BAB II
TINJAUAN PUSTAKA

A. Keamanan Digital

1. Definisi Keamanan Digital

Keamanan digital (digital security) secara konseptual merujuk pada serangkaian langkah, praktik, dan teknologi yang bertujuan melindungi informasi pribadi, identitas digital, perangkat, dan aktivitas seseorang di ruang siber dari berbagai ancaman yang tidak sah (Kayes & Iamnitchi, 2017). Dalam dimensi yang lebih luas, keamanan digital bukan hanya menyangkut perlindungan teknis berupa password atau enkripsi data, tetapi juga mencakup aspek kesadaran, pengetahuan, dan perilaku pengguna dalam menavigasi dunia digital secara aman. Sari, R. A., & Putra (2022) mendefinisikan keamanan digital sebagai kemampuan individu dan sistem untuk melindungi aset digital dari akses tidak sah, manipulasi data, penipuan, maupun penyalahgunaan informasi pribadi.

2. Tujuan Keamanan Digital

Tujuan keamanan digital mencakup tiga aspek utama yang dikenal dengan triad CIA: Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan). Dalam konteks individu khususnya remaja, keamanan digital bertujuan untuk melindungi privasi personal, menjaga identitas digital dari pembajakan atau penyalahgunaan, mencegah paparan terhadap konten berbahaya, serta melindungi diri dari berbagai bentuk kejahatan siber termasuk pelecehan virtual (Bate & Prasetyo, 2025). Aspek keamanan digital yang paling relevan bagi remaja meliputi manajemen privasi di media sosial, penggunaan autentikasi yang kuat, kewaspadaan terhadap tautan atau konten mencurigakan, serta pemahaman tentang hak digital sebagai pengguna.

3. Edukasi Keamanan Digital

Edukasi keamanan digital adalah proses terencana dan sistematis dalam mentransfer pengetahuan, keterampilan, dan nilai-nilai yang berkaitan dengan penggunaan teknologi digital secara aman, bertanggung jawab, dan etis kepada

individu atau kelompok tertentu (Zulfa Ar Rahman, 2024; Syahid et al., 2024). Lebih dari sekadar penyampaian informasi, edukasi keamanan digital merupakan upaya pemberdayaan yang bertujuan mengubah pola pikir, sikap, dan perilaku individu dalam berinteraksi dengan dunia digital. Herawati et al. (2024)menekankan bahwa edukasi digital safety yang efektif harus mampu meningkatkan kecakapan bermedia digital, yang mencakup kemampuan kognitif untuk memahami risiko, kemampuan afektif untuk merespons risiko secara tepat, dan kemampuan konatif untuk mengambil tindakan pencegahan.

Dalam kerangka Social Learning Theory (Bandura, 1977), edukasi keamanan digital bekerja melalui mekanisme observasi, imitasi, dan penguatan perilaku. Remaja belajar bukan hanya dari paparan informasi langsung, tetapi juga dari melihat bagaimana orang lain menghadapi situasi risiko digital, mengidentifikasi diri dengan model perilaku positif, dan mendapatkan penguatan melalui pengakuan atas perilaku aman yang mereka tampilkan. Oleh karena itu, materi edukasi yang efektif harus memuat contoh-contoh kasus nyata, strategi respons konkret, serta mendorong refleksi personal. Indikator keberhasilan edukasi keamanan digital meliputi: peningkatan pengetahuan tentang ancaman digital, perubahan persepsi risiko, peningkatan rasa efikasi diri dalam menghadapi ancaman, serta perubahan perilaku nyata dalam penggunaan media digital sehari-hari (Darimis et al., 2023).

B. Media Edukasi: Buku Saku Digital

Media pembelajaran adalah segala bentuk alat atau sarana yang digunakan untuk menyampaikan pesan atau informasi dalam proses belajar sehingga dapat merangsang pikiran, perasaan, perhatian, dan kemauan belajar peserta didik (Hairunisa et al., 2025). Dalam konteks edukasi kesehatan, pemilihan media yang tepat sangat menentukan efektivitas penyampaian pesan dan terbentuknya pemahaman serta perubahan sikap pada sasaran. Media yang sesuai dengan karakteristik sasaran akan meningkatkan keterlibatan, motivasi belajar, dan retensi informasi secara signifikan.

Buku saku digital (digital pocket book) adalah media edukasi berbasis digital yang menyajikan konten ringkas, padat, dan terstruktur dalam format yang

dapat diakses melalui perangkat pintar (smartphone, tablet, atau komputer). Berbeda dari buku teks konvensional, buku saku digital menggabungkan elemen teks, gambar, ikon, dan tata letak visual yang menarik untuk memudahkan pemahaman pembaca dalam waktu singkat (Bate & Prasetyo, 2025). Sari (2025) menjelaskan bahwa format digital ini memungkinkan integrasi elemen interaktif seperti navigasi bab, hyperlink, dan tampilan responsif yang menyesuaikan ukuran layar perangkat pengguna.

Kelebihan buku saku digital dibandingkan media edukasi konvensional antara lain:

a. Mudah diakses kapan saja dan di mana saja tanpa memerlukan koneksi internet yang konstan jika telah diunduh
b. Tidak memerlukan biaya cetak dan distribusi
c. Konten dapat diperbarui dengan mudah
d. Tampilan visual yang menarik meningkatkan minat baca remaja
e. Ukuran file yang kecil membuatnya tidak membebani penyimpanan perangkat
f. Selaras dengan kebiasaan belajar generasi Z yang akrab dengan konsumsi konten digital (Hairunisa et al., 2025; Bate & Prasetyo, 2025).

Keunggulan-keunggulan ini menjadikan buku saku digital sebagai media yang strategis untuk menyampaikan edukasi keamanan digital kepada remaja, yang merupakan kelompok dengan tingkat literasi digital dan adopsi teknologi tertinggi.

C. Sikap

1. Definisi Sikap

Sikap (attitude) dalam perspektif psikologi sosial didefinisikan sebagai kecenderungan atau predisposisi yang dipelajari individu untuk merespons suatu objek, orang, kejadian, atau situasi secara konsisten, baik dalam arah yang menyenangkan maupun tidak menyenangkan (Ajzen, 1991).

Sikap bukan merupakan perilaku itu sendiri, melainkan sebuah kondisi internal yang mengarahkan atau mempredisposisikan individu untuk berperilaku dengan cara tertentu. Dalam konteks penelitian ini, sikap yang dimaksud adalah kecenderungan remaja putri dalam merespons situasi yang berpotensi menjadi

pelecehan virtual, baik dari sisi pengenalan, penilaian, maupun kesiapan untuk bertindak.

Sikap memiliki tiga komponen yang saling berinteraksi dan membentuk kesatuan respons yang utuh yaitu:

a. Komponen kognitif, yaitu keyakinan dan pengetahuan individu tentang objek sikap, dalam hal ini pengetahuan tentang apa itu pelecehan virtual, bentuk-bentuknya, dan risikonya.
b. Komponen afektif, yaitu perasaan atau emosi yang dihubungkan dengan objek sikap, misalnya rasa tidak nyaman, takut, atau marah ketika menghadapi atau menyaksikan pelecehan virtual.
c. Komponen konatif, yaitu kecenderungan untuk bertindak atau berperilaku tertentu terhadap objek sikap, seperti kesiapan untuk melaporkan, menolak, atau mencari bantuan ketika menghadapi pelecehan virtual (Espelage et al., 2023).

Ketiga komponen ini saling memperkuat dan secara bersama-sama menentukan arah dan kekuatan sikap seseorang.

2. Faktor yang Mempengaruhi Pembentukan & Perubahan Sikap

Faktor-faktor yang mempengaruhi pembentukan dan perubahan sikap meliputi pengalaman langsung, informasi yang diterima melalui media, pengaruh orang-orang yang signifikan (significant others), serta konteks sosial dan budaya tempat individu berkembang (Wright, 2017).

Dalam Theory of Planned Behavior (Ajzen, 1991), sikap bersama-sama dengan norma subjektif dan persepsi kontrol perilaku membentuk niat, yang kemudian memprediksi perilaku aktual. Implikasi dari teori ini adalah bahwa intervensi edukasi yang berhasil mengubah komponen kognitif dan afektif sikap akan secara tidak langsung menggerakkan perubahan perilaku preventif pada remaja putri.

D. Pelecehan Virtual

1. Definisi Pelecehan Virtual

Pelecehan virtual atau cyber harassment adalah segala bentuk perilaku yang disengaja, berulang, dan bersifat merugikan yang dilakukan melalui media elektronik atau platform digital, dengan tujuan membuat target merasa terancam, direndahkan, dipermalukan, atau tidak aman (Kowalski & Wingate, 2023). Definisi ini mencakup spektrum perilaku yang luas, mulai dari cyberbullying, sexting tidak diinginkan, grooming digital, doxing (penyebaran informasi pribadi tanpa izin), hingga non-consensual intimate image sharing (NCIIS) atau yang populer disebut revenge porn (Cheng et al., 2015; Organization, 2022).

2. Jenis-Jenis Pelecehan Virtual

Jenis-jenis pelecehan virtual yang paling sering dialami remaja putri meliputi:

a. Pelecehan berbasis teks, yaitu pengiriman pesan, komentar, atau kata-kata kasar, merendahkan, atau mengancam melalui media sosial, aplikasi pesan, atau email
b. Pelecehan berbasis visual, yaitu pengiriman gambar atau video pornografi yang tidak diminta, atau permintaan untuk mengirimkan foto/video intim
c. Pelecehan berbasis identitas, yaitu peniruan identitas korban (impersonation) untuk merusak reputasi
d. Stalking siber, yaitu pemantauan atau pengawasan aktivitas online korban secara obsesif dan menimbulkan rasa tidak aman
e. Grooming digital, yaitu pendekatan manipulatif oleh orang dewasa kepada remaja dengan tujuan eksploitasi seksual (Smith & Livingstone, 2017; Espelage et al., 2023).

3. Dampak Pelecehan Virtual

Dampak pelecehan virtual terhadap kesehatan mental remaja putri sangat signifikan dan multidimensional. Korban pelecehan virtual berisiko mengalami depresi, kecemasan, gangguan tidur, penurunan prestasi akademik, isolasi sosial, dan dalam kasus yang parah dapat berujung pada ideasi atau percobaan bunuh diri (Organization, 2022; Gaffney et al., 2019).

Dina (2025) dalam perspektif psikologi humanistik menegaskan bahwa pelecehan online menyerang kebutuhan dasar manusia akan rasa aman dan penghargaan, sehingga dampaknya bukan hanya pada kondisi psikologis jangka pendek tetapi juga pada pembentukan identitas diri remaja secara keseluruhan. Inilah yang menjadikan pencegahan pelecehan virtual melalui peningkatan sikap preventif sebagai prioritas kesehatan remaja yang tidak bisa diabaikan.

Pencegahan pelecehan virtual memerlukan pendekatan multilapis yang melibatkan individu, keluarga, sekolah, dan komunitas. Di tingkat individu, pengembangan sikap preventif melalui literasi digital dan keamanan digital merupakan lini pertama yang paling efektif (Finkelhor et al., 2021). Remaja yang memiliki pengetahuan tentang bentuk-bentuk pelecehan virtual, cara melindungi privasi digital, dan prosedur pelaporan akan memiliki kapasitas yang lebih besar untuk menghindari atau merespons situasi pelecehan secara tepat. Sari (2025) juga menekankan pentingnya penggunaan autentikasi dua faktor (2FA) dan pengaturan privasi yang ketat pada akun media sosial sebagai langkah teknis pencegahan pelecehan virtual.

E. Remaja Putri

Remaja (adolescent) merupakan periode perkembangan manusia yang ditandai oleh transisi dari masa kanak-kanak menuju dewasa, umumnya berlangsung antara usia 10 hingga 19 tahun (World Health Organization, 2021). Periode ini ditandai oleh perubahan fisik, psikologis, dan sosial yang signifikan, termasuk perkembangan identitas diri, perluasan jaringan sosial, dan peningkatan otonomi dari orang tua (Espelage et al., 2023). Karakteristik remaja yang relevan dengan konteks penelitian ini antara lain: tingginya rasa ingin tahu dan eksperimentasi, kebutuhan untuk diakui oleh teman sebaya, kecenderungan untuk berbagi informasi personal di media sosial, serta kemampuan penilaian risiko yang belum sepenuhnya matang.

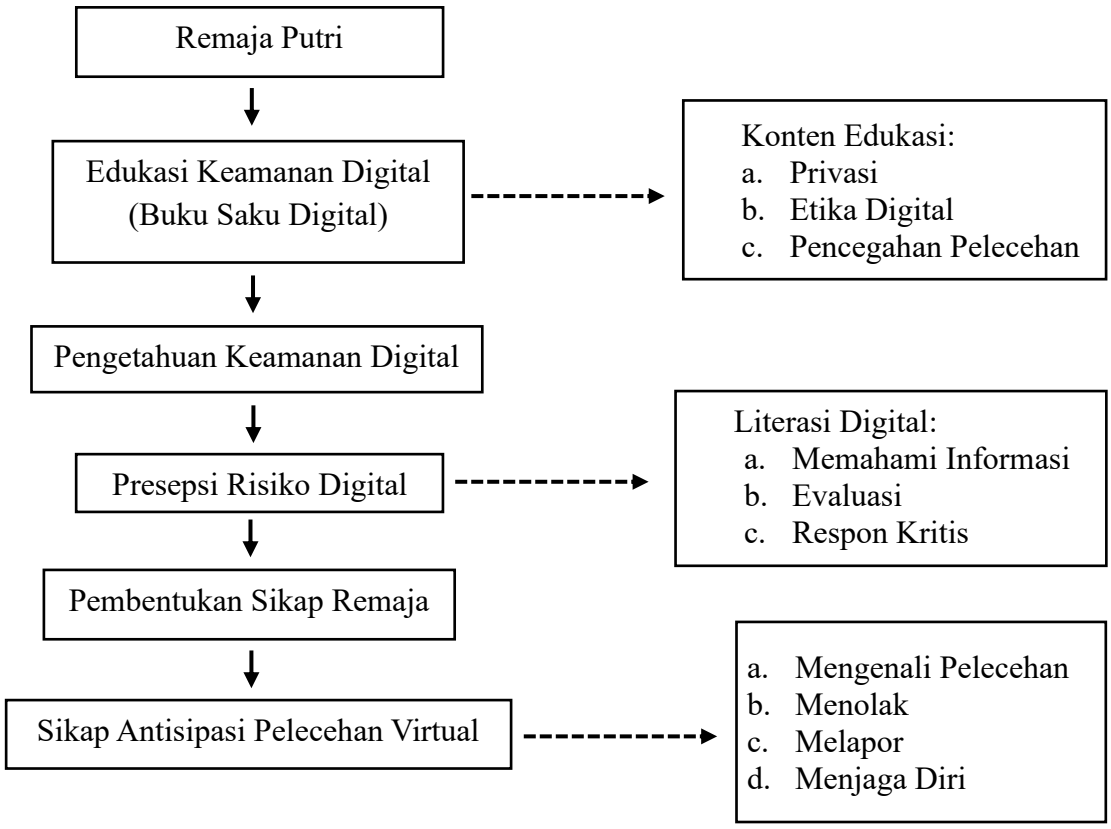
Remaja putri dalam konteks digital menghadapi tantangan yang lebih spesifik dibandingkan remaja laki-laki. Norma gender yang berlaku di masyarakat seringkali menempatkan perempuan pada posisi yang lebih rentan dalam interaksi digital, baik karena stereotip tentang peran gender yang dimainkan persis seperti di

dunia nyata, maupun karena remaja putri cenderung lebih aktif dalam berbagi konten personal di media sosial (Wright, 2017).

Kerentanan remaja putri terhadap pelecehan virtual juga diperkuat oleh kecenderungan untuk mempertahankan harmoni sosial, sehingga mereka seringkali tidak segera merespons atau melaporkan pelecehan yang dialami karena takut mengganggu hubungan pertemanan atau mendapatkan penilaian negatif dari lingkungan (Dina, 2025). Dalam konteks MTsN 3 Medan, siswi kelas VIII berada pada rentang usia 13–15 tahun, yang merupakan usia dengan kerentanan tertinggi terhadap pelecehan virtual berdasarkan data epidemiologis yang ada.

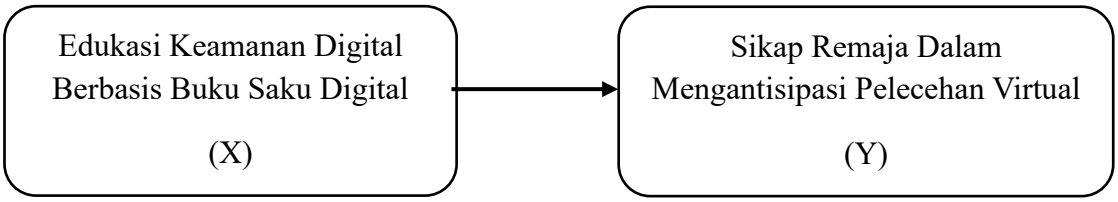
F. Kerangka Teori

Penelitian ini didasarkan pada Theory of Planned Behavior, Social Learning Theory, dan Teori Literasi Digital yang menjelaskan bahwa edukasi keamanan digital dapat membentuk sikap dan perilaku remaja putri dalam mencegah pelecehan virtual.



Gambar 2.1 Kerangka Teori

G. Kerangka Konseptual



Gambar 2.2 Kerangka Konseptual

H. Hipotesis

Berdasarkan uraian teoritis dan empiris yang telah dikemukakan, hipotesis penelitian dirumuskan sebagai berikut:

H_0 (Hipotesis Nol): Tidak terdapat pengaruh yang signifikan dari pemberian edukasi keamanan digital berbasis buku saku digital terhadap sikap remaja putri dalam mengantisipasi pelecehan virtual di MTsN 3 Medan Tahun 2026.

H_1 (Hipotesis Alternatif): Terdapat pengaruh yang signifikan dari pemberian edukasi keamanan digital berbasis buku saku digital terhadap sikap remaja putri dalam mengantisipasi pelecehan virtual di MTsN 3 Medan Tahun 2026.