seperti kelelahan privasi dan wishful thinking dapat menghambat tindakan perlindungan. Selain itu, perbedaan dalam fokus

regulasi juga berperan dalam respons terhadap ancaman privasi. Mengingat Generasi Z merupakan pengguna aktif media sosial dengan tingkat keterpaparan data tinggi, penelitian ini diharapkan dapat berkontribusi dalam mengembangkan strategi edukasi dan kebijakan untuk meningkatkan kesadaran serta perlindungan privasi digital.



Tabel 2. 1 Studi Sebelumnya

No	Peneliti	Tahun	Tujuan	Metode	Hasil
1	Randana & Syakurah [24]	2021	Untuk menganalisis dampak intervensi media sosial pada populasi dewasa selama pandemi COVID-19 berdasarkan PMT.	<i>Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA)</i>	Terdapat lima studi <i>cross-sectional</i> yang melibatkan total 2.448 partisipan yang dipublikasikan pada tahun 2020. Di antara semua kategori berdasarkan 2.448 partisipan yang diteliti, ditunjukkan bahwa <i>cyberchondria</i> , Hasil penelitian ini menunjukkan bahwa dalam konteks pandemi COVID-19, <i>cyberchondria</i> , <i>perceived severity</i> , dan <i>perceived vulnerability</i> adalah faktor-faktor penting dalam media sosial yang memengaruhi respons perilaku individu. Penelitian ini menyoroti perlunya penyampaian informasi kesehatan yang terstruktur dan terpercaya untuk mengurangi kelebihan informasi dan dampak negatif dari <i>cyberchondria</i> , <i>perceived severity</i> , dan <i>perceived vulnerability</i> .
2	Mehdy dkk, [28]	2021	Menganalisis bagaimana faktor situasional mempengaruhi persepsi privasi dan niat untuk mengungkapkan informasi pribadi	Theory of Planned Behavior (TPB), survei online (N=401)	Norma subjektif dan kontrol perilaku yang dirasakan berhubungan positif dengan sikap privasi situasional, yang pada gilirannya mempengaruhi niat untuk mengungkapkan informasi

No	Peneliti	Tahun	Tujuan	Metode	Hasil
3	Kuo-Cheng Chung [29]	2021	Communication Privacy Management (CPM)	Communication Privacy Management (CPM), Structural Equation Modeling (SEM)	Kesadaran keamanan dan kontrol privasi yang dirasakan berpengaruh signifikan terhadap bagaimana pengguna mengelola privasi dan seberapa banyak mereka mengungkapkan diri
4	Erlangga Andi Sukma [30]	2018	Untuk mengetahui Pengaruh pada sikap terhadap penggunaan jejaring sosial berdasarkan persepsi kemudahan penggunaan individu (PEU)	Technology Acceptance Model	Hasil penelitian menunjukkan bahwa model TAM media sosial yang diusulkan dalam penelitian ini mendukung semua hipotesis sikap terhadap penggunaan media sosial. Hasil penelitian ini memberikan bukti untuk pentingnya variabel kunci tambahan untuk TAM dalam mempertimbangkan keterlibatan pengguna di situs media sosial dan strategi bisnis terkait media sosial lainnya
5	Yel & Nasution [25]	2022	Menganalisis dan mengetahui tingkat kesadaran risiko keamanan dan privasi dalam penggunaan media sosial berdasarkan gender dan generasi	Metode Blended, yaitu kombinasi penelitian pustaka dan analisis literatur terkait keamanan informasi di media sosial.	Penelitian menemukan bahwa enam faktor utama dalam perlindungan privasi data di media sosial adalah keamanan data, kesadaran pengguna, pengaturan kontrol, manajemen risiko, transparansi, dan etika. Selain itu, penelitian menyoroti pentingnya kepercayaan dalam desain sistem informasi serta

No	Peneliti	Tahun	Tujuan	Metode	Hasil
					perlunya kontrol pengguna terhadap data pribadi mereka.
6	Niu dkk, [26]	2024	Untuk mengeksplorasi bagaimana kesadaran pengungkapan informasi daring dan masalah privasi memengaruhi tindakan perlindungan pengguna media sosial, seperti penggunaan media sosial yang diatur dan detoksifikasi, sebagai respons terhadap pengalaman negatif seperti pencurian data dan perundungan siber.	Survey	Penelitian ini menemukan bahwa kesadaran akan pengungkapan informasi daring memediasi hubungan antara pencurian data dan penggunaan media sosial yang diatur, sementara masalah privasi memediasi hubungan antara pengalaman perundungan siber dan detoksifikasi media sosial. Hasil ini sejalan dengan Teori Motivasi Perlindungan (PMT), yang menunjukkan bahwa pengalaman negatif daring, seperti pencurian data dan perundungan <i>siber</i> , berkorelasi langsung dengan perilaku keamanan privasi. Selain itu, penelitian ini menyoroti bahwa motivasi tidak selalu mendorong tindakan perlindungan, sehingga memahami dinamika antara masalah privasi, pengalaman <i>negative</i> daring, dan perilaku protektif menjadi krusial dalam meningkatkan privasi dan keamanan digital pengguna.

No	Peneliti	Tahun	Tujuan	Metode	Hasil
7	Chen dkk, [23]	2023	Untuk mengembangkan model mediasi rantai yang dimoderasi berdasarkan Teori Motivasi Perlindungan (PMT) dan Teori Fokus Regulasi, serta memperkenalkan kelelahan privasi sebagai variabel emosional untuk memahami bagaimana pengalaman pelanggaran privasi memengaruhi niat perlindungan privasi pengguna media sosial.	Pendekatan Kuantitatif	Penelitian ini menemukan bahwa pengalaman pelanggaran privasi meningkatkan niat perlindungan privasi, tetapi efek ini dimediasi oleh biaya respons dan kelelahan privasi. Kelelahan privasi terbukti mengurangi niat perlindungan, meskipun pengguna mengalami pelanggaran sebelumnya. Individu dengan fokus regulasi promosi lebih tahan terhadap kelelahan privasi, sedangkan mereka dengan focus regulasi pencegahan lebih rentan mengalaminya. Hasil ini menunjukkan bahwa kelelahan privasi menjadi faktor utama yang membuat pengguna cenderung mengabaikan perlindungan privasi, namun dapat diatasi melalui strategi fokus regulasi.
8	Rahman dkk, [27]	2024	Untuk menganalisis niat adopsi layanan perlindungan pencurian identitas di media sosial dalam konteks negara tertentu dengan menggunakan kerangka Teori Motivasi Perlindungan (PMT).	Pendekatan berbasis PMT	Hasil penelitian ini menunjukkan bahwa variabel PMT memiliki pengaruh sebesar 47% terhadap adopsi layanan perlindungan pencurian identitas di media sosial, sedangkan pengaruhnya terhadap <i>wishful thinking</i> sebesar 35%. Dengan demikian, niat adopsi lebih besar dibandingkan <i>wishful thinking</i> , yang berarti

No	Peneliti	Tahun	Tujuan	Metode	Hasil
					sebagian besar orang menyadari bahwa pencurian identitas adalah masalah serius dan ingin mengadopsi layanan perlindungan identitas.

Tabel 2. 2 Perbandingan Teori Studi Sebelumnya

Aspek	Protection Motivation Theory (PMT)	Theory of Planned Behavior (TPB)	Communication Privacy Management (CPM)	Technology Acceptance Model (TAM)
Fokus	Motivasi perlindungan dari ancaman	Perilaku yang dipengaruhi oleh niat dan kontrol	Manajemen privasi dan pengungkapan informasi	Penerimaan dan penggunaan teknologi
Komponen Utama	Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy, Response Costs	Niat, Sikap, Norma Subjektif, Kontrol Perilaku	Boundary Management, Privacy Rules, Communication	Persepsi Kemudahan Penggunaan, Persepsi Manfaat
Proses Kognitif	Penilaian ancaman dan penilaian tindakan perlindungan	Evaluasi sikap dan norma sosial	Pengelolaan batasan privasi	Evaluasi kemudahan dan manfaat teknologi

Tindakan Perlindungan	Dipicu oleh persepsi ancaman dan efikasi tindakan	Dipengaruhi oleh niat yang dibentuk oleh sikap	Mengatur informasi yang dibagi dan batasan privasi	Mengadopsi teknologi yang dianggap berguna dan mudah
Konteks Penggunaan	Keamanan data, kesehatan, perilaku risiko	Berbagai perilaku sosial dan individu	Interaksi di media sosial dan pengungkapan informasi	Adopsi teknologi baru, termasuk media sosial
Aplikasi di Media Sosial	Meningkatkan kesadaran privasi dan tindakan perlindungan	Memahami faktor yang mempengaruhi perilaku pengguna	Mengelola informasi pribadi dan privasi di platform	Menerima fitur keamanan dalam aplikasi media sosial

Berdasarkan perbandingan empat teori *Protection Motivation Theory (PMT)*, *Theory of Planned Behavior (TPB)*, *Communication Privacy Management (CPM)*, dan *Technology Acceptance Model (TAM)*, dapat disimpulkan bahwa PMT merupakan teori yang paling relevan. PMT secara khusus menekankan pada bagaimana individu merespons ancaman terhadap keamanan data melalui proses kognitif seperti persepsi terhadap tingkat bahaya, kerentanan, dan keyakinan akan efektivitas tindakan perlindungan. Berbeda dengan teori lain yang lebih fokus pada niat umum, penerimaan teknologi, atau pengelolaan privasi dalam komunikasi, PMT menawarkan kerangka yang kuat untuk menjelaskan mengapa dan bagaimana pengguna media sosial mengambil tindakan nyata untuk menjaga keamanan datanya, seperti memperbarui pengaturan privasi, menggunakan autentikasi dua faktor, dan membatasi informasi yang dibagikan. Oleh karena itu, PMT dipilih karena paling sesuai untuk menjelaskan dan mendorong perilaku perlindungan data pribadi di media sosial, serta dapat menjadi dasar dalam merancang intervensi yang meningkatkan kesadaran dan tindakan pengguna dalam menghadapi risiko digital.

2.2 Dasar Teori

2.2.1. Media Sosial

Media sosial merupakan salah satu hasil dari perkembangan teknologi berbasis internet, seperti Instagram, Facebook, Twitter, dan lainnya. Namun, tidak dapat dipungkiri bahwa setiap kemajuan pasti memiliki tantangan, termasuk dalam penggunaan media sosial yang kini banyak menimbulkan berbagai masalah, khususnya di kalangan generasi Z. Generasi ini dikenal sebagai generasi yang tumbuh seiring dengan berkembangnya teknologi digital. Keterikatan remaja terhadap teknologi membuat mereka hampir tidak pernah melewatkan hari tanpa mengakses media sosial, sehingga banyak dari mereka lebih memilih menghabiskan waktu di dunia maya. Dimana, manusia merupakan makhluk sosial yang secara alami memerlukan interaksi tatap muka. Namun, ketergantungan terhadap media sosial justru berdampak pada menurunnya kualitas hubungan sosial dalam kehidupan nyata sehari-hari [2].

Studi sebelumnya mendefinisikan media sosial sebagai "sekelompok aplikasi berbasis internet yang dibangun di atas dasar ideologis dan teknologi Web 2.0, yang memungkinkan penciptaan dan pertukaran konten yang dihasilkan oleh pengguna (*user-generated content*).\" Definisi ini menekankan peran aktif pengguna dalam menciptakan dan berbagi informasi melalui platform digital, yang menjadi ciri khas utama media sosial dalam era teknologi saat ini [31]. Menurut Kotler dan Keller, media sosial adalah "sarana bagi konsumen untuk berbagi teks, gambar, audio, dan informasi video dengan satu sama lain dan dengan perusahaan, dan sebaliknya.\" Definisi ini menyoroti fungsi media sosial sebagai alat komunikasi dua arah antara konsumen dan perusahaan, memungkinkan interaksi yang lebih personal dan langsung dalam konteks pemasaran dan layanan pelanggan [32].

2.2.2. Konsep Keamanan Data Pribadi

Definisi oleh *General Data Protection Regulation* (GDPR) Menurut Pasal 4(1) GDPR, data pribadi *didefinisikan* sebagai Setiap informasi yang berkaitan dengan orang perseorangan yang diidentifikasi atau dapat diidentifikasi ('subjek data'); orang perseorangan yang dapat diidentifikasi adalah seseorang yang dapat diidentifikasi, secara langsung atau tidak langsung, khususnya dengan merujuk pada pengenal seperti nama, nomor identifikasi, data lokasi, pengenal daring, atau satu atau lebih faktor khusus

untuk identitas fisik, fisiologis, genetik, mental, ekonomi, budaya, atau sosial orang perseorangan tersebut [33]. Definisi ini menekankan bahwa informasi yang dapat mengidentifikasi seseorang, baik secara langsung maupun tidak langsung, termasuk dalam kategori data pribadi dan harus dilindungi sesuai dengan peraturan yang berlaku.

Dalam *Dataversity* Michelle Knight mendefinisikan *privasi data* sebagai Serangkaian prinsip dan pedoman untuk memastikan pemrosesan, perlindungan, dan penanganan data sensitif yang terkait dengan individu secara hormat. Konsep ini berkaitan dengan siapa yang dapat mendefinisikan, mengamati, menggunakan, dan mengontrol informasi seseorang serta bagaimana caranya [34]. Keamanan data pribadi mengacu pada upaya individu dalam melindungi informasi pribadi mereka dari ancaman digital seperti peretasan, pencurian identitas, dan penyalahgunaan data. kesadaran akan privasi dan langkah-langkah keamanan sangat penting dalam dunia digital saat ini [25]. motivasi individu dalam menjaga keamanan data sangat dipengaruhi oleh pemahaman mereka terhadap risiko serta manfaat dari tindakan perlindungan yang diambil [35].

Meskipun keamanan data penting, masih banyak individu yang tidak menerapkan langkah-langkah perlindungan yang diperlukan. Faktor seperti rendahnya literasi digital, kemudahan akses terhadap berbagai platform daring, serta kecenderungan untuk mengutamakan kenyamanan dibandingkan keamanan, sering kali membuat seseorang lebih rentan terhadap ancaman *siber*. Selain itu, pengaruh sosial dan kebiasaan berbagi informasi di media sosial juga berperan dalam membentuk motivasi individu terkait privasi digital. Oleh sebab itu, dibutuhkan pendekatan yang menyeluruh, termasuk pendidikan berkelanjutan mengenai risiko keamanan siber serta penerapan regulasi yang mendukung perlindungan data, agar kesadaran dan upaya pencegahan dalam menjaga keamanan data pribadi dapat lebih meningkat [14].

2.2.3. Motivasi Gen Z dalam Menjaga Keamanan Data Pribadi

Generasi Z, yang lahir antara tahun 1997 hingga 2012, dikenal sebagai generasi yang tumbuh bersama teknologi dan sangat mengandalkan perangkat digital dalam kehidupan sehari-hari. Gen Z memiliki tingkat keterpaparan yang tinggi terhadap risiko keamanan digital namun sering kali kurang menyadari pentingnya perlindungan data pribadi [16]. Hal ini disebabkan oleh kebiasaan mereka dalam membagikan informasi

pribadi secara terbuka di berbagai platform media sosial, baik untuk berinteraksi dengan teman maupun mengikuti tren digital. Meskipun mereka tumbuh di era teknologi, literasi keamanan siber di kalangan Gen Z masih perlu ditingkatkan.

Mayoritas dari kelompok ini cenderung menggunakan kata sandi yang lemah, tidak mengaktifkan fitur autentikasi dua langkah, dan kurang waspada saat mengakses situs atau aplikasi yang belum dikenal. Hal ini membuat mereka lebih mudah menjadi sasaran ancaman seperti pencurian identitas, pembobolan akun, serta penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Generasi Z sering memanfaatkan media sosial dan platform daring untuk berkomunikasi dan berinteraksi. Namun, mereka mungkin tidak sepenuhnya menyadari sejauh mana informasi pribadi mereka dapat diakses oleh pihak lain. Ancaman seperti pencurian identitas, peretasan akun media sosial, serta penyebaran data pribadi tanpa izin merupakan permasalahan serius yang berpotensi mereka hadapi [36].

2.2.4. Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) dikembangkan untuk menjelaskan bagaimana individu memotivasi diri mereka dalam menghadapi ancaman [37]. Teori ini menyatakan bahwa keputusan seseorang untuk mengambil tindakan perlindungan dipengaruhi oleh dua proses utama, yaitu *threat appraisal* (penilaian ancaman) dan *coping appraisal* (penilaian kemampuan mengatasi ancaman). PMT sering digunakan dalam berbagai konteks, termasuk kesehatan dan keamanan informasi, karena memberikan kerangka kerja dalam memahami bagaimana individu menilai risiko dan mengambil langkah-langkah perlindungan [26].

Protection Motivation Theory (PMT) terdiri dari dua komponen utama, yaitu *threat appraisal* (penilaian ancaman) dan *coping appraisal* (penilaian cara mengatasi ancaman). Setiap komponen ini memiliki faktor-faktor yang mempengaruhi keputusan individu dalam merespons suatu ancaman.

1. *Threat Appraisal* (Penilaian Ancaman)

Threat appraisal mencakup proses kognitif yang digunakan individu untuk mengevaluasi tingkat ancaman yang dihadapi. Faktor-faktor dalam *threat appraisal* meliputi:

- a. *Perceived Severity* (Keseriusan Ancaman): Sejauh mana individu percaya bahwa ancaman tersebut memiliki konsekuensi yang serius jika tidak diatasi.
 - b. *Perceived Vulnerability* (Kerentanan terhadap Ancaman): Tingkat di mana individu merasa rentan terhadap ancaman yang ada.
2. *Coping appraisal* berkaitan dengan bagaimana individu mengevaluasi kemampuannya untuk mengatasi ancaman dan mengambil tindakan perlindungan. Faktor-faktor dalam *coping appraisal* meliputi:
- a. *Response Efficacy* (Efikasi Respons): Keyakinan individu bahwa tindakan tertentu akan efektif dalam mencegah atau mengurangi ancaman.
 - b. *Self-Efficacy* (Efikasi Diri): Seberapa yakin individu bahwa ia mampu melakukan tindakan perlindungan.
 - c. *Response Costs* (Biaya Respons): Hambatan atau biaya yang terkait dengan tindakan perlindungan, seperti waktu, usaha, atau sumber daya yang dibutuhkan.

Protection Motivation Theory (PMT) menjelaskan bahwa motivasi individu dalam menghadapi ancaman keamanan data pribadi dipengaruhi oleh dua proses utama, yaitu penilaian ancaman (*threat appraisal*) dan penilaian cara mengatasi ancaman (*coping appraisal*). Dalam *threat appraisal*, individu menilai seberapa serius ancaman tersebut dan seberapa rentan dirinya terhadap ancaman itu. Sementara itu, *coping appraisal* melibatkan keyakinan individu terhadap efektivitas tindakan perlindungan, kemampuan diri untuk melaksanakan tindakan tersebut, serta pertimbangan biaya atau hambatan yang mungkin timbul. Kombinasi dari penilaian ancaman dan kemampuan mengatasi ancaman ini menentukan sejauh mana seseorang termotivasi untuk menjaga keamanan data pribadinya.

2.3 Pengembangan Hipotesis

Protection Motivation Theory (PMT) menjelaskan bagaimana individu termotivasi untuk mengambil tindakan perlindungan ketika dihadapkan pada ancaman. Teori ini terdiri dari dua proses utama: *Threat Appraisal* (Penilaian Ancaman) dan *Coping Appraisal* (Penilaian Cara Mengatasi Ancaman). *Threat appraisal* melibatkan evaluasi terhadap tingkat bahaya dari suatu ancaman, sedangkan *coping appraisal* berfokus pada

kemampuan individu dalam mengatasi ancaman tersebut melalui tindakan perlindungan. Dalam konteks penelitian ini, PMT digunakan untuk memahami bagaimana Gen Z menilai ancaman terhadap keamanan data pribadinya di media sosial dan bagaimana mereka memutuskan untuk mengambil langkah perlindungan.

2.3.1. Pengaruh *Perceived Severity* Terhadap motivasi perlindungan data pribadi di media sosial.

Perceived Severity mengacu pada sejauh mana individu memandang suatu ancaman sebagai hal yang serius dan memiliki dampak negatif yang besar jika diabaikan. Dalam konteks perlindungan data pribadi di media sosial, jika individu menyadari bahwa kebocoran data dapat menyebabkan pencurian identitas atau penyalahgunaan informasi pribadi, maka mereka cenderung lebih termotivasi untuk melindungi data mereka [18]. Oleh karena itu, hipotesis pertama yang diajukan adalah:

H1: *Perceived Severity* berpengaruh positif dan signifikan terhadap motivasi perlindungan data pribadi di media sosial.

2.3.2. Pengaruh *Perceived Vulnerability* terhadap motivasi perlindungan data pribadi di media sosial.

Perceived Vulnerability merujuk pada sejauh mana individu merasa rentan terhadap ancaman yang ada. Dalam PMT, semakin besar persepsi individu bahwa mereka dapat menjadi korban ancaman, semakin tinggi kemungkinan mereka untuk mengambil langkah perlindungan. Dalam konteks media sosial, individu yang merasa lebih rentan terhadap pencurian data atau peretasan akun akan lebih terdorong untuk mengadopsi langkah perlindungan [38]. Oleh karena itu, hipotesis kedua yang diajukan adalah:

H2: *Perceived Vulnerability* berpengaruh positif dan signifikan terhadap motivasi perlindungan data pribadi di media sosial.

2.3.3. Pengaruh *Response Efficacy* terhadap motivasi perlindungan data pribadi di media sosial.

Response Efficacy dalam PMT mengacu pada keyakinan individu bahwa suatu tindakan perlindungan akan efektif dalam mencegah atau mengurangi ancaman. Jika

individu percaya bahwa mengaktifkan autentikasi dua faktor, mengubah kata sandi secara berkala, atau membatasi informasi yang dibagikan dapat secara efektif mencegah peretasan atau kebocoran data, maka mereka akan lebih termotivasi untuk menerapkan langkah-langkah tersebut [39]. persepsi terhadap efektivitas suatu tindakan merupakan faktor utama dalam membentuk motivasi keamanan siber seseorang. Oleh karena itu, hipotesis ketiga yang diajukan adalah:

H3: *Response Efficacy* berpengaruh positif dan signifikan terhadap motivasi perlindungan data pribadi di media sosial.

2.3.4. Pengaruh *Self-Efficacy* terhadap motivasi perlindungan data pribadi di media sosial.

Self-Efficacy adalah sejauh mana individu yakin bahwa mereka mampu melakukan tindakan perlindungan dengan efektif. Dalam PMT, individu dengan tingkat *self-efficacy* yang tinggi lebih mungkin untuk mengambil langkah-langkah keamanan karena mereka merasa mampu melakukannya. Dalam konteks perlindungan data pribadi, individu yang merasa mampu mengatur pengaturan privasi, mengenali ancaman siber, atau menggunakan teknologi keamanan akan lebih cenderung menjaga data pribadinya [38]. Individu dengan tingkat *self-efficacy* yang tinggi lebih aktif dalam menerapkan langkah-langkah keamanan siber. Oleh karena itu, hipotesis keempat yang diajukan adalah:

H4: *Self-Efficacy* berpengaruh positif dan signifikan terhadap motivasi perlindungan data pribadi di media sosial.

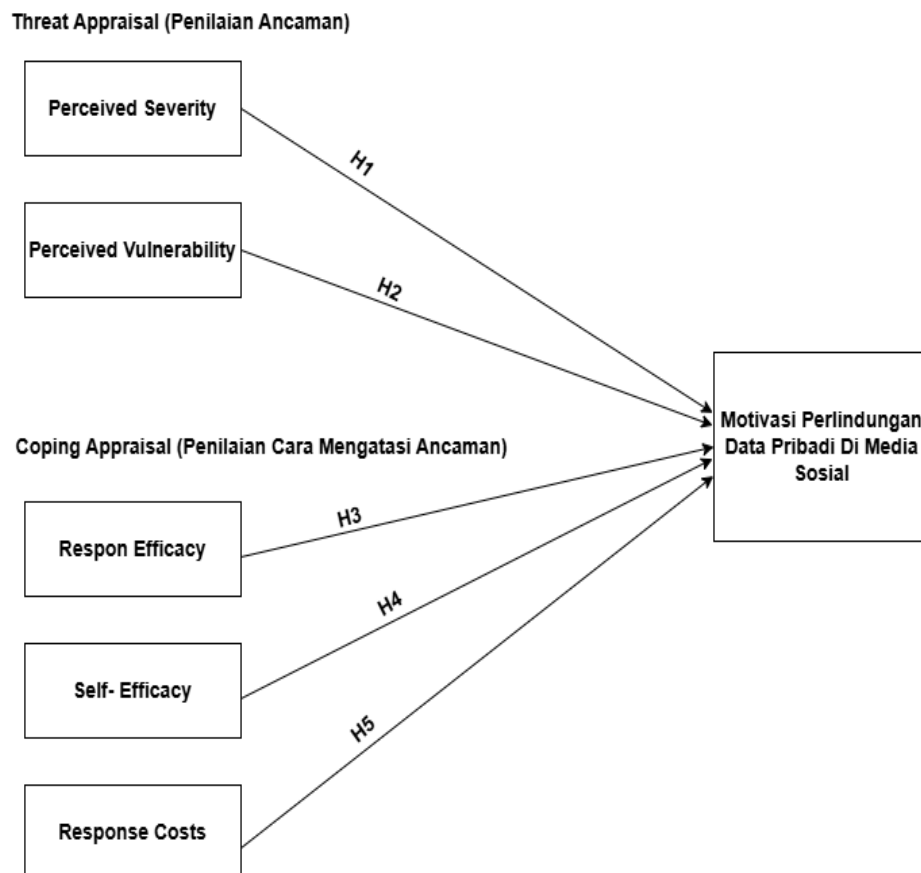
2.3.5. Pengaruh *Response Costs* terhadap motivasi perlindungan data pribadi di media sosial.

Secara umum, dalam kerangka *Protection Motivation Theory* (PMT), *response costs* memang diasumsikan dapat menurunkan kecenderungan individu untuk melakukan perilaku perlindungan. Namun, dalam konteks penelitian ini, *response costs* tidak memiliki pengaruh signifikan terhadap niat atau perilaku perlindungan, yang mungkin disebabkan oleh persepsi responden bahwa biaya yang diperlukan baik dalam bentuk waktu, usaha, maupun sumber daya tidak terlalu membebani atau tidak relevan dengan situasi mereka. Selain itu, bisa jadi responden memiliki tingkat *self-efficacy* dan

response efficacy yang cukup tinggi, sehingga mereka merasa mampu melakukan tindakan perlindungan tanpa terlalu mempertimbangkan biaya yang menyertainya. Dalam kondisi seperti ini, responden lebih fokus pada manfaat dan urgensi tindakan dibandingkan dengan hambatan atau biaya yang mungkin muncul, sehingga variabel *response costs* tidak memberikan pengaruh berarti dalam membentuk motivasi perlindungan [40]. Oleh karena itu, hipotesis kelima yang diajukan adalah:

H5: *Response Costs* tidak berpengaruh signifikan terhadap motivasi perlindungan data pribadi di media sosial.

Kerangka pemikiran menggambarkan bagaimana faktor-faktor dalam PMT mempengaruhi motivasi Generasi Z dalam menjaga keamanan data pribadi mereka. Dengan memahami mekanisme ini, penelitian ini dapat memberikan wawasan yang lebih dalam mengenai cara meningkatkan kesadaran dan tindakan perlindungan data pribadi di era digital sebagai berikut:



Gambar 2.1 Model Penelitian