JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 4, No. 2, Mei 2025, pp. 162 - 174
p-ISSN: 2803-1507 (media cetak) | e-ISSN: 2803-1531 (media online)
*Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/134*

# The Role of Digital Education in Protecting User Privacy and Preventing Social Impact

**Amelia Salsabisa Hakim*[1], Putri Jihan Mustaqim[2], Atha Naufal Karom[3]**
[1,2,3] UIN Sulthan Thaha Saifuddin Jambi
Jl. Jambi - Muara Bulian No.KM. 16, Simpang Sungai Duren, Kec. Jambi Luar Kota, Kabupaten Muaro Jambi, Jambi 36361
e-mail*[1]: ameeell2002@gmail.com

**ARTICLE INFO**

Article History:

Received: 20 Maret 2025
Revised: 30 Maret 2025
Accepted: 15 April 2025
Published: 21 Mei 2025

**ABSTRACT**

*In the digital era, personal data protection has become a crucial issue due to the growing risks of privacy breaches. This study aims to explore the role of digital education in enhancing privacy literacy and mitigating the social impacts of data violations. Utilizing a mixed-methods approach, primary data was collected through online surveys and in-depth interviews with users and experts, while secondary data was analyzed from academic journals and industry reports. Results reveal that only 42.7% of respondents understood how to safely manage their personal information, reflecting a significant gap in privacy awareness. Moreover, a positive correlation (R = 0.72) was identified between improved privacy literacy and reduced social risks, such as identity theft and cyberbullying. Simulations proved to be effective educational tools, with every 10% increase in digital privacy literacy reducing social risks by 7%. The findings highlight the need for integrating privacy education into formal curricula at all educational levels, complemented by community-based initiatives for underserved populations. Collaborative efforts between governments, educational institutions, and technology organizations are essential to develop relevant and effective learning resources. The study underscores the importance of adopting holistic educational strategies to empower individuals in navigating the challenges of data protection in the digital age.*

**Keywords:** *Digital Privacy Literacy, Data Protection, Cybersecurity Education, Social Risk Mitigation, Privacy Awarenesst.*

**Abstrak**

Di era digital, perlindungan data pribadi telah menjadi isu krusial akibat meningkatnya risiko pelanggaran privasi. Studi ini bertujuan untuk mengeksplorasi peran pendidikan digital dalam meningkatkan literasi privasi dan mengurangi dampak sosial dari pelanggaran data. Dengan menggunakan pendekatan metode campuran, data primer dikumpulkan melalui survei online dan wawancara mendalam dengan pengguna serta para ahli, sementara data sekunder dianalisis dari jurnal akademik dan laporan industri. Hasil penelitian menunjukkan bahwa hanya 42,7% responden yang memahami cara mengelola informasi pribadi mereka dengan aman, mencerminkan adanya kesenjangan signifikan dalam kesadaran privasi. Selain itu, ditemukan korelasi positif (R = 0,72) antara peningkatan literasi privasi dan penurunan risiko sosial, seperti pencurian identitas dan perundungan daring. Simulasi terbukti menjadi alat edukasi yang efektif, di mana setiap

DOI: https://doi.org/10.51903/k9cvkc90

p-ISSN: 2803-1507 e-ISSN: 2803-1531

peningkatan 10% dalam literasi privasi digital mampu mengurangi risiko sosial sebesar 7%. Temuan ini menyoroti perlunya integrasi pendidikan privasi ke dalam kurikulum formal di semua jenjang pendidikan, yang dilengkapi dengan inisiatif berbasis komunitas untuk populasi yang kurang terlayani. Upaya kolaboratif antara pemerintah, institusi pendidikan, dan organisasi teknologi sangat penting untuk mengembangkan sumber belajar yang relevan dan efektif. Studi ini menegaskan pentingnya strategi pendidikan holistik untuk memberdayakan individu dalam menghadapi tantangan perlindungan data di era digital.
**Kata Kunci**: *Digital Privacy Literacy, Data Protection, Cybersecurity Education, Social Risk Mitigation, Privacy Awarenesst.*

## 1. PENDAHULUAN

Di era digital ini, informasi pribadi pengguna media sosial menjadi aset berharga yang sering dieksploitasi untuk keuntungan finansial dan tujuan tidak etis. Dengan lebih dari 5,3 miliar pengguna internet aktif di seluruh dunia sehingga risiko pelanggaran privasi meningkat signifikan, termasuk lonjakan pelanggaran data populasi dunia hingga 66% dalam dekade terakhir [1]. Platform digital seperti media sosial dan e-commerce memfasilitasi pengumpulan data yang luas, tetapi juga meningkatkan kerentanan terhadap ancaman siber. Penelitian ini menunjukkan bahwa individu dengan literasi digital tinggi lebih mampu mengidentifikasi dan menghindari risiko terhadap data pribadi [2]. Pendidikan mengenai perlindungan data pribadi dan keamanan siber sangat krusial, dan kerjasama antara pemerintah serta lembaga pendidikan dapat memperkuat literasi privasi digital sebagai bagian penting dari sistem pendidikan untuk mengurangi risiko kebocoran data.

Rendahnya pemahaman masyarakat mengenai perlindungan data pribadi berkontribusi pada meningkatnya kasus penyalahgunaan data di seluruh dunia. Pengguna internet tidak mengetahui bagaimana data mereka diproses oleh platform digital yang mereka gunakan, menciptakan celah bagi penyalahgunaan data. Menurut [3], 50,79% perusahaan di Amerika Serikat mengakui bahwa mereka mengalami kebocoran data secara kolektif akibat kesalahan pengguna, termasuk pengguna kata sandi yang lemah dan kurangnya pelatihan keamanan. Dampak dari situasi ini dapat berujung pada masalah sosial serius, termasuk penipuan identitas, pencurian finansial, dan tekanan psikologis akibat eksploitasi data sensitif. Dalam konteks ini, literasi digital menjadi sangat penting; penelitian menunjukkan bahwa individu dengan literasi digital yang baik lebih mampu mengenali dan menghindari risiko terhadap data pribadi mereka. Menurut [4] ; [5] and [6] literasi digital mencakup pemahaman tentang cara melindungi informasi pribadi, penggunaan kata sandi yang kuat, dan pengelolaan izin aplikasi. Oleh karena itu, peningkatan literasi digital perlu menjadi prioritas untuk melindungi data pribadi dan mengurangi risiko kebocoran informasi di era digital ini [7] [8] and [9]. Hal ini juga memerlukan kerjasama antara pemerintah dan institusi pendidikan untuk secara luas dan efektif menyebarkan pengetahuan tentang perlindungan data pribadi [10]. Penelitian ini bertujuan untuk mengeksplorasi dan mengidentifikasi peran pendidikan digital dalam meningkatkan literasi privasi pengguna serta mengurangi dampak sosial yang diakibatkan oleh pelanggaran data. Dengan mengadopsi pendekatan pendidikan yang menyeluruh, penelitian ini juga berupaya mengembangkan model pembelajaran yang efektif untuk memberikan pengguna pengetahuan dan keterampilan praktis dalam melindungi privasi mereka.

Meskipun banyak penelitian yang membahas kebijakan privasi dan teknologi keamanan, penelitian oleh [11] menyatakan bahwa masih sedikit yang menekankan peran pendidikan digital sebagai alat pencegahan untuk melindungi privasi pengguna. Sebagian besar literatur lebih berfokus pada solusi teknologi seperti enkripsi dan firewall, sementara aspek edukasi, terutama yang ditujukan kepada masyarakat umum, kurang mendapat perhatian. Padahal, pendidikan memiliki potensi besar untuk meningkatkan kesadaran pengguna mengenai risiko privasi dan memperkuat perilaku digital [12]. Penelitian ini memberikan kontribusi pada literatur dengan menyajikan perspektif baru mengenai bagaimana pendidikan digital dapat berperan sebagai ekosistem holistik dalam melindungi privasi pengguna dan mengurangi dampak sosial. Menurut [13] and [14], pendekatan yang diusulkan mengintegrasikan teknologi pendidikan dengan prinsip-prinsip literasi digital, menawarkan wawasan inovatif bagi pembuat kebijakan dan pengembang platform digital. Selain itu, penelitian ini memperkenalkan kerangka evaluasi untuk menilai keberhasilan pendidikan digital yang berfokus pada privasi, yang dapat disesuaikan dengan berbagai konteks budaya dan geografis.

## 2. TINJAUAN PUSTAKA

### 2.1. *Pendidikan Digital untuk Privasi*

Pendidikan digital sekarang ini merupakan bagian integral dari proses transformasi digital, dengan fokus utamanya pada meningkatkan kesadaran publik akan isu privasi data. Memahami cara mengelola informasi

p-ISSN: 2803-1507 e-ISSN: 2803-1531

pribadi dan risiko kecurangan atau penyalahgunaan data oleh pihak lain adalah hal yang sangat penting. Menurut [15] and [16] pendidikan digital tidak hanya berfokus pada penguasaan alat teknologi, tetapi juga harus membekali individu dengan pengetahuan untuk berpartisipasi secara etis di dunia maya. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mewajibkan pemenuhan kewajiban paling lambat pada Oktober 2024. Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi sesuai dengan UU PDP [17]. Hal ini menjadi sangat relevan mengingat meningkatnya risiko kebocoran data dan penyalahgunaan informasi pribadi. Namun, rata-rata indeks literasi digital remaja Indonesia adalah 4,15, yang menunjukkan tingkat literasi digital yang cukup tinggi, ini juga mengindikasikan bahwa semakin mahir seseorang dalam teknologi digital, semakin besar risiko yang mereka hadapi di dunia maya [18]. Hal ini menegaskan perlunya peningkatan kesadaran dan langkah konkret untuk melindungi data pribadi. Generasi muda, yang aktif menggunakan internet dan perangkat digital, perlu pendidikan formal tentang keamanan data dan privasi, terutama dalam pembelajaran daring dan media sosial, yang harus diintegrasikan ke dalam kurikulum. Hal ini dapat dilakukan melalui metode interaktif yang melibatkan simulasi situasi nyata dan penggunaan alat privasi *DuckDuckGo* dapat digunakan untuk mengajarkan masyarakat cara melindungi diri dari ancaman siber [19]. Selain itu, pemerintah perlu memastikan penegakan UU PDP dan menyelesaikan peraturan turunan yang diperlukan agar perlindungan data pribadi dapat lebih optimal, sehingga masyarakat Indonesia dapat lebih siap menghadapi tantangan di era digital saat ini [20].

Privasi pengguna di dunia digital sangat rentan terhadap pelanggaran. Menurut laporan Global Web Index pada tahun 2023, terjadi peningkatan dalam pelanggaran privasi selama dua tahun terakhir, dengan sebagian besar insiden terjadi melalui platform media sosial [21]. Kebiasaan berbagi informasi secara berlebihan, terutama di kalangan generasi muda, membuka peluang bagi pelaku kejahatan siber untuk mengeksploitasi data pribadi mereka. Penelitian oleh [22], menunjukkan bahwa 42,7% siswa menyadari pentingnya menjaga privasi, sementara 60,7% siswa mengabaikan hal tersebut. Hal ini menciptakan kesenjangan signifikan antara kesadaran dan tindakan yang perlu diatasi melalui pendidikan yang lebih efektif.

Dampak sosial dari teknologi digital sangat signifikan dan tidak dapat diabaikan, dengan masalah seperti penyebaran informasi palsu, *cyberbullying*, dan polarisasi sosial menjadi ancaman nyata bagi kesejahteraan masyarakat. Menurut penelitian [23] lebih dari 61,8% pengguna media sosial di Indonesia menghabiskan lebih dari 3 jam setiap hari di platform online, yang dapat mengurangi kualitas interaksi sosial dan meningkatkan risiko masalah kesehatan mental, seperti kecemasan dan depresi. Meskipun teknologi memudahkan komunikasi dan akses informasi, penggunaan yang berlebihan dapat menyebabkan isolasi sosial, di mana individu merasa terputus dari interaksi langsung dengan orang lain. Oleh karena itu, pendidikan digital perlu mencakup topik-topik ini untuk memberikan pemahaman yang lebih komprehensif tentang dampak teknologi terhadap kehidupan sosial serta bagaimana individu dapat berkontribusi pada lingkungan digital yang lebih aman dan bertanggung jawab. Penelitian oleh [24] kurikulum pendidikan harus mencakup keterampilan teknis, etika digital, dan kesadaran akan risiko privasi, serta membekali siswa dengan pengetahuan untuk mengenali informasi palsu dan menangani *cyberbullying*. Pendekatan berbasis komunitas juga penting untuk meningkatkan kesadaran sosial tentang penggunaan teknologi yang sehat dan bertanggung jawab.

Meningkatkan kesadaran risiko privasi di kalangan pengguna, terutama generasi muda, memerlukan pendekatan interaktif yang menyeluruh. Program pendidikan harus mencakup simulasi situasi nyata agar siswa belajar melindungi data mereka dari ancaman siber. Menurut [25] & [26] menunjukkan bahwa kesadaran digital mahasiswa masih rendah, meskipun mereka memahami pentingnya menjaga privasi. Pemanfaatan mesin pencari yang menghormati privasi pengguna juga penting dalam strategi pendidikan ini. Selain itu, literasi digital yang baik, termasuk etika digital dan pengelolaan informasi pribadi, sangat diperlukan untuk membekali individu dengan pengetahuan dan keterampilan dalam menciptakan lingkungan digital yang aman dan bertanggung jawab.

### **2.2.** *Communication Privacy Management (CPM) dan Literasi Digital untuk Privasi*

Manajemen Privasi Komunikasi (CPM) dikembangkan untuk memberikan kerangka dalam memahami bagaimana individu mengelola informasi pribadi [27]. Penelitian oleh [28] menunjukkan bahwa individu membuat keputusan mengenai informasi yang ingin dibagikan atau disembunyikan berdasarkan penilaian risiko dan manfaat. Dalam konteks pendidikan digital, teori ini relevan untuk melatih individu dalam melindungi privasi mereka dengan menekankan bahwa privasi melibatkan negosiasi dan pengaturan batas antara individu dan pihak lain terkait informasi yang dibagikan. Selain itu, penelitian ini mengusulkan lima

p-ISSN: 2803-1507 e-ISSN: 2803-1531

prinsip dasar untuk membantu individu mengelola privasi: hak untuk mengontrol informasi pribadi, penerapan aturan privasi, kepemilikan bersama informasi ketika diakses oleh orang lain, perlunya negosiasi antar *co-owner*, dan potensi konflik jika negosiasi tidak berhasil [29]. Memahami penelitian ini sangat penting dalam merancang program pendidikan yang efektif untuk meningkatkan kesadaran privasi di kalangan pengguna teknologi, termasuk simulasi situasi nyata dan penggunaan alat yang menghargai privasi pengguna.

Menurut [30] dan [31] literasi digital menekankan pentingnya kemampuan mahasiswa dalam mengakses, menganalisis, dan mengevaluasi informasi yang bersifat digital. Literasi digital menjadi dasar pendidikan digital dan sangat penting untuk membedakan informasi yang benar dari yang salah. Menurut [32] orang dewasa merasa terjebak oleh banyaknya informasi yang tersedia secara online dan kesulitan dalam mengidentifikasi sumber informasi yang dapat diandalkan. Ini menekankan pentingnya pendidikan digital yang mencakup pelatihan dalam mengevaluasi sumber informasi dan mengenali berita palsu. Kemampuan literasi digital terdiri dari lima kompetensi inti: akses, analisis dan evaluasi, produksi, kolaborasi, serta tanggung jawab sosial [33]. Akses mencakup kemampuan untuk mencari dan menggunakan media digital; analisis dan evaluasi melibatkan pemahaman serta penilaian kualitas informasi; produksi berfokus pada penciptaan konten; kolaborasi menekankan kerja sama dalam berbagi pengetahuan; dan tanggung jawab sosial berkaitan dengan etika dalam penggunaan media digital. Selain itu, meningkatnya kompleksitas informasi di era digital, penting bagi program pendidikan untuk mengintegrasikan pelatihan literasi digital yang komprehensif agar individu dapat menggunakan informasi dengan bijaksana dan berpartisipasi aktif dalam masyarakat yang lebih terinformasi.

Mengintegrasikan CPM dan literasi digital ke dalam kurikulum pendidikan dapat memberikan individu pengetahuan dan keterampilan untuk menavigasi dunia digital dengan aman serta melindungi privasi mereka. Pendidikan yang efektif harus mencakup simulasi situasi nyata di mana siswa dapat belajar melindungi data mereka dari ancaman siber, serta menggunakan alat yang menghargai privasi pengguna [34]. Dengan membekali individu dengan keterampilan ini, kita dapat menciptakan masyarakat yang lebih sadar akan pentingnya privasi data dan dampak sosial dari teknologi, sehingga mereka lebih siap menghadapi tantangan di era digital saat ini.

### 2.3. *Pendidikan Digital untuk Privasi dan Dampak Sosial*

Privasi pengguna di era digital menjadi isu penting seiring meningkatnya risiko pelanggaran data. Penelitian oleh [35] menunjukkan bahwa rendahnya kesadaran privasi dapat meningkatkan kemungkinan pelanggaran data pribadi, sementara [36] menemukan bahwa banyak pengguna tidak memahami bagaimana data mereka digunakan, membuat mereka merasa tidak berdaya dalam melindungi informasi pribadi. Data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa tingkat penetrasi internet di Indonesia mencapai 77% pada tahun 2021 hingga 2022 di antaranya merupakan kebocoran data [37]. Selain itu, penggunaan Internet of Things (IoT) menambah tantangan dalam perlindungan data karena semakin banyak perangkat terhubung yang meningkatkan risiko kebocoran [38]. Oleh karena itu, pendidikan literasi digital yang mencakup pelatihan dalam mengevaluasi sumber informasi dan mengenali berita palsu sangat penting untuk meningkatkan kesadaran tentang privasi.

Penelitian oleh [39] menunjukkan bahwa program pendidikan digital yang terintegrasi dalam kurikulum sekolah dapat meningkatkan kesadaran privasi di kalangan remaja setelah dilakukan intervensi. Selain itu, [40] menemukan bahwa pelatihan guru tentang literasi digital secara signifikan meningkatkan pemahaman siswa tentang etika digital dan tanggung jawab penggunaan teknologi. Selain itu, penting untuk merancang kurikulum yang tidak hanya mengajarkan keterampilan teknis, tetapi juga memberikan pemahaman tentang hak-hak privasi dan cara melindungi data pribadi. Penelitian oleh [41] menunjukkan bahwa pendidikan harus menjadi komponen penting dalam strategi perlindungan privasi, membekali individu dengan keterampilan untuk menjelajahi dunia digital secara aman dan bertanggung jawab, serta mengurangi risiko penyalahgunaan data pribadi.

Dampak sosial dari teknologi digital sangat signifikan, terutama terkait dengan fenomena seperti filter *bubble* dan *cyberbullying*. Menurut [42] and [43] menunjukkan bahwa algoritma di platform media sosial dapat memperkuat bias informasi dan berkontribusi pada polarisasi sosial, di mana individu hanya terpapar pada sudut pandang yang sejalan dengan keyakinan mereka. Selain itu, studi oleh [44] menyoroti dampak negatif *cyberbullying* terhadap kesehatan mental remaja, yang semakin diperburuk oleh penggunaan media sosial yang tidak bijaksana. Data dari Komisi Perlindungan Anak Indonesia menunjukkan bahwa sekitar 25% anak-

p-ISSN: 2803-1507 e-ISSN: 2803-1531

anak dan remaja di Indonesia mengalami *bullying* online sejak tahun 2011 hingga 2014, yang dapat menyebabkan masalah kesehatan mental seperti kecemasan dan depresi [45]. Oleh karena itu, penting bagi program pendidikan untuk fokus tidak hanya pada literasi privasi, tetapi juga pada dampak sosial dari teknologi. Membangun kesadaran tentang risiko dan tanggung jawab dalam penggunaan teknologi akan membantu individu berpartisipasi secara lebih etis di dunia maya, menciptakan lingkungan digital yang lebih aman dan mendukung pengembangan keterampilan kritis dalam mengevaluasi informasi.

## 3. METODOLOGI PENELITIAN

### 3.1 *Data Penelitian*

Data primer diperoleh melalui survei online yang dilakukan terhadap pengguna digital, terutama peserta platform pendidikan untuk orang dewasa yang lebih tua, memberikan gambaran tentang tingkat literasi digital dan pemahaman privasi data di kalangan generasi muda [46]. Survei ini mencakup pertanyaan tentang kebiasaan online, kesadaran akan keamanan data, dan pengalaman terkait pelanggaran privasi. Selain itu, wawancara mendalam dengan pakar privasi digital, pengembang platform edukasi, dan pendidik memberikan wawasan lebih dalam mengenai tantangan serta solusi dalam meningkatkan literasi digital. Metode pengumpulan data lainnya termasuk diskusi kelompok terarah yang melibatkan siswa dan pendidik untuk membahas hubungan antara pendidikan digital dan privasi data serta dampak sosial dari pelanggaran privasi.

Data sekunder digunakan untuk melengkapi analisis dan memberikan konteks yang lebih luas, dengan sumber yang mencakup artikel jurnal dan laporan industri, data dari organisasi internasional, serta studi kasus. Penelitian sebelumnya dan laporan industri dianalisis untuk memperoleh wawasan terbaru tentang tren dalam pendidikan digital dan privasi data, termasuk peningkatan global dalam pelanggaran privasi yang menunjukkan urgensi isu ini. Laporan dari UNESCO membantu memahami adopsi teknologi pendidikan dan dampaknya terhadap perlindungan privasi [47]. Selain itu, studi kasus mengenai pelanggaran data di institusi pendidikan memberikan contoh konkret tentang risiko yang dihadapi pengguna teknologi pendidikan. Penggabungan data primer dan sekunder memungkinkan penelitian ini untuk memahami fenomena secara teoritis dan menghasilkan wawasan empiris yang mendalam, serta mengidentifikasi celah dalam praktik pendidikan digital dan merumuskan rekomendasi kebijakan yang relevan.

### 3.2 *Teknik Penelitian*

Penelitian ini mengadopsi pendekatan campuran (*mixed-method*) untuk memberikan pemahaman yang mendalam dan komprehensif tentang literasi privasi digital di kalangan pengguna. Pendekatan ini terdiri dari dua komponen utama: kuantitatif dan kualitatif. Dalam aspek kuantitatif, survei sistematis akan dilaksanakan untuk mengukur tingkat literasi privasi digital, dengan fokus pada pemahaman pengguna mengenai kebijakan privasi dan praktik perlindungan data yang tepat. Survei ini akan mencakup berbagai pertanyaan yang dirancang untuk mengeksplorasi pengetahuan responden tentang hak-hak privasi mereka, serta pengalaman mereka terkait pelanggaran data. Data yang diperoleh akan dianalisis menggunakan teknik *Descriptive Statistics* untuk menggambarkan distribusi dan tren dalam literasi privasi. Selain itu, analisis Korelasi dan Regresi akan dilakukan untuk mengevaluasi hubungan antara tingkat literasi privasi digital dengan penurunan risiko dampak sosial, seperti *cyberbullying* dan penyalahgunaan data pribadi. Pendekatan ini bertujuan untuk memberikan gambaran yang lebih jelas mengenai faktor-faktor yang mempengaruhi keamanan digital individu dan bagaimana literasi dapat berkontribusi pada perlindungan diri di dunia maya.

Di sisi kualitatif, penelitian ini menggali sudut pandang pengguna serta pakar melalui wawancara mendalam dan diskusi kelompok terfokus (*focus group discussions*). Melalui metode ini, peneliti akan mendapatkan wawasan tentang persepsi pengguna terhadap pentingnya pendidikan digital dalam meningkatkan kesadaran privasi dan keamanan informasi. Data kualitatif ini akan dianalisis menggunakan *Content Analysis* untuk menilai materi pendidikan digital terkait privasi, termasuk kurikulum yang diterapkan di lembaga pendidikan dan program pelatihan yang ditawarkan oleh platform edukasi. Dengan mengintegrasikan hasil dari kedua pendekatan tersebut, penelitian ini tidak hanya berfokus pada pengukuran literasi privasi digital tetapi juga pada pemahaman konteks sosial dan budaya.

### 3.3 *Pemrosesan dan Analisis Data*

Pemrosesan data dalam penelitian ini dilakukan secara sistematis dan metodologis untuk menjamin akurasi dan keandalan hasil. Langkah-langkah tersebut mencakup beberapa elemen penting yang saling mendukung. Pertama, koding kualitatif dilakukan dengan mengkategorikan data wawancara menggunakan analisis

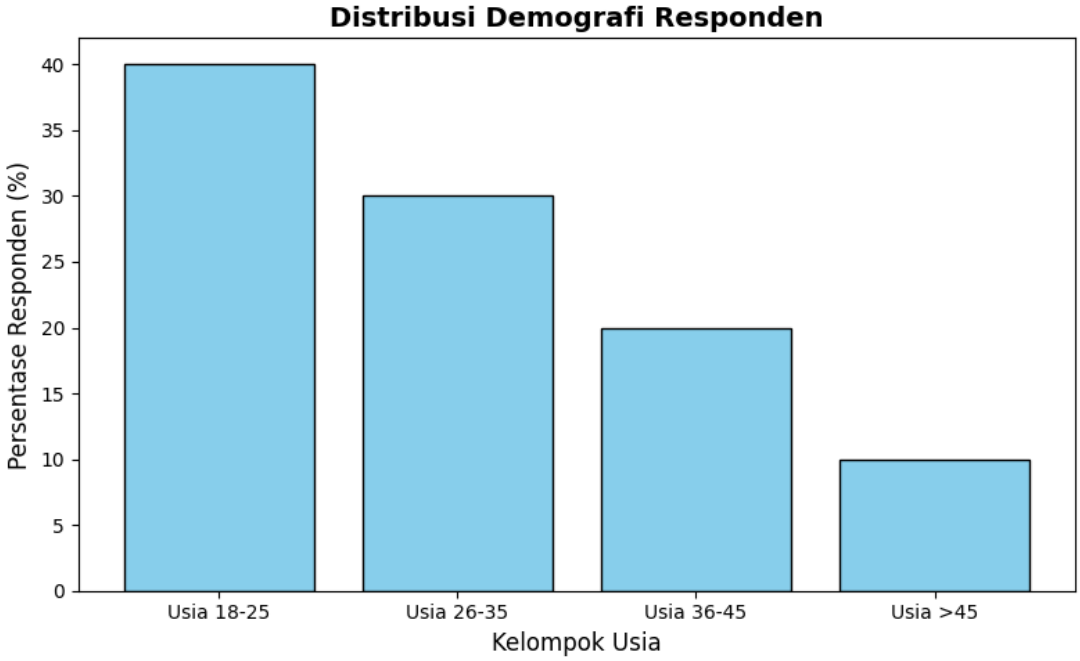
p-ISSN: 2803-1507 e-ISSN: 2803-1531

tematik berbasis *framework analysis*. Metode ini memungkinkan peneliti untuk mengorganisir dan menginterpretasikan data kualitatif dengan cara yang terstruktur dan terarah. Dalam *framework analysis*, data dari wawancara dibagi menjadi unit-unit analisis yang lebih kecil dan kemudian dikelompokkan ke dalam kategori-kategori yang telah ditentukan sebelumnya sesuai dengan tujuan penelitian. Proses ini tidak hanya membantu dalam mengidentifikasi pola dan tema utama dalam respons partisipan, tetapi juga memberikan pemahaman tentang nuansa dan konteks di balik jawaban mereka. Dengan pendekatan ini, peneliti dapat lebih mendalam mengeksplorasi persepsi pengguna terhadap privasi digital serta tantangan yang mereka hadapi dalam menjaga informasi pribadi mereka. Tabel 1 memberikan penjelasan tentang analisis teknik data.

**Tabel 1.** Teknik Analisis Data

| Jenis Data | Teknik Data | Tujuan Analisis |
|---|---|---|
| Kuantitatif | Statistik Deskriptif | Menggambarkan karakterisik responden. |
| Kualitatif | Analisis Tematik | Mengidentifikasi pola dan tema utama dalam data wawancara. |
| Kuantitatif | Korelasi | Menentukan hubungan antar variabel. |
| Kualitatif | Framework Analysis | Mengorganisir data berdasarkan kerangka kerja teoritis. |

Analisis statistik dilakukan untuk mengolah data survei menggunakan perangkat lunak R. Analisis deskriptif digunakan untuk menggambarkan karakteristik dasar populasi, termasuk demografi responden dan tingkat literasi digital mereka. Ini memberikan gambaran umum tentang siapa yang berpartisipasi dalam penelitian dan bagaimana mereka berinteraksi dengan teknologi. Di sisi lain, analisis inferensial digunakan untuk melakukan generalisasi dari sampel ke populasi lebih luas, memungkinkan peneliti untuk menarik kesimpulan yang lebih signifikan. Dalam konteks ini, analisis korelasi akan membantu menunjukkan apakah ada hubungan linier antara tingkat literasi digital dan kesadaran privasi, sedangkan analisis regresi akan digunakan untuk menentukan variabel-variabel apa saja yang mempengaruhi tingkat kesadaran privasi. Dengan demikian, analisis statistik ini tidak hanya memberikan data numerik tetapi juga informasi kontekstual yang dapat digunakan untuk merumuskan rekomendasi kebijakan atau program pendidikan. Gambar 1 menunjukkan analisis distribusi demografi para responden berdasarkan kelompok usia.




**Gambar 1.** Distribusi Demografi Responden

Penelitian ini mengadopsi model evaluasi berbasis pendekatan CPM sebagai kerangka konseptual untuk menilai perilaku privasi pengguna dengan mempertimbangkan tiga elemen utama: komunikasi, privasi, dan

p-ISSN: 2803-1507 e-ISSN: 2803-1531

manajemen privasi. Dengan menggunakan model ini, peneliti dapat mengevaluasi bagaimana pengguna mengelola informasi pribadi mereka dalam berbagai situasi spesifik serta mengidentifikasi faktor-faktor yang mempengaruhi perilaku privasi mereka. Pendekatan ini sangat berguna dalam memahami bagaimana pengguna mengadaptasi prinsip-prinsip privasi dalam interaksi harian mereka dengan teknologi digital.

### 3.4 *Langkah-langkah Penelitian*

Data dikumpulkan menggunakan berbagai metode, termasuk survei, wawancara mendalam, dan dokumentasi laporan yang berkaitan dengan literasi digital dan pelanggaran privasi. Survei dirancang untuk mengukur tingkat literasi digital serta kesadaran privasi di kalangan pengguna dari berbagai latar belakang. Selain itu, wawancara dengan pakar di bidang privasi digital dan pengembang platform edukasi akan memberikan wawasan tambahan mengenai tantangan yang dihadapi serta praktik terbaik dalam pendidikan digital. Dokumentasi laporan dari lembaga-lembaga terkait juga akan digunakan untuk memberikan konteks yang lebih luas mengenai isu-isu ini. Dengan pendekatan triangulasi data ini, penelitian dapat menghasilkan informasi yang lebih komprehensif dan akurat.

Setelah data terkumpul, langkah selanjutnya adalah pengolahan data menggunakan perangkat lunak analisis statistik dan kualitatif. Data kuantitatif dari survei akan dianalisis dengan teknik statistik deskriptif dan inferensial untuk mengidentifikasi pola serta hubungan antara literasi digital dan kesadaran privasi. Sementara itu, data kualitatif dari wawancara akan dianalisis menggunakan metode analisis tematik untuk mengidentifikasi tema-tema utama yang muncul dari pengalaman responden. Setelah pengolahan data selesai, penelitian ini akan melanjutkan ke tahap penyusunan model pembelajaran yang mengintegrasikan literasi digital dan privasi. Model ini menyediakan kerangka kerja yang jelas bagi lembaga pendidikan dalam merancang kurikulum yang efektif untuk meningkatkan kesadaran privasi di antara siswa. Selanjutnya, uji validasi akan dilakukan untuk memastikan efektivitas model tersebut sebelum hasil penelitian disusun dalam format laporan jurnal akademik serta rekomendasi kebijakan bagi pemangku kepentingan terkait.

### 3.5 *Metrik Evaluasi*

1. Korelasi (R)

Korelasi (R) digunakan untuk menganalisis hubungan antara variabel dalam penelitian, khususnya antara tingkat literasi privasi digital dan dampak sosial yang ditimbulkan. Korelasi yang tinggi menunjukkan adanya hubungan signifikan antara kedua variabel, sementara korelasi yang rendah menandakan tidak adanya hubungan yang berarti. Dalam konteks ini, penelitian dapat memanfaatkan analisis korelasi untuk mengukur sejauh mana pemahaman mengenai privasi digital berkaitan dengan peningkatan dan penurunan dampak sosial akibat kebocoran data pribadi. Untuk menghitung evaluasi metrik Korelasi (R), digunakan rumus (1).

$$R = \frac{n\sum xy - \sum x \sum y}{\sqrt{(n\sum x^2 - (\sum x)^2)(n\sum y^2 - (\sum y)^2)}} \quad (1)$$

Di mana:

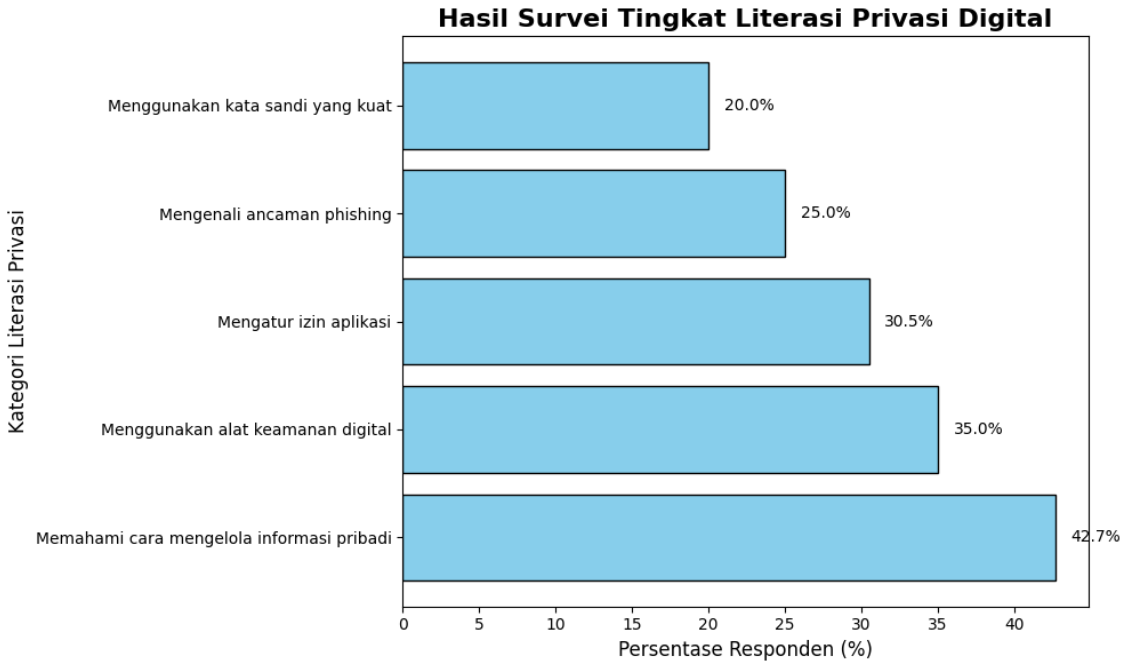
- $x$ dan $y$ adalah nilai dari dua variabel yang ingin diukur korelasinya.
- $n$ adalah jumlah data.

## 4. HASIL DAN PEMBAHASAN

### 4.1 *Interpretasi Data Pengujian*

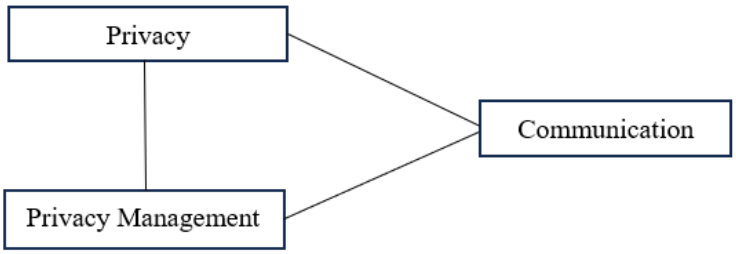
Hasil analisis data menunjukkan bahwa model korelasi (R) berhasil mengidentifikasi hubungan signifikan antara tingkat literasi privasi digital dan pengurangan dampak sosial akibat pelanggaran privasi, dengan nilai korelasi R=0.72. Namun 42,7% responden yang menyatakan memahami cara mengelola informasi pribadi dengan aman. Hal ini menunjukkan bahwa banyak individu belum sepenuhnya menyadari pentingnya perlindungan data pribadi mereka di dunia maya. Kurangnya pemahaman ini menciptakan celah yang memungkinkan terjadinya pelanggaran data dan penyalahgunaan informasi. Selain itu, wawancara dengan para ahli mengungkapkan bahwa sebagian besar pengguna tidak memahami bagaimana platform digital memanfaatkan data mereka, sehingga mereka merasa tidak memiliki kontrol penuh atas informasi pribadi yang dimiliki. Gambar 2 menunjukkan hasil survei mengenai tingkat literasi privasi digital.

p-ISSN: 2803-1507 e-ISSN: 2803-1531




**Gambar 2.** Hasil Survei Tingkat Literasi Privasi Digital

Penelitian ini menggunakan CPM model untuk menganalisis hubungan antara literasi privasi digital dan risiko sosial. Model ini menunjukkan bahwa individu dengan literasi digital yang baik lebih mampu mengelola informasi pribadi mereka, menjaga kontrol atas data sensitif, dan menggunakan alat perlindungan seperti enkripsi dan pengaturan privasi. Hasil penelitian juga menegaskan bahwa pendidikan digital berperan signifikan dalam meningkatkan kesadaran privasi, terutama melalui program simulasi yang mencakup pengenalan ancaman *phishing* dan pengaturan izin aplikasi. Integrasi pendidikan digital ke dalam kurikulum formal direkomendasikan untuk memperluas jangkauan dan efektivitas program ini, sehingga lebih banyak individu dapat melindungi data pribadi mereka dengan lebih baik. Gambar 3 memperlihatkan model evaluasi yang berbasis CMP.




**Gambar 3.** Communication Privacy Management Model

### 4.2 *Hasil Pengujian*

Analisis data kuantitatif menunjukkan bahwa setiap peningkatan 10% dalam literasi privasi digital berkontribusi pada penurunan risiko dampak sosial sebesar 7%. Hal ini menegaskan bahwa peningkatan literasi privasi digital memiliki dampak langsung dalam mengurangi ancaman seperti pencurian identitas, *cyberbullying*, dan eksploitasi data sensitif. Pendekatan berbasis simulasi yang diterapkan dalam program pendidikan terbukti efektif dalam meningkatkan kesadaran responden terhadap ancaman seperti phishing serta memperbaiki kemampuan mereka dalam mengelola izin aplikasi pada perangkat digital. Program ini memberikan pengalaman praktis yang membantu responden mengenali risiko nyata dan belajar cara mengatasinya, terutama di kalangan generasi muda yang paling sering menghadapi risiko tersebut.

p-ISSN: 2803-1507 e-ISSN: 2803-1531

**Tabel 2.** Hubungan Literasi Privasi Digital dengan Penurunan Risiko Sosial

| Tingkat Literasi Privasi Digital (%) | Penurunan Risiko Dampak Ssial (%) | Deskripsi |
|---|---|---|
| 10 | 7 | Peningkatan awal yang menunjukkan dampak positif dalam pengurangan risiko. |
| 20 | 14 | Literasi meningkat dua kali lipat, risiko berkurang secara signifikan. |
| 30 | 21 | Dampak semakin terlihat, dengan penurunan risiko yang konsisten. |
| 40 | 28 | Literasi yang lebih tinggi memberikan manfaat besar dalam mengurangi risiko. |

Selain itu, wawancara mendalam dengan pakar dan diskusi kelompok fokus mengungkapkan bahwa kurangnya pelatihan formal tentang privasi digital menjadi salah satu penghalang utama bagi masyarakat dalam memahami risiko siber dan strategi mitigasi. Banyak responden mengungkapkan bahwa meskipun mereka menyadari pentingnya melindungi data pribadi, mereka tidak memiliki pengetahuan praktis atau alat untuk melakukannya. Temuan ini menunjukkan pentingnya intervensi pendidikan yang terstruktur untuk mempersempit kesenjangan ini.

### 4.3 *Evaluasi Hasil*

Model korelasi (R) yang digunakan dalam penelitian ini memberikan validitas tinggi untuk mengevaluasi hubungan antara literasi privasi digital dan dampak sosial. Dengan nilai R=0.72, model ini menunjukkan adanya hubungan positif yang signifikan, di mana peningkatan literasi privasi digital berkontribusi secara langsung terhadap kemampuan individu untuk mengelola informasi pribadi mereka. Individu dengan literasi privasi digital yang lebih baik menunjukkan pemahaman yang lebih mendalam tentang pengaturan privasi pada platform digital, seperti pemanfaatan fitur kontrol akses, pengelolaan izin aplikasi, dan perlindungan terhadap ancaman phishing. Hal ini memperkuat temuan bahwa literasi privasi digital berperan penting dalam menciptakan lingkungan digital yang lebih aman dan berkelanjutan.

Hasil penelitian ini menyoroti pentingnya integrasi literasi privasi digital ke dalam kurikulum pendidikan formal di berbagai tingkatan, mulai dari sekolah dasar hingga perguruan tinggi. Pendekatan berbasis simulasi sangat disarankan karena mampu memberikan pengalaman nyata yang membantu pengguna memahami dan menangani risiko secara praktis. Dengan demikian, simulasi berbasis situasi dapat melatih siswa untuk mengenali ancaman seperti *phishing* atau eksploitasi data, sehingga mereka memiliki keterampilan praktis untuk mengurangi risiko. Selain itu, teknologi interaktif seperti permainan edukasi dan alat pengajaran berbasis realitas virtual dapat menjadi inovasi yang efektif untuk meningkatkan daya tarik dan efektivitas pendidikan privasi digital.

## 5. DISKUSI

### 5.1 *Simulasi dalam Privasi Digital*

Temuan penelitian menunjukkan bahwa setiap peningkatan 10% dalam literasi privasi digital dapat mengurangi risiko dampak sosial sebesar 7%. Hasil ini sejalan dengan penelitian sebelumnya yang menekankan pentingnya literasi digital dalam mengurangi risiko kebocoran data. Namun, penelitian ini menambahkan bukti kuantitatif yang menunjukkan hubungan linier antara peningkatan literasi dan pengurangan dampak sosial, sementara penelitian lain lebih banyak fokus pada implikasi teoretis tanpa menyajikan data kuantitatif spesifik. Selain itu, penelitian ini menemukan bahwa pendekatan berbasis simulasi memberikan hasil signifikan dalam meningkatkan kesadaran dan keterampilan praktis pengguna terhadap ancaman siber, termasuk *phishing* dan pengelolaan izin aplikasi. Temuan ini memperkaya rekomendasi sebelumnya yang menyarankan penggunaan alat interaktif untuk meningkatkan literasi digital, tetapi tidak menyediakan model simulasi terstruktur sebagaimana dilakukan dalam penelitian ini.

Penelitian ini menawarkan pendekatan konkret untuk meningkatkan kesadaran privasi melalui simulasi situasi nyata, termasuk pengenalan ancaman phishing dan pengaturan izin aplikasi. Penelitian ini mengisi kekosongan dalam literatur sebelumnya dengan menunjukkan bahwa simulasi tidak hanya meningkatkan

p-ISSN: 2803-1507 e-ISSN: 2803-1531

pemahaman teoretis, tetapi juga keterampilan praktis pengguna dalam melindungi data. Program pendidikan berbasis simulasi yang diusulkan sejalan dengan rekomendasi mengenai pentingnya pendekatan holistik untuk literasi digital, dengan fokus pada aplikasi langsung di berbagai tingkat pendidikan. Selain itu, penelitian ini memperdalam konsep literasi privasi digital sebagai komponen penting dalam kurikulum pendidikan formal dengan memperkenalkan model yang menggabungkan teori dan praktik, termasuk penggunaan teknologi realitas virtual dan permainan edukatif. Penelitian ini juga mendukung lima kompetensi inti literasi digital akses, analisis, produksi, kerja sama, dan tanggung jawab sosial dengan memberikan rekomendasi untuk pengembangan kurikulum berbasis simulasi yang meningkatkan kesadaran privasi serta keterampilan teknis dan sosial siswa.

### 5.2 *Pendidikan Digital untuk Privasi*

Hasil penelitian ini sejalan dengan temuan sebelumnya yang menekankan pentingnya pendidikan digital dalam meningkatkan literasi privasi pengguna. Penelitian sebelumnya menunjukkan bahwa pendidikan berbasis simulasi dapat secara signifikan meningkatkan kesadaran pengguna terhadap risiko privasi, memberikan pengalaman langsung dalam mengidentifikasi dan menangani situasi berisiko. Selain itu, penelitian ini menekankan bahwa pendidikan merupakan metode yang efektif untuk mengatasi kesenjangan yang tidak dapat dijangkau oleh solusi teknis, enkripsi, maupun firewall, dengan penekanan pada pengembangan kemampuan individu untuk mengenali dan mengurangi ancaman terhadap privasi. Pendekatan ini berbeda dari solusi teknis yang sering kali hanya berfungsi sebagai alat pendukung tanpa memberikan pemahaman mendalam tentang risiko yang dihadapi pengguna.

Penelitian ini juga mengungkapkan bahwa implementasi pendidikan digital belum sepenuhnya optimal, terutama dalam konteks masyarakat yang lebih luas [48]. Temuan ini sejalan dengan hasil penelitian penelitian sebelumnya, yang menunjukkan bahwa banyak pengguna masih merasa tidak memiliki kontrol penuh atas data pribadi mereka. Meskipun platform digital menyediakan pengaturan privasi, banyak pengguna tidak memahami cara memanfaatkannya secara efektif. Kurangnya pelatihan formal tentang pengelolaan privasi data menjadi salah satu faktor utama yang menyebabkan kesenjangan ini. Selain itu, penelitian sebelumnya menekankan pentingnya intervensi pendidikan di tingkat formal untuk menjangkau audiens yang lebih luas, termasuk remaja dan anak-anak, yang sering menjadi target utama ancaman siber. Anak-anak dan remaja yang tumbuh di era digital sering kali merupakan pengguna aktif teknologi tanpa memahami risiko yang terkait. Dengan memasukkan pendidikan privasi digital dalam kurikulum sekolah, mereka dapat belajar tentang pentingnya melindungi data pribadi sejak usia dini, termasuk pengajaran tentang kata sandi yang kuat, pengelolaan izin aplikasi, dan cara mengenali tanda-tanda *phishing.*

Lebih jauh lagi, pentingnya pendidikan komunitas tidak dapat diabaikan. Pendidikan digital berbasis komunitas dapat menjangkau kelompok yang kurang terlayani, termasuk populasi pedesaan atau mereka yang memiliki akses terbatas ke teknologi. Dengan melibatkan komunitas lokal, program pendidikan ini dapat disesuaikan dengan kebutuhan dan tantangan spesifik yang dihadapi oleh kelompok tersebut, termasuk rendahnya literasi teknologi dan kurangnya pemahaman mengenai ancaman terhadap privasi. Dengan demikian, pendidikan digital dapat menjadi alat inklusif dan efektif dalam meningkatkan literasi privasi di berbagai segmen masyarakat.

### 5.3 *Literasi Privasi Digital*

Hasil penelitian menunjukkan bahwa peningkatan literasi privasi digital secara signifikan mengurangi risiko sosial, termasuk pencurian identitas, *cyberbullying*, dan eksploitasi data sensitif. Dengan menggunakan model CPM, individu dengan literasi privasi yang lebih baik terbukti lebih mampu mengelola informasi pribadi, memanfaatkan alat keamanan, dan memahami pengaturan izin aplikasi. Temuan ini menekankan pentingnya pendidikan digital yang terintegrasi dalam kurikulum formal untuk meningkatkan kesadaran privasi masyarakat secara menyeluruh. Ini mencakup pendekatan berbasis simulasi dan pelatihan langsung yang memungkinkan individu untuk mempraktikkan perlindungan data dalam situasi nyata.

Selain itu, hubungan positif antara literasi privasi digital dan penurunan dampak sosial menunjukkan perlunya kolaborasi antara pemerintah, lembaga pendidikan, dan pengembang platform digital. Hasil ini mengindikasikan bahwa program pendidikan berbasis teknologi interaktif, termasuk permainan edukatif dan realitas virtual, dapat menjadi cara efektif untuk mengajarkan keterampilan privasi secara menyeluruh. Integrasi literasi digital dengan pendekatan berbasis komunitas dapat membantu mengatasi kesenjangan kesadaran privasi, terutama di kalangan pengguna muda yang sering menjadi target ancaman siber. Penelitian

p-ISSN: 2803-1507 e-ISSN: 2803-1531

ini juga menegaskan pentingnya kebijakan dan regulasi yang mendukung pendidikan privasi digital sebagai elemen kunci dalam perlindungan data nasional. Dengan nilai korelasi (R) sebesar 0,72, penelitian ini menunjukkan urgensi adopsi kebijakan berbasis literasi privasi untuk menciptakan lingkungan digital yang lebih aman dan inklusif, serta mendorong perubahan perilaku digital yang lebih bertanggung jawab dalam era transformasi digital.

## 6. KESIMPULAN DAN SARAN

### 6.1 Kesimpulan

Penelitian ini menyoroti pentingnya pendidikan digital dalam meningkatkan literasi privasi pengguna di era digital yang penuh risiko. Temuan utama menunjukkan bahwa literasi privasi digital di antara pengguna masih berada pada tingkat moderat, dengan hanya 42,7% responden yang memahami cara melindungi informasi pribadi mereka secara efektif. Ketidakpahaman ini menciptakan peluang bagi terjadinya pelanggaran data, penyalahgunaan informasi, serta dampak sosial yang meliputi cyberbullying dan pencurian identitas. Model evaluasi berbasis CPM berhasil menunjukkan hubungan signifikan antara literasi privasi digital yang lebih baik dengan pengurangan risiko dampak sosial, mencerminkan pentingnya pendekatan holistik dalam pendidikan digital.

### 6.2 Saran

Penelitian ini merekomendasikan agar pendidikan literasi privasi digital diintegrasikan ke dalam kurikulum formal dari tingkat sekolah dasar hingga perguruan tinggi, menggunakan pendekatan simulasi situasi nyata. Program tersebut harus mencakup pengelolaan izin aplikasi, pengenalan ancaman *phishing*, dan pentingnya kata sandi yang kuat. Selain itu, pendidikan berbasis komunitas diperlukan untuk menjangkau populasi yang kurang terlayani di daerah pedesaan. Kerja sama antara pemerintah, lembaga pendidikan, dan organisasi teknologi sangat penting untuk mengembangkan materi pembelajaran yang relevan dengan kebutuhan lokal. Penelitian mendatang perlu memperluas fokus pada kelompok masyarakat yang berbeda dan menganalisis pengaruh faktor budaya serta ekonomi terhadap literasi privasi digital. Dengan alat evaluasi risiko yang lebih baik dan program pendidikan yang adaptif, masyarakat dapat lebih siap menghadapi tantangan privasi di era digital, menciptakan lingkungan online yang lebih aman.

## DAFTAR PUSTAKA

[1] M. Safaei Pour, C. Nader, K. Friday, and E. Bou-Harb, "A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security," *Comput Secur*, vol. 128, p. 103123, May 2023, doi: 10.1016/j.cose.2023.103123.

[2] D Cetindamar Kozanoglu, "Understanding the role of employees in digital transformation: conceptualization of digital literacy of employees as a multi-dimensional organizational affordance," *Journal of Enterprise Information Management*, vol. 34, no. 6, pp. 1649–1672, 2021, doi: 10.1108/JEIM-01-2020-0010.

[3] G. A. P. Rodrigues, A. L. M. Serrano, G. F. Vergara, R. de O. Albuquerque, and G. D. A. Nze, "Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies," *Future Internet 2024, Vol. 16, Page 201*, vol. 16, no. 6, p. 201, Jun. 2024, doi: 10.3390/FI16060201.

[4] R. Belen Saglam, J. R. C. Nurse, and D. Hodges, "Personal information: Perceptions, types and evolution," *Journal of Information Security and Applications*, vol. 66, p. 103163, May 2022, doi: 10.1016/j.jisa.2022.103163.

[5] J. Lee and S. H. Tak, "Factors associated with eHealth literacy focusing on digital literacy components: A cross-sectional study of middle-aged adults in South Korea," *https://doi.org/10.1177/20552076221102765*, vol. 8, pp. 1–9, May 2022, doi: 10.1177/20552076221102765.

[6] S. Maqsood and S. Chiasson, "Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens," *ACM Transactions on Privacy and Security (TOPS)*, vol. 24, no. 4, pp. 1–37, Sep. 2021, doi: 10.1145/3469821.

p-ISSN: 2803-1507 e-ISSN: 2803-1531

[7] L. Huang, J. Zhou, J. Lin, and S. Deng, "View analysis of personal information leakage and privacy protection in big data era—based on Q method," *Aslib Journal of Information Management*, vol. 74, no. 5, pp. 901–927, Sep. 2022, doi: 10.1108/AJIM-05-2021-0144.

[8] I. Herrera Montano, J. J. García Aranda, J. Ramos Diaz, S. Molina Cardín, I. de la Torre Díez, and J. J. P. C. Rodrigues, "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat," *Cluster Comput*, vol. 25, pp. 4289–4302, Jul. 2022, doi: 10.1007/s10586-022-03668-2.

[9] F. B. Zhu and Z. Song, "Systematic Regulation of Personal Information Rights in the Era of Big Data," *Sage Open*, vol. 12, pp. 1–11, Jan. 2022, doi: 10.1177/21582440211067529.

[10] J. R. Saura, D. Ribeiro-Soriano, and D. Palacios-Marqués, "Assessing behavioral data science privacy issues in government artificial intelligence deployment," *Gov Inf Q*, vol. 39, p. 101679, Feb. 2022, doi: 10.1016/j.giq.2022.101679.

[11] F. Huang, T. Teo, and R. Scherer, "Investigating the antecedents of university students' perceived ease of using the Internet for learning," *Interactive Learning Environments*, vol. 30, no. 6, pp. 1–18, Jan. 2022, doi: 10.1080/10494820.2019.1710540.

[12] J. R. Saura, D. Ribeiro-Soriano, and D. Palacios-Marqués, "From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets," *Int J Inf Manage*, vol. 60, p. 102331, Feb. 2021, doi: 10.1016/j.ijinfomgt.2021.102331.

[13] J. Valverde-Berrocoso, M. R. Fernández-Sánchez, F. I. R. Dominguez, and M. J. Sosa-Díaz, "The educational integration of digital technologies preCovid-19: Lessons for teacher education," *PLoS One*, vol. 16, no. 8, p. e0256283, Aug. 2021, doi: 10.1371/journal.pone.0256283.

[14] A Christopoulos and P. Sprangers, "Integration of educational technology during the Covid-19 pandemic: An analysis of teacher and student receptions," *Cogent Education*, vol. 8, no. 1, Aug. 2021, doi: 10.1080/2331186X.2021.1964690.

[15] E. Zvereva, "Digital ethics in higher education: Modernizing moral values for effective communication in cyberspace," *Online J Commun Media Technol*, vol. 13, no. 2, p. e202319, Mar. 2023, doi: 10.30935/ojcmt/13033.

[16] H. A. Althibyani and A. M. Al-Zahrani, "Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime," *Sustainability 2023, Vol. 15, Page 11512*, vol. 15, no. 15, p. 11512, Jul. 2023, doi: 10.3390/su151511512.

[17] A. Reksoprodjo, M. Dachyar, N. P.-J. of S. and, and undefined 2024, "A Decision-Making Model for Selecting Personal Data Protection Frameworks for Companies in Indonesia," *Journal of System and Management Sciences*, vol. 14, no. 2, pp. 156–171, 2024, doi: 10.33168/JSMS.2024.0210.

[18] A. Luthfia, D. Wibowo, M. A. Widyakusumastuti, and M. Angeline, "The Role of Digital Literacy on Online Opportunity and Online Risk in Indonesian Youth," *Asian Journal for Public Opinion Research*, vol. 9, no. 2, pp. 142–160, May 2021, doi: 10.15206/ajpor.2021.9.2.142.

[19] P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing," *Journal of Web Engineering*, vol. 21, no. 7, pp. 2187–2208, Dec. 2022, doi: 10.13052/jwe1540-9589.2178.

[20] I. Makhdoom, M. Abolhasan, J. Lipman, N. Shariati, D. Franklin, and M. Piccardi, "Securing Personally Identifiable Information: A Survey of SOTA Techniques, and a Way Forward," *IEEE Access*, vol. 12, pp. 116740–116770, Aug. 2024, doi: 10.1109/ACCESS.2024.3447017.

[21] D Goyeneche, S Singaraju, and L. Arango, "Linked by age: a study on social media privacy concerns among younger and older adults," *Industrial Management and Data Systems*, vol. 124, no. 2, pp. 640–665, Dec. 2023, doi: 10.1108/IMDS-07-2023-0462.

[22] T. Alharbi and A. T. Computing, "Assessment of cybersecurity awareness among students of Majmaah University," *mdpi.com*, vol. 5, no. 2, May 2021, doi: 10.3390/bdcc5020023.

[23] E. R. Purboningsih, K. Massar, Z. R. Hinduan, H. Agustiani, R. A. C. Ruiter, and P. Verduyn, "Perception and use of social media by Indonesian adolescents and parents: A qualitative study," *Front Psychol*, vol. 13, p. 985112, Jan. 2023, doi: 10.3389/fpsyg.2022.985112.

[24] O. A. Alismaiel, "Digital Media Used in Education: The Influence on Cyberbullying Behaviors among Youth Students," *International Journal of Environmental Research and Public Health 2023, Vol. 20, Page 1370*, vol. 20, no. 2, p. 1370, Jan. 2023, doi: 10.3390/ijerph20021370.

[25] V. I. Marín, J. P. Carpenter, and G. Tur, "Pre-service teachers' perceptions of social media data privacy policies," *British Journal of Educational Technology*, vol. 52, no. 2, pp. 519–535, 2021, doi: 10.1111/bjet.13035.

[26] Y. Zhao, M. C. Sánchez Gómez, A. M. Pinto Llorente, and L. Zhao, "Digital Competence in Higher Education: Students' Perception and Personal Factors," *MDPI*, vol. 13, no. 21, p. 12184, Nov. 2021, doi: 10.3390/su132112184.

[27] A. Mansour and H. Francke, "Collective Privacy Management Practices: A Study of Privacy Strategies and Risks in a Private Facebook Group," *Proc ACM Hum Comput Interact*, vol. 5, no. CSCW2, pp. 1–28, Oct. 2021, doi: 10.1145/3479504.

[28] S. Aiolfi, S. Bellini, and D. Pellegrini, "Data-driven digital advertising: benefits and risks of online behavioral advertising," *International Journal of Retail and Distribution Management*, vol. 49, no. 7, pp. 1089–1110, 2021, doi: 10.1108/IJRDM-10-2020-0410.

[29] Z Peng, "Your growth is my growth: examining sharenting behaviours from a multiparty privacy perspective," *Communication Research and Practice*, vol. 9, no. 3, pp. 271–289, Jun. 2023, doi: 10.1080/22041451.2023.2216584.

[30] O. Vorobel, T. T. Voorhees, and D. Gokcora, "Language learners' digital literacies: Focus on students' information literacy and reading practices online," *J Comput Assist Learn*, vol. 37, no. 4, pp. 1127–1140, Apr. 2021, doi: 10.1111/jcal.12550.

[31] G. Polizzi, "Internet users' utopian/dystopian imaginaries of society in the digital age: Theorizing critical digital literacy and civic engagement," *Sage Journals*, vol. 25, no. 6, pp. 1205–1226, Jun. 2021, doi: 10.1177/14614448211018609.

[32] F. H. Chun Wong *et al.*, "Consuming information related to COVID-19 on social media among older adults and its association with anxiety, social trust in information, and COVID-safe behaviors: Cross-sectional telephone survey," *J Med Internet Res*, vol. 23, no. 2, p. e26570, Feb. 2021, doi: 10.2196/26570.

[33] M. C. Martínez-Bravo, C. S. Chalezquer, and J. Serrano-Puche, "Dimensions of Digital Literacy in the 21st Century Competency Frameworks," vol. 14, no. 3, p. 1867, Feb. 2022, doi: 10.3390/su14031867.

[34] T. Berghout, M. Benbouzid, and S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100547, Sep. 2022, doi: 10.1016/j.ijcip.2022.100547.

[35] H. N. Chua, J. S. Ooi, and A. Herbland, "The effects of different personal data categories on information privacy concern and disclosure," *Comput Secur*, vol. 110, p. 102453, 2021, doi: 10.1016/j.cose.2021.102453.

[36] J. H. Zhang, T. Koivumäki, and D. Chalmers, "Privacy vs convenience: Understanding intention-behavior divergence post-GDPR," *Comput Human Behav*, vol. 160, p. 108382, 2024, doi: 10.1016/j.chb.2024.108382.

[37] Y. Kurniawan, S. I. Santoso, R. R. Wibowo, N. Anwar, G. Bhutkar, and E. Halim, "Analysis of Higher Education Students' Awareness in Indonesia on Personal Data Security in Social Media," *Sustainability*, vol. 15, no. 4, p. 3814, 2023, doi: 10.3390/su15043814.

[38] M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," *Wirel Commun Mob Comput*, vol. 2022, no. 1, p. 8669348, 2022, doi: 10.1155/2022/8669348.

p-ISSN: 2803-1507 e-ISSN: 2803-1531

[39] T. Schulenkorf, V. Krah, K. Dadaczynski, and O. Okan, "Addressing Health Literacy in Schools in Germany: Concept Analysis of the Mandatory Digital and Media Literacy School Curriculum," *Front Public Health*, vol. 9, p. 687389, 2021, doi: 10.3389/fpubh.2021.687389.

[40] W. H. Prasetiyo, B. Sumardjoko, A. Muhibbin, N. B. M. Naidu, and A. Muthali'in, "Promoting Digital Citizenship among Student-Teachers: The Role of Project-Based Learning in Improving Appropriate Online Behaviors," *Participatory Educational Research*, vol. 10, no. 1, pp. 389–407, 2023, doi: 10.17275/per.23.21.10.1.

[41] M. C. Buchan, J. Bhawra, and T. R. Katapally, "Navigating the digital world: development of an evidence-based digital literacy program and assessment tool for youth," *Smart Learning Environments*, vol. 11, pp. 1–24, 2024, doi: 10.1186/s40561-024-00293-x.

[42] S. Modgil, R. K. Singh, S. Gupta, and D. Dennehy, "A Confirmation Bias View on Social Media Induced Polarisation During Covid-19," *Information Systems Frontiers*, vol. 26, pp. 417–441, 2024, doi: 10.1007/s10796-021-10222-9.

[43] E. Rodilosso, "Filter Bubbles and the Unfeeling: How AI for Social Media Can Foster Extremism and Polarization," *Philos Technol*, vol. 37, no. 71, pp. 1–21, 2024, doi: 10.1007/s13347-024-00758-4.

[44] M. A. Throuvala *et al.*, "Perceived Challenges and Online Harms from Social Media Use on a Severity Continuum: A Qualitative Psychological Stakeholder Perspective," *Int J Environ Res Public Health*, vol. 18, no. 6, p. 3227, 2021, doi: 10.3390/ijerph18063227.

[45] I. Krisnana *et al.*, "Adolescent characteristics and parenting style as the determinant factors of bullying in Indonesia: A cross-sectional study," *Int J Adolesc Med Health*, vol. 33, no. 5, Oct. 2021, doi: 10.1515/ijamh-2019-0019.

[46] O. Sarah Soyeon, K. A. Kim, M. Kim, J. Oh, S. H. Chu, and J. Y. Choi, "Measurement of digital literacy among older adults: Systematic review," *J Med Internet Res*, vol. 23, no. 2, p. e26145, 2021, doi: 10.2196/26145.

[47] A. Nguyen, H. N. Ngo, Y. Hong, B. Dang, and B. P. T. Nguyen, "Ethical principles for artificial intelligence in education," *Educ Inf Technol (Dordr)*, vol. 28, no. 4, pp. 4221–4241, Apr. 2023, doi: 10.1007/S10639-022-11316-W/TABLES/1.

[48] M. Odinokaya, E. Tsimerman, M. Akour, and M. Alenezi, "Higher Education Future in the Era of Digital Transformation," *Educ Sci (Basel)*, vol. 12, no. 11, p. 784, 2022, doi: 10.3390/educsci12110784.