



Analisis Kesadaran Mahasiswa dalam Menjaga Keamanan Data Pribadi pada Penggunaan Media

Muhammad Alief Rasyidin^{1*}, Allyssa Putri², Maulina Diah Lestari³, Riska Nurnajmah⁴,
Danish Alifian Safaraz⁵

¹⁻⁵Informatika, Universitas Islam Negeri Sultan Maulana Hasanudin Banten, Serang, Indonesia

Email: muhammadaliefasyidin@gmail.com^{1*}, allyssaputri777@gmail.com², maulinadiah538@gmail.com³,
nurnajmahrisk@gmail.com⁴, danish.12092006@gmail.com⁵

*Penulis korespondensi: muhammadaliefasyidin@gmail.com¹

Abstract. *This study examines the level of personal data security awareness among college students, an age group that is vulnerable to digital risks due to the intensity of social media use. The main objective of the research is to measure the extent to which students understand, behave, and behave in protecting their personal data in an ecosystem of digital platforms such as Instagram, Twitter, and TikTok. The research method used a descriptive quantitative approach through the distribution of questionnaires to 33 students. The results of the study show that students have a sufficient level of knowledge about the types of personal data and potential threats that may arise. However, it was found that there was a significant gap between knowledge and actual behavior, where most respondents were still negligent in activating security features and managing the privacy of social media accounts. These findings confirm that increasing awareness is not enough just through providing information, but must be followed by internalizing consistent data security attitudes and practices. Thus, this research makes an important contribution in understanding the pattern of student awareness of personal data security, as well as being the basis for the development of more effective digital education strategies to encourage safe behavior in cyberspace.*

Keywords: Information Security; Personal Data; Security Awareness; Social Media; Students

Abstrak. Penelitian ini mengkaji tingkat kesadaran keamanan data pribadi di kalangan mahasiswa, kelompok usia yang rentan terhadap risiko digital akibat intensitas penggunaan media sosial. Tujuan utama penelitian adalah mengukur sejauh mana mahasiswa memahami, bersikap, dan berperilaku dalam melindungi data pribadi mereka di ekosistem platform digital seperti Instagram, Twitter, dan TikTok. Metode penelitian menggunakan pendekatan kuantitatif deskriptif melalui penyebaran kuesioner kepada 33 mahasiswa. Hasil penelitian menunjukkan bahwa mahasiswa memiliki tingkat pengetahuan yang cukup memadai mengenai jenis-jenis data pribadi serta potensi ancaman yang mungkin timbul. Namun, ditemukan adanya kesenjangan signifikan antara pengetahuan dan perilaku aktual, di mana sebagian besar responden masih lalai dalam mengaktifkan fitur keamanan maupun mengatur privasi akun media sosial. Temuan ini menegaskan bahwa peningkatan kesadaran tidak cukup hanya melalui pemberian informasi, melainkan harus diikuti dengan internalisasi sikap serta praktik keamanan data yang konsisten. Dengan demikian, penelitian ini memberikan kontribusi penting dalam memahami pola kesadaran mahasiswa terhadap keamanan data pribadi, sekaligus menjadi dasar bagi pengembangan strategi edukasi digital yang lebih efektif untuk mendorong perilaku aman di ruang siber.

Kata kunci: Data Pribadi; Keamanan Informasi; Kesadaran Keamanan; Mahasiswa; Media Sosial

1. LATAR BELAKANG

Perkembangan teknologi informasi yang sangat pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Penggunaan internet, media sosial, dan berbagai aplikasi digital telah menjadi bagian yang tidak terpisahkan dari aktivitas sehari-hari masyarakat, khususnya mahasiswa. Kemajuan ini memberikan kemudahan dalam mengakses informasi dan berkomunikasi, namun di sisi lain juga menimbulkan berbagai risiko, terutama terkait dengan keamanan dan perlindungan data pribadi (Judijanto et al., 2024; Sadeli & Irawati, 2023).

Data pribadi merupakan informasi yang melekat pada individu dan bersifat sensitif, sehingga harus dilindungi dari potensi penyalahgunaan. Dalam konteks digital, data pribadi dapat berupa identitas diri, nomor telepon, alamat email, data keuangan, hingga aktivitas daring seseorang. Meningkatnya kasus kebocoran data dan kejahatan siber menunjukkan bahwa masih rendahnya kesadaran masyarakat terhadap pentingnya menjaga keamanan data pribadi (Rahman, 2024).

Mahasiswa sebagai kelompok yang aktif menggunakan teknologi digital seharusnya memiliki tingkat kesadaran yang tinggi terhadap perlindungan data pribadi. Namun, pada kenyataannya masih banyak mahasiswa yang kurang memperhatikan aspek keamanan data dalam aktivitas digitalnya, seperti penggunaan kata sandi yang lemah, membagikan informasi pribadi secara berlebihan, serta kurang waspada terhadap ancaman phishing dan penipuan daring (Juli et al., 2025; Saputra, 2023).

Kesadaran terhadap keamanan data pribadi tidak hanya dipengaruhi oleh kemampuan teknis, tetapi juga oleh literasi digital yang mencakup pengetahuan, sikap, dan perilaku pengguna dalam memanfaatkan teknologi informasi. Literasi digital yang baik dapat membantu individu memahami risiko yang ada serta menerapkan langkah-langkah pencegahan untuk melindungi data pribadinya (Rahman, 2024; Sadeli & Irawati, 2023).

Di Indonesia, perlindungan data pribadi telah diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai upaya negara dalam melindungi hak privasi warga negara. Regulasi ini menegaskan pentingnya perlindungan data pribadi sebagai bagian dari hak asasi manusia yang harus dihormati dan dilindungi oleh seluruh pihak, baik individu, institusi, maupun penyedia layanan digital (Judijanto et al., 2024; Priyantiwi, 2025).

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji peran literasi digital dalam meningkatkan kesadaran mahasiswa terhadap keamanan data pribadi di era teknologi informasi. Dengan meningkatnya literasi digital, diharapkan mahasiswa mampu memahami pentingnya perlindungan data pribadi serta menerapkan praktik keamanan yang tepat dalam aktivitas digital sehari-hari (Juli et al., 2025).

2. KAJIAN TEORITIS

Data Pribadi dan Privasi Digital

Data Pribadi di era digital didefinisikan sebagai setiap informasi yang dapat mengidentifikasi atau menghubungi individu tertentu, baik secara langsung maupun tidak langsung, yang dikumpulkan melalui metode elektronik dan/atau non-elektronik (Judijanto et al., 2024; Sadeli & Irawati, 2023). Dalam konteks Indonesia, Undang-Undang Nomor 27

Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) mengkategorikan data pribadi menjadi dua:

- a. Data Pribadi Umum: Termasuk nama lengkap, jenis kelamin, alamat email, dan foto/video.
- b. Data Pribadi Spesifik: Termasuk informasi yang bersifat sensitif seperti riwayat kesehatan, data biometrik (sidik jari, wajah), riwayat keuangan, dan data kehidupan seksual (Priyantiwi, 2025).

Privasi Digital adalah hak individu untuk mengontrol kapan, di mana, dan bagaimana informasi mengenai dirinya dikumpulkan, digunakan, atau diungkapkan. Di media sosial, privasi seringkali terkikis karena pengguna secara sukarela membagikan informasi dalam jumlah besar, yang kemudian dapat dieksploitasi untuk berbagai tujuan (Abdullah, 2024)

Model Kesadaran Keamanan Data (Knowledge-Attitude-Behavior)

Kesadaran Keamanan Data (Data Security Awareness) merupakan upaya kognitif yang dilakukan individu untuk menyadari dan memahami ancaman keamanan informasi dan privasi, serta tindakan yang diperlukan untuk melindungi informasi tersebut (Rahman, 2024).

Untuk mengukur kesadaran secara komprehensif, penelitian ini mengadopsi model yang banyak digunakan dalam konteks keamanan informasi: Knowledge-Attitude-Behavior (KAB) Model. Model ini membagi kesadaran menjadi tiga dimensi utama yang saling berkaitan :

Tabel 1. Knowledge-Attitude-Behavior (KAB) Model.

Dimensi	Definisi Kontekstual	Contoh Pengukuran pada Mahasiswa
1. Knowledge (Pengetahuan)	Pemahaman teoritis individu terhadap konsep data pribadi, ancaman siber (<i>phishing</i> , <i>malware</i>), dan fitur keamanan (misalnya, <i>two-factor authentication</i>).	Sejauh mana mahasiswa tahu apa itu data biometrik dan risiko berbagi <i>password</i> .
2. Attitude (Sikap)	Kecenderungan perasaan atau emosi individu terhadap perlindungan data pribadi. Sikap mencerminkan kepedulian atau kekhawatiran mereka terhadap risiko.	Seberapa setuju mahasiswa bahwa data pribadi mereka sangat berharga dan harus dilindungi.
3. Behavior (Perilaku)	Tindakan nyata atau praktik yang dilakukan individu untuk melindungi data pribadi. Perilaku adalah refleksi dari pengetahuan dan sikap yang diterapkan.	Frekuensi mahasiswa mengganti kata sandi, menggunakan VPN, atau meninjau <i>privacy setting</i> media sosial.

Kesenjangan yang sering ditemukan adalah bahwa pengetahuan yang tinggi tidak selalu menghasilkan perilaku perlindungan data yang konsisten. Inilah yang menjadi fokus utama dalam analisis hasil penelitian ini.

Ancaman Data Pribadi di Era Media Sosial

Media sosial telah menjadi area fokus utama dalam pengukuran kesadaran keamanan (Parsons et al., 2014). Ancaman yang relevan bagi mahasiswa di platform ini meliputi:

- a. *Penyalahgunaan Data Pribadi*: Data yang dikumpulkan (seperti riwayat pencarian atau lokasi) digunakan oleh pihak ketiga tanpa persetujuan, seringkali untuk target iklan atau *profiling* politik.
- b. *Social Engineering* dan *Phishing*: Mahasiswa rentan menjadi target penipuan yang memanfaatkan informasi yang mereka bagikan di media sosial untuk membangun kepercayaan sebelum meluncurkan serangan (Priyantiwi, 2025)
- c. *Pengambilan Alih Akun (Account Takeover)*: Akibat penggunaan *password* yang lemah atau berulang, yang menyebabkan data pribadi tersebar dan digunakan untuk tindakan kriminal (Juli et al., 2025)

Penelitian Terdahulu yang Relevan

Beberapa penelitian terdahulu menunjukkan tren yang konsisten di kalangan mahasiswa Indonesia:

- a. Penelitian di Yogyakarta menemukan bahwa mayoritas mahasiswa memiliki tingkat kesadaran privasi sedang (skor rata-rata 3,2 dari 5). Meskipun mereka menyadari risiko berbagi informasi pribadi, mereka belum melakukan tindakan pencegahan yang cukup.
- b. Ditemukan adanya perbedaan signifikan pada kesadaran privasi berdasarkan jenis kelamin, di mana mahasiswa perempuan cenderung lebih berhati-hati dibandingkan laki-laki.
- c. Tingginya perilaku berbagi foto pribadi (70%) menunjukkan adanya risiko kebocoran data pribadi yang dikombinasikan dengan kesadaran yang rendah.

3. METODE PENELITIAN

Jenis dan Desain Penelitian

Penelitian ini menerapkan pendekatan kuantitatif dengan rancangan deskriptif cross-sectional. Rancangan ini digunakan untuk menggambarkan tingkat kesadaran mahasiswa dalam menjaga keamanan data pribadi pada penggunaan berbagai platform media sosial, seperti Instagram, TikTok, WhatsApp, dan media sosial lainnya, yang diukur pada satu periode waktu tertentu. Pendekatan cross-sectional banyak digunakan dalam kajian kesadaran

keamanan informasi dan privasi digital karena mampu memberikan gambaran kondisi responden secara aktual tanpa intervensi peneliti (Fattah et al., 2023; Jayasinghe et al., 2023; Kurnia et al., 2025).

Analisis penelitian ini didasarkan pada kerangka Knowledge–Attitude–Behavior (KAB) yang digunakan untuk mema keterkaitan antara pengetahuan, sikap, dan perilaku mahasiswa dalam melindungi data pribadi saat berinteraksi di media sosial. Kerangka ini telah diaplikasikan secara luas dalam penelitian keamanan siber di lingkungan pendidikan (Breckner et al., 2011; Jayasinghe et al., 2023; Mesra Betty Yel & Mahyuddin K. M. Nasution, 2022).

Lokasi dan Waktu Penelitian

Penelitian dilaksanakan secara daring dengan melibatkan mahasiswa aktif di wilayah Serang yang menggunakan media sosial sebagai bagian dari aktivitas digital sehari-hari. Platform media sosial yang menjadi fokus utama penelitian ini meliputi Instagram, TikTok, dan WhatsApp. Pengumpulan data dilakukan pada periode 18-19 Desember 2025. Metode pengumpulan data secara online dipilih karena sesuai dengan karakteristik mahasiswa sebagai pengguna aktif media sosial dan telah banyak digunakan dalam penelitian terkait privasi dan keamanan data digital (Fattah et al., 2023; Puwa et al., 2023; Setiawan, 2018).

Populasi, Sampel, dan Teknik Sampling

Populasi dalam penelitian ini adalah mahasiswa aktif yang menggunakan media sosial. Teknik pengambilan sampel yang digunakan adalah purposive sampling, dengan kriteria sebagai berikut:

- a. berstatus sebagai mahasiswa aktif,
- b. menggunakan setidaknya satu platform media sosial, yaitu Instagram, TikTok, atau WhatsApp,
- c. mengakses media sosial minimal satu kali dalam sehari, dan
- d. bersedia berpartisipasi dalam penelitian dengan mengisi kuesioner secara sukarela.

Penggunaan teknik purposive sampling dinilai sesuai karena penelitian ini berfokus pada responden yang memiliki pengalaman langsung dalam penggunaan media sosial dan berpotensi menghadapi risiko keamanan data pribadi (Farida et al., 2023; Firmansyah & Darmawan, 2020; Saputra, 2023).

Variabel dan Operasionalisasi Penelitian

Variabel utama dalam penelitian ini adalah kesadaran keamanan data pribadi mahasiswa dalam penggunaan media sosial, yang dioperasionalisasikan berdasarkan kerangka Knowledge–Attitude–Behavior (KAB), dengan penjelasan sebagai berikut:

- a. Pengetahuan (Knowledge), yaitu tingkat pemahaman mahasiswa mengenai jenis data pribadi yang dibagikan melalui Instagram, TikTok, dan WhatsApp, potensi risiko kebocoran data, pengaturan privasi akun, serta ancaman keamanan seperti phishing dan penyalahgunaan akun (Elrayah & Jamil, 2023).
- b. Sikap (Attitude), yang mencerminkan tingkat kepedulian, persepsi risiko, serta pandangan mahasiswa terhadap pentingnya perlindungan data pribadi dalam aktivitas bermedia sosial.
- c. Perilaku (Behavior), yaitu tindakan nyata mahasiswa dalam menjaga keamanan data pribadi, seperti pengaturan privasi akun, penggunaan autentikasi dua faktor (2FA), pembatasan akses aplikasi, dan kehati-hatian dalam membagikan informasi pribadi.

Seluruh indikator diukur menggunakan skala Likert lima poin, yang umum digunakan dalam penelitian kesadaran keamanan dan privasi digital.

Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui kuesioner daring menggunakan Google Forms, yang disebarluaskan melalui media sosial dan grup komunikasi mahasiswa. Metode ini dipilih karena efektif dalam menjangkau responden yang merupakan pengguna aktif Instagram, TikTok, dan WhatsApp, serta telah banyak diterapkan dalam penelitian sejenis. Aspek etika penelitian diperhatikan dengan memberikan informed consent kepada responden, menjamin anonimitas data, serta memastikan partisipasi responden bersifat sukarela.

Teknik Analisis Data

Data yang diperoleh dianalisis secara deskriptif, meliputi perhitungan frekuensi, persentase, dan nilai rata-rata untuk menggambarkan tingkat kesadaran keamanan data pribadi mahasiswa pada masing-masing platform media sosial.

Selain itu, analisis korelasi dan regresi digunakan untuk mengkaji hubungan antara pengetahuan, sikap, dan perilaku mahasiswa dalam menjaga keamanan data pribadi pada penggunaan media sosial.

Analisis lanjutan berupa uji ANOVA dapat digunakan untuk membandingkan tingkat kesadaran keamanan data pribadi antar platform media sosial, sebagaimana diterapkan dalam penelitian perbandingan privasi digital lintas platform (Rahman, 2024).

Pertimbangan Etika dan Keterbatasan Penelitian

Penelitian ini menjunjung tinggi prinsip etika penelitian dengan menjaga kerahasiaan identitas responden serta menggunakan data secara anonim. Seluruh data digunakan hanya untuk kepentingan akademik.

Keterbatasan penelitian ini meliputi penggunaan data berbasis self-report, yang berpotensi menimbulkan bias subjektivitas responden, serta perbedaan karakteristik fitur privasi antar platform media sosial yang dapat memengaruhi persepsi dan perilaku responden.

4. HASIL DAN PEMBAHASAN

Karakteristik Responden

Penelitian ini melibatkan 33 responden mahasiswa aktif yang menggunakan media sosial, khususnya Instagram, TikTok, dan WhatsApp, dalam aktivitas digital sehari-hari. Seluruh responden memenuhi kriteria purposive sampling, yaitu mengakses media sosial minimal satu kali dalam sehari. Karakteristik ini menunjukkan bahwa responden merupakan kelompok pengguna aktif yang berpotensi tinggi terekspos terhadap risiko keamanan data pribadi, sehingga relevan untuk dianalisis dalam konteks kesadaran keamanan data (Hastuti et al., 2024).

Hasil Pengukuran Dimensi Knowledge (Pengetahuan)

Hasil kuesioner menunjukkan bahwa sebagian besar mahasiswa memiliki tingkat pengetahuan yang relatif baik terkait konsep data pribadi dan risiko keamanan di media sosial. Mayoritas responden memahami bahwa data seperti alamat email, nomor telepon, foto pribadi, serta data biometrik termasuk ke dalam kategori data pribadi yang perlu dilindungi. Selain itu, responden juga menunjukkan pemahaman terhadap ancaman umum seperti phishing, penyalahgunaan akun, dan kebocoran data.

Temuan ini mengindikasikan bahwa paparan informasi mengenai keamanan data, baik melalui media, pendidikan formal, maupun pengalaman pribadi, telah membentuk tingkat literasi dasar yang cukup di kalangan mahasiswa. Hasil ini sejalan dengan penelitian yang menyatakan bahwa mahasiswa umumnya telah memiliki kesadaran kognitif yang baik terkait risiko privasi digital, namun belum tentu diikuti dengan penerapan yang konsisten.

Hasil Pengukuran Dimensi Attitude (Sikap)

Pada dimensi sikap, mayoritas responden menyatakan setuju bahwa perlindungan data pribadi merupakan hal yang penting dan bahwa kebocoran data dapat menimbulkan dampak negatif, baik secara sosial maupun akademik. Responden juga menunjukkan tingkat kekhawatiran tertentu terhadap potensi penyalahgunaan data pribadi di media sosial (Juli et al., 2025).

Namun, meskipun sikap yang ditunjukkan cenderung positif, tingkat kepedulian tersebut belum sepenuhnya mencerminkan urgensi perlindungan data dalam praktik sehari-hari. Hal ini terlihat dari masih adanya responden yang menganggap pengaturan privasi sebagai hal yang

tidak terlalu mendesak atau hanya dilakukan ketika terjadi masalah. Kondisi ini menunjukkan bahwa sikap positif belum sepenuhnya terinternalisasi menjadi komitmen perlindungan data yang kuat.

Hasil Pengukuran Dimensi Behavior (Perilaku)

Berbeda dengan dimensi pengetahuan dan sikap, dimensi perilaku menunjukkan hasil yang relatif lebih rendah. Sebagian responden mengaku jarang melakukan pengaturan ulang privasi akun, tidak secara rutin mengganti kata sandi, serta belum sepenuhnya memanfaatkan fitur keamanan tambahan seperti autentikasi dua faktor (2FA) (Sadeli & Irawati, 2023).

Selain itu, masih ditemukan perilaku berisiko, seperti penggunaan kata sandi yang sama pada beberapa platform media sosial dan kecenderungan membagikan informasi pribadi tanpa pertimbangan risiko jangka panjang. Temuan ini menunjukkan bahwa meskipun mahasiswa mengetahui pentingnya keamanan data dan memiliki sikap yang cukup positif, hal tersebut belum diterjemahkan ke dalam tindakan nyata yang konsisten.

Analisis Kesenjangan antara Knowledge, Attitude, dan Behavior

Hasil penelitian ini menegaskan adanya kesenjangan signifikan antara pengetahuan dan perilaku mahasiswa dalam menjaga keamanan data pribadi di media sosial. Pengetahuan yang relatif tinggi tidak secara otomatis menghasilkan perilaku perlindungan data yang baik. Fenomena ini dikenal sebagai *knowledge-behavior gap*, yang juga ditemukan dalam berbagai penelitian keamanan informasi sebelumnya.

Salah satu faktor yang diduga berkontribusi terhadap kesenjangan ini adalah persepsi risiko yang masih rendah. Mahasiswa cenderung merasa bahwa ancaman keamanan data bersifat abstrak atau tidak berdampak langsung, sehingga mengurangi motivasi untuk menerapkan langkah-langkah keamanan secara konsisten. Selain itu, faktor kenyamanan penggunaan media sosial dan kompleksitas pengaturan privasi juga menjadi penghambat dalam perubahan perilaku.

Implikasi terhadap Keamanan Data Mahasiswa

Temuan penelitian ini memiliki implikasi penting terhadap upaya peningkatan keamanan data pribadi di lingkungan perguruan tinggi. Hasil menunjukkan bahwa pendekatan edukasi yang hanya berfokus pada peningkatan pengetahuan belum cukup efektif. Diperlukan strategi yang mendorong perubahan perilaku, seperti pelatihan praktis, simulasi ancaman siber, serta integrasi materi keamanan data ke dalam kurikulum.

Selain itu, keberadaan Undang-Undang Pelindungan Data Pribadi (UU PDP) menuntut mahasiswa tidak hanya sebagai subjek yang dilindungi, tetapi juga sebagai individu yang

bertanggung jawab terhadap pengelolaan data pribadinya sendiri. Tanpa perilaku yang konsisten, perlindungan hukum yang ada tidak akan berjalan secara optimal.

5. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa mahasiswa memiliki tingkat pengetahuan dan sikap yang cukup baik terkait pentingnya perlindungan data pribadi dalam penggunaan media sosial. Mahasiswa umumnya telah memahami jenis data pribadi serta risiko keamanan yang mungkin terjadi. Namun, pada dimensi perilaku, masih ditemukan kelemahan dalam penerapan langkah-langkah perlindungan data secara konsisten, seperti pengaturan privasi akun dan penggunaan fitur keamanan tambahan. Temuan ini menunjukkan adanya kesenjangan antara pengetahuan, sikap, dan perilaku mahasiswa dalam menjaga keamanan data pribadi di media sosial.

Saran

Berdasarkan kesimpulan tersebut, disarankan agar perguruan tinggi tidak hanya memberikan edukasi teoretis mengenai keamanan data pribadi, tetapi juga menyelenggarakan pelatihan praktis yang mendorong perubahan perilaku mahasiswa. Mahasiswa diharapkan lebih meningkatkan kesadaran dan konsistensi dalam menerapkan praktik keamanan data pribadi saat bermedia sosial. Selain itu, diperlukan peran aktif pemerintah dalam meningkatkan sosialisasi Undang-Undang Pelindungan Data Pribadi agar kesadaran hukum dan perlindungan data pribadi di kalangan mahasiswa dapat berjalan lebih optimal.

DAFTAR REFERENSI

- Abdullah, A. M. (2024). Pelindungan hak privasi terhadap pengumpulan data pribadi oleh AI generatif berdasarkan percakapan dengan pengguna. *Padjadjaran Law Review*, 12(2), 145–156. <https://doi.org/10.56895/plr.v12i2.1796>
- Breckner, B. E., Rădulescu, V. D., & Varga, C. (2011). Infinitely many solutions for the Dirichlet problem on the Sierpinski gasket. *Analysis and Applications*, 9(3), 235–248. <https://doi.org/10.1142/S0219530511001844>
- Elrayah, M., & Jamil, S. (2023). Impact of digital literacy and online privacy concerns on cybersecurity behaviour: The moderating role of cybersecurity awareness. *International Journal of Cyber Criminology*, 17(2), 166–187. <https://doi.org/10.5281/zenodo.4766711>
- Farida, N., Bakhtiar, A., & Rif'at, M. (2023). Analisis kesadaran keamanan informasi dan privasi pengguna Instagram. *Jurnal Informatika dan Sistem Informasi*, 415–420. <https://jurnal.uisu.ac.id/index.php/informasi/article/view/7803>

- Fattah, A., Wagimin, & Nurlia. (2023). Enhancing cybersecurity awareness among university students: A study on the relationship between knowledge, attitude, behavior, and training. *JSI: Jurnal Sistem Informasi (E-Journal)*, 15(1), 3139–3149. <https://doi.org/10.18495/jsi.v15i1.115>
- Firmansyah, R., & Darmawan, D. (2020). Kesadaran masyarakat terhadap perlindungan data pribadi di era digital. *Jurnal Ilmiah Komputer dan Informatika*, 8(2), 123.
- Hastuti, P. T., Fitriandra, B., & Lestari, S. (2024). Kesadaran dan perlindungan privasi dalam penggunaan media sosial. *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB)*, 518–523. <https://ojs.udb.ac.id/Senatib/article/view/4641>
- Jayasinghe, S., Johnson, L. W., Udayanga, N., Kumarapperuma, L., & Ranjitha, S. (2023). Drivers enabling developing countries to enter high-tech production networks through global production sharing: Evidence from Malaysia, Taiwan, and Vietnam. *Sustainability*, 15(3), Article 2154. <https://doi.org/10.3390/su15032154>
- Judijanto, L., Lubis, A. F., Karauwan, D. E. S., Bungin, S. S., & Mau, H. A. (2024). Efektivitas kebijakan perlindungan data pribadi dalam menjaga hak asasi manusia di era teknologi di Indonesia. *Sanskara Hukum dan HAM*, 3(1), 34–42. <https://doi.org/10.58812/shh.v3i01.445>
- Juli, N., Carisa, F., & Saputra, D. A. (2025). Pengaruh kesadaran mahasiswa teknologi informasi Universitas Bangka Belitung terhadap keamanan data pribadi. *Jurnal Teknologi Informasi*, 3(2), 425–428.
- Kurnia, F., Salsabila, A., Haniah, M., & Federal, R. (2025). Peningkatan literasi digital dalam perlindungan data pribadi masyarakat. *Abdi Laksana: Jurnal Pengabdian kepada Masyarakat*, 6(2), 352–360.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Priyantiwi, R. D. (2025). Ensuring legal protection of personal data in Indonesia's digital identity system. *Justitia Jurnal Hukum*, 9(2), 205–215. <https://doi.org/10.36501/justitia.v1i2.205>
- Puwa, S. I. P., Puluulawa, F. U., & Rahim, E. I. (2023). Gagasan ideal pengaturan perlindungan data pribadi sebagai bentuk hak privasi di Indonesia. *PALAR (Pakuan Law Review)*, 9(2), 25–37.
- Rahman, B. C. U. A. A. (2024). Analisis kesadaran keamanan data pribadi pada pengguna e-wallet DANA. *Jurnal Riset Sains dan Teknologi*, 8(2), 155–166.
- Sadeli, A. F., & Irawati, I. (2023). Awareness of personal data protection law in concern to literacy. *Jurnal Kajian Informasi & Perpustakaan*, 11(2), 241–256.
- Saputra, D. F. (2023). Literasi digital untuk perlindungan data pribadi. *Jurnal Ilmu Kepolisian*, 17(3), 1–8.
- Setiawan, A. B. (2018). Revolusi bisnis berbasis platform sebagai penggerak ekonomi digital di Indonesia. *Masyarakat Telematika dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi*, 9(1), 61. <https://doi.org/10.17933/mti.v9i1.118>
- Yel, M. B., & Nasution, M. K. M. (2022). Keamanan informasi digital pribadi pada media sosial. *Jurnal Informatika Kaputama*, 6(1), 92–101.