

Analisis Tingkat Kesadaran Keamanan dan Privasi Data di Kalangan Civitas Akademika Menggunakan Model Knowledge-Attitude-Practice

Putu Wida Gunawan^{1*}, I Gede Pramana Ade Saputra²

^{1,2} Program Studi Teknik Informatika, Universitas Dhyana Pura

*putuwida@undhirabali.ac.id

Abstrak

Transformasi digital yang pesat di perguruan tinggi meningkatkan risiko kebocoran data dan ancaman keamanan informasi. Penelitian ini menganalisis tingkat pengetahuan, sikap, dan praktik (Knowledge, Attitude, Practice/KAP) terkait keamanan dan privasi data di kalangan civitas akademika Universitas XYZ. Pendekatan kuantitatif berbasis survei digunakan dengan instrumen KAP sebanyak 30 butir skala Likert yang diujikan melalui pilot study kepada 112 responden yang terdiri atas mahasiswa, dosen, dan tenaga kependidikan. Analisis deskriptif menunjukkan bahwa pengetahuan berada pada kategori baik (mean = 34,98/50), sikap sangat baik (mean = 37,39/50), sedangkan praktik hanya berada pada kategori cukup (mean = 31,30/50). Temuan ini mengindikasikan bahwa sebagian besar responden memahami konsep dasar keamanan dan privasi data serta memiliki sikap positif terhadap perlindungan data pribadi, namun belum secara konsisten menerapkan perilaku digital yang aman, seperti penggantian kata sandi berkala, aktivasi autentikasi dua faktor, dan verifikasi tanda tangan digital. Temuan utama menunjukkan adanya kesenjangan signifikan antara sikap yang tinggi dan praktik keamanan yang relatif rendah, yang mencerminkan privacy paradox di lingkungan kampus. Hasil pilot study ini menjadi dasar untuk penyempurnaan instrumen dan perancangan studi skala penuh guna mengkaji faktor-faktor yang memengaruhi perilaku keamanan digital di perguruan tinggi.

Kata kunci : Keamanan Data, Kesadaran Digital, Model KAP, Privasi Data

Abstract

The rapid digital transformation in higher education increases the risk of data breaches and information security threats. This study analyzes the level of knowledge, attitude, and practice (KAP) regarding data security and privacy among academic community members at Universitas XYZ. A quantitative survey design was employed using a 30-item KAP instrument on a Likert scale, administered in a pilot study to 112 respondents consisting of students, lecturers, and administrative staff. Descriptive analysis shows that knowledge is at a good level (mean = 34.98/50), attitude is very good (mean = 37.39/50), while practice is only at a fair level (mean = 31.30/50). These results indicate that most respondents understand basic concepts of data security and privacy, and have a positive attitude toward protection of personal data, but have not consistently implemented secure digital behaviors in daily activities, such as password rotation, activation of two-factor authentication, and verification of digital signatures. The main finding reveals a significant gap between high attitudes and relatively low security practices, reflecting a privacy paradox in the campus context. The pilot study provides a strong basis to refine the KAP instrument and design a full-scale study to further explore factors influencing digital security behavior in higher education environments..

Keywords : Data Privacy, Data Security, Digital Awareness, Knowledge-Attitude-Practice (KAP)

1. Pendahuluan

Isu keamanan informasi dan privasi data menjadi perhatian global yang semakin mendesak, terutama di lingkungan perguruan tinggi yang kini

sangat bergantung pada teknologi digital. Perguruan tinggi menghadapi risiko kebocoran data, serangan siber, dan penyalahgunaan informasi pribadi yang dapat merusak reputasi

institusi dan merugikan sivitas akademika. Di tingkat internasional, perkembangan teknologi seperti metaverse dan *big data* menimbulkan tantangan baru terkait pengelolaan data tiga dimensi, algoritma, dan ketergantungan pada perusahaan swasta, yang berpotensi mengancam privasi dan otonomi akademik^{[1],[2]}. Di tingkat nasional, fenomena serupa terjadi dengan meningkatnya penggunaan media sosial dan platform digital di kalangan mahasiswa, yang sering kali belum diimbangi dengan kesadaran dan keterampilan menjaga keamanan data pribadi^{[3],[4]}.

Menanggapi isu tersebut, para peneliti berupaya mengembangkan kerangka kerja dan instrumen untuk mengukur dan meningkatkan kesadaran keamanan informasi (Information Security Awareness/ISA) di perguruan tinggi. Salah satu respons penting adalah pengembangan skala pengukuran ISA yang komprehensif, seperti Academia InfoSec Awareness Scale (AIAS), yang mengintegrasikan dimensi pengetahuan, sikap, perilaku, tanggung jawab individu, dan pengaruh sosial^[5]. Selain itu, penelitian juga menyoroti pentingnya pendekatan holistik yang melibatkan pelatihan, kebijakan institusional, dan penguatan budaya keamanan siber untuk mengatasi kerentanan yang disebabkan oleh faktor manusia^{[6],[7]}. Ada juga kajian tentang dampak teknologi baru seperti *big data* dan metaverse terhadap keamanan dan privasi, serta

mengusulkan strategi mitigasi yang adaptif dan berkelanjutan ^{[1],[8]}.

Penelitian sebelumnya telah banyak mengungkapkan tingkat kesadaran keamanan informasi yang masih beragam di kalangan sivitas akademika, dengan kecenderungan pengetahuan dan sikap yang moderat namun praktik yang belum optimal^{[3],[4],[5]}. Studi literatur sistematis menunjukkan bahwa manajemen keamanan informasi di perguruan tinggi masih kurang mendapat perhatian dibanding sektor lain, dengan kebutuhan mendesak untuk penelitian yang lebih mendalam tentang budaya keamanan, perbandingan antar institusi, dan aspek ekonomi keamanan informasi^[6]. Namun, terdapat gap signifikan dalam pemahaman pengaruh faktor sosial dan tanggung jawab individu terhadap ISA, serta kurangnya instrumen yang mengakomodasi dimensi tersebut secara menyeluruh^[5]. Selain itu, isu privasi data dalam konteks teknologi canggih seperti metaverse dan *big data* masih relatif baru dan kurang dieksplorasi secara empiris, terutama terkait persepsi dan kesiapan sivitas akademika dalam menghadapi risiko tersebut ^{[1],[2]}.

Integrasi dimensi sosial dan tanggung jawab individu dalam pengukuran ISA, yang didukung oleh teori perilaku terencana (Theory of Planned Behavior) dan model Knowledge-Attitude-Practice (KAP) yang relevan dalam konteks keamanan informasi relatif baru^[5]. Pendekatan ini memungkinkan pemahaman yang lebih

komprehensif tentang bagaimana pengetahuan dan sikap dipengaruhi oleh faktor eksternal dan internal, serta bagaimana hal tersebut memengaruhi perilaku keamanan. Selain itu, penelitian ini mengadopsi kerangka konseptual yang menggabungkan aspek teknis dan etis, termasuk perlindungan data pribadi dan etika penggunaan teknologi baru, sehingga memberikan kontribusi teoritis dan praktis yang signifikan dalam pengembangan kebijakan keamanan di perguruan tinggi^{[1][7]}.

Penelitian ini berfokus pada pengukuran dan analisis tingkat kesadaran keamanan informasi dan privasi data di kalangan sivitas akademika perguruan tinggi dengan menggunakan skala yang mengakomodasi dimensi pengetahuan, sikap, perilaku, tanggung jawab individu, dan pengaruh sosial. Penelitian juga bertujuan mengidentifikasi faktor-faktor yang memengaruhi kesadaran tersebut serta mengungkap gap antara kesadaran dan praktik nyata dalam menjaga keamanan data pribadi. Hasil penelitian diharapkan dapat memberikan rekomendasi strategis bagi pengembangan program pelatihan, kebijakan institusional, dan intervensi yang efektif untuk meningkatkan keamanan informasi dan perlindungan privasi di lingkungan akademik.

2. Tinjauan Pustaka

2.1. Penelitian Terkait

Dalam penelitian ini, penulis merujuk pada sejumlah penelitian terdahulu sebagai acuan, diantaranya:

- Alammary et al. dengan kesimpulan faktor yang meningkatkan kesadaran adalah persepsi keamanan, familiaritas aplikasi, dan literasi digital, sementara sikap terhadap TIK justru negatif di dosen senior. Temuan ini menekankan perlunya pelatihan terarah bagi dosen^[9].
- Adamova et al. menyurvei 370 mahasiswa S1 dan S2 (Ilmu Komputer & Rekayasa Perangkat Lunak) untuk mengukur tingkat kesadaran terhadap keamanan dan privasi perangkat IoT. Kuesioner mencakup pengetahuan umum IoT, langkah pengamanan, ancaman & kerentanan, serta kebijakan/praktik dan tanggung jawab bersama^[10].
- Rohan et al. mengembangkan Academia InfoSec Awareness Scale (AIAS) untuk mengukur kesadaran keamanan informasi di perguruan tinggi. Analisis multigrup menunjukkan perbedaan kesadaran antara mahasiswa, dosen, dan staf non-akademik, sehingga dapat digunakan untuk merancang intervensi yang lebih spesifik^[5].
- Pratama et al. mengukur security awareness terhadap akun SSO. Analisis regresi menunjukkan adanya kesenjangan generasi, di mana mahasiswa memiliki kesadaran lebih

rendah dibanding dosen dan staf, tanpa perbedaan signifikan berdasarkan gender^[11].

- I Gede et al. mendapatkan hasil Kesadaran “baik”: 85% (keamanan informasi), 89% (privasi), sedangkan Perilaku di area password, perangkat mobile, insiden, dan login masih “rata-rata” sehingga perlu sosialisasi/pelatihan^[12].

2.2. Landasan Teori

1 Keamanan Informasi dan Keamanan Siber.

Keamanan informasi mencakup upaya menjaga kerahasiaan, integritas, dan ketersediaan data digital dari ancaman seperti pencurian, kebocoran, dan modifikasi tidak sah^{[12][13]}. Di lingkungan perguruan tinggi, aset informasi mencakup data akademik, administratif, dan data pribadi sivitas akademika yang banyak diproses melalui sistem digital (SSO, LMS, video conference, email, IoT, dsb.)^{[9][11][12]}.

2 Konsep *Information Security Awareness* (ISA) / *Cybersecurity Awareness*. ISA didefinisikan sebagai tingkat pemahaman, sikap, dan perilaku individu terhadap ancaman keamanan informasi serta tindakan yang tepat untuk melindunginya^{[5][13]}. ISA dianggap sebagai salah satu mekanisme kunci untuk mengurangi risiko serangan siber di institusi pendidikan tinggi^{[5][14][15]}.

3 Model *Knowledge–Attitude–Behavior* (KAB). Model *Knowledge–Attitude–Behavior* (KAB) atau

Knowledge–Attitude–Practice (KAP) banyak dipakai untuk menjelaskan bagaimana pengetahuan memengaruhi sikap, dan keduanya membentuk perilaku aktual terkait keamanan informasi^{[9][14][15]}. Pengetahuan (*Knowledge*) adalah pemahaman tentang ancaman, kebijakan, prosedur, dan cara pengamanan (misalnya pengaturan privasi, enkripsi, otentikasi)^{[9][10][15]}. Sikap (*Attitude*) adalah keyakinan, persepsi risiko, dan nilai yang diberikan terhadap pentingnya menjaga keamanan data^{[9][14][15]}. Perilaku (*Behavior/Practice*) didefinisikan sebagai tindakan konkret, seperti membuat kata sandi kuat, mengaktifkan pengaturan privasi, melaporkan insiden, dan menghindari tautan penipuan seperti *phishing*^{[12][15]}.

Regulasi, Literasi Privasi, dan Tanggung Jawab Individu. Regulasi dapat dipahami sebagai seluruh aturan hukum yang mengatur pengumpulan, pemrosesan, penyimpanan, dan penggunaan data pribadi serta hak privasi individu di ruang digital. Dalam konteks ini, regulasi kunci meliputi: UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022 / UU PDP) yang memberikan kerangka komprehensif perlindungan data pribadi dan mengatur kewajiban pengendali/pemroses data serta hak subjek data^{[16][17][18]}. UU ITE dan perubahannya, serta PP PSTE, yang menekankan kewajiban memperoleh persetujuan (*consent*) pemilik data sebelum data pribadi digunakan, dan menjadikan hak atas privasi

sebagai bagian dari hak asasi yang harus dijaga negara^{[17][19][20]}

menafsirkan temuan berdasarkan teori dan menyusun simpulan serta saran.

3. Metode Penelitian

Jenis penelitian ini adalah kuantitatif deskriptif dengan pendekatan survei K.A.P. Instrumen yang digunakan adalah kuesioner berbasis tiga dimensi utama yaitu: *Knowledge*, *Attitude* dan *Practice* yang masing masing dibuatkan 10 item pernyataan dengan skala Likert 1–5.

3.1. Tahap Penelitian

Tahapan penelitian dalam penelitian ini adalah:

1. Identifikasi masalah dan menentukan variabel seperti: regulasi, literasi privasi, tanggung jawab individual, serta hubungan antarvariabel.
2. Studi pustaka dan penyusunan kerangka teori. Mengkaji teori dan penelitian terdahulu untuk mendefinisikan dan menyusun indikator kuesioner yang valid secara konseptual.
3. Perancangan instrumen kuesioner. Menentukan skala (menggunakan skala Likert 1–5). Menyusun butir pernyataan untuk tiap dimensi.
4. Pengumpulan data. Setelah instrumen final, kuesioner disebar ke sampel yang sudah ditentukan, secara online (Google Form)
5. Pengolahan dan analisis data. Analisis deskriptif (mean, SD, frekuensi) dan inferensial sesuai tujuan dilakukan setelah data setelah data cukup. Interpretasi hasil dan

3.2. Metode Pengumpulan Data

Penelitian menggunakan data primer dengan metode Kuesioner Terstruktur (Survey). Alat utama pengumpulan data kuantitatif adalah kuesioner yang berisi pertanyaan tertutup/terstruktur, dapat disebar secara daring.

3.3. Metode Analisis Data

Metode yang digunakan adalah Analisis deskriptif KAP. Data akan dianalisis menggunakan software statistik dengan menghitung rerata, standar deviasi, median, minimum–maksimum persentase untuk setiap dimensi (*knowledge*, *attitude*, *practice*).

3.4. Lokasi Penelitian

Untuk menjaga privasi dan keamanan data yang dipublikasikan pada penelitian ini, maka penulis menyamarkan lokasi penelitian dimana Lokasi penelitian dilakukan di sebuah institusi pendidikan tinggi yaitu Universitas XYZ.

4. Hasil dan Pembahasan

4.1. Hasil Penelitian

Dari 112 responden yang mengisi kuesioner KAP berjumlah 30 item dengan skala Likert lima poin, valid untuk dianalisis setelah dilakukan proses *cleaning* dan *reverse scoring* pada item negatif.

Tidak ditemukan nilai kosong yang signifikan sehingga seluruh respons dapat digunakan dalam analisis statistik lanjutan.

- Pada dimensi pengetahuan (*Knowledge*), responden umumnya memahami konsep dasar keamanan dan privasi data, seperti definisi data pribadi, perbedaan tanda tangan digital dengan hasil pemindaian, serta peran autentikasi dua faktor dalam melindungi akun digital.
- Pada dimensi sikap (*Attitude*), responden secara umum menyatakan persetujuan terhadap pentingnya perlindungan data pribadi, tanggung jawab bersama antara kampus dan pengguna, serta perlunya investasi institusi pada mekanisme keamanan seperti enkripsi dan autentikasi dua faktor. Namun, masih ada yang menunjukkan sikap permisif terhadap penggunaan kata sandi yang sama pada beberapa akun demi kemudahan.
- Pada dimensi praktik (*Practice*), beberapa item menunjukkan nilai rata-rata yang lebih rendah dibandingkan dua dimensi lainnya. Temuan ini terutama terlihat pada praktik keamanan seperti kebiasaan mengganti kata sandi secara berkala, penerapan autentikasi dua faktor, verifikasi tanda tangan digital, serta membagikan kata sandi kepada orang yang sudah dipercaya. Pola ini mengindikasikan bahwa praktik keamanan

digital belum sepenuhnya diterapkan secara konsisten oleh responden.

- Rekapitulasi statistik per dimensi menunjukkan perbedaan yang jelas antara pengetahuan, sikap, dan praktik keamanan data. Nilai rata-rata dimensi *Knowledge* tercatat sebesar 34,98, diikuti oleh *Attitude* dengan nilai rata-rata 37,39, sedangkan *Practice* memiliki nilai rata-rata terendah yaitu 31,30. Total skor KAP memiliki nilai rata-rata 103,67 dengan sebaran data yang relatif moderat..

4.2. Pembahasan

Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan dan privasi data pada Universitas XYZ memperlihatkan pola yang tidak merata antar dimensi *Knowledge*, *Attitude*, dan *Practice*. Dimensi sikap (*Attitude*) memiliki skor rata-rata tertinggi, diikuti oleh pengetahuan (*Knowledge*), sementara praktik (*Practice*) berada pada posisi terendah. Pola ini mengindikasikan bahwa responden memiliki kepedulian dan pandangan positif terhadap pentingnya keamanan dan privasi data, namun pada penerapan perilaku keamanan digital dalam aktivitas sehari-hari belum dilakukan secara konsisten.

- Dalam konteks keamanan informasi, hubungan antar dimensi KAP sering kali dipengaruhi oleh faktor situasional,

kebiasaan, serta persepsi kemudahan dan risiko. Skor pengetahuan yang relatif baik menunjukkan bahwa responden telah memahami konsep dasar keamanan dan privasi data, seperti perlindungan data pribadi, autentikasi, dan tanggung jawab pengelolaan data. Namun, pengetahuan tersebut belum sepenuhnya diterjemahkan menjadi tindakan nyata.

- Tingginya skor sikap menunjukkan adanya kesadaran normatif yang kuat, di mana responden mengakui pentingnya perlindungan data pribadi dan mendukung penerapan kebijakan keamanan informasi di lingkungan kampus. Sikap positif ini mencerminkan adanya penerimaan nilai terhadap prinsip-prinsip keamanan data. Akan tetapi, kesenjangan antara sikap dan praktik yang ditemukan dalam penelitian ini menguatkan keberadaan fenomena *privacy paradox*, yaitu kondisi ketika individu menyatakan kepedulian tinggi terhadap privasi dan keamanan data, namun tetap melakukan perilaku yang berisiko, seperti penggunaan kata sandi yang lemah, tidak mengaktifkan autentikasi dua faktor, atau membagikan kredensial akun.
- Rendahnya skor pada dimensi praktik dapat disebabkan karena beberapa faktor. Pertama, praktik keamanan digital sering kali dianggap sebagai aktivitas tambahan yang

memerlukan usaha dan waktu lebih, sehingga kurang diprioritaskan dalam rutinitas akademik. Kedua, absennya pelatihan keamanan siber yang terstruktur dan berkelanjutan dapat menyebabkan pengguna tidak memiliki keterampilan praktis yang memadai meskipun memiliki pengetahuan konseptual. Ketiga, budaya keamanan informasi di lingkungan perguruan tinggi masih cenderung reaktif, yaitu baru diperhatikan setelah terjadi insiden, bukan bersifat preventif.

5. Kesimpulan

Penelitian mengenai tingkat kesadaran keamanan dan privasi data civitas akademika Universitas XYZ dengan model *Knowledge-Attitude-Practice (KAP)* menyimpulkan beberapa hal berikut (1) Pada dimensi pengetahuan (*Knowledge*), responden umumnya memahami konsep dasar keamanan dan privasi data, seperti definisi data pribadi, perbedaan tanda tangan digital dengan hasil pemindaian, serta peran autentikasi dua faktor dalam melindungi akun digital. Tingkat pengetahuan civitas akademika tentang keamanan dan privasi data berada pada kategori cukup baik (mean 34,98/50 atau 69,96. (2) Sikap terhadap keamanan dan privasi data berada pada kategori sangat baik (mean 37,39/50 atau 74,78%). Responden memandang data pribadi sebagai aset penting dan mendukung

penerapan mekanisme keamanan seperti 2FA, enkripsi, dan audit keamanan, serta mengharapkan transparansi institusi saat terjadi insiden kebocoran data. (3) Praktik keamanan dan privasi data masih berada pada kategori cukup dan menjadi aspek terlemah (mean 31,30/50 atau 62,6%), dengan perilaku berisiko seperti jarang mengganti kata sandi, tidak mengaktifkan 2FA, serta penggunaan kata sandi berulang. Secara keseluruhan, penelitian ini menyimpulkan adanya kesenjangan yang jelas antara pengetahuan dan sikap yang relatif tinggi dengan praktik keamanan data yang masih rendah, sehingga diperlukan intervensi lanjutan berupa penguatan kebijakan, pelatihan praktis, dan perbaikan instrumen untuk studi skala penuh di masa mendatang.

6. Daftar Pustaka

- [1] N. Gündüz and M. Sincar, "Data Privacy And Security Challenges In Metaversities: The Ethical Dilemmas In The Future Of Higher Education," *Problems of Education in the 21st Century*, vol. 83, no. 4, pp. 525–544, Aug. 2025, doi: 10.33225/pec/25.83.525.
- [2] D. Florea and S. Florea, "Big Data and the Ethical Implications of Data Privacy in Higher Education Research," *Sustainability*, vol. 12, no. 20, p. 8744, 2020, doi: 10.3390/su12208744.
- [3] 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.
- [4] J. P. Runtuwene, R. A. Mege, V. R. Palilingan, and J. R. Batmetan, "Information Security Awareness on Data Privacy in Higher Education," in *Proceedings of the 5th UPI International Conference on Technical and Vocational Education and Training (ICTVET 2018)*, Atlantis Press, 2019, doi: 10.2991/ictvet-18.2019.38.
- [5] R. Rohan, W. Chutimaskul, R. Roy, J. Hautamäki, S. Funilkul, and D. Pal, "Developing a scale for measuring the information security awareness of stakeholders in higher education institutions," *Educ. Inf. Technol. (Dordr.)*, vol. 30, no. 10, pp. 13713–13777, 2025, doi: 10.1007/s10639-024-13307-5.
- [6] I. Bongiovanni, "The least secure places in the universe? A systematic literature review on information security management in higher education," *Comput. Secur.*, vol. 86, pp. 350–357, 2019, doi: 10.1016/j.cose.2019.07.003.
- [7] R. Rohan, S. Funilkul, W. Chutimaskul, P. Kanthmanon, B. Papasratorn, and D. Pal, "Information Security Awareness in Higher Education Institutes: A Work in Progress," in *2023 15th International Conference on Knowledge and Smart Technology (KST)*, IEEE, Feb. 2023, pp. 1–6, doi: 10.1109/KST57286.2023.10086884.
- [8] Y. Cheng and S. Zhang, "Issues and Countermeasures of Information Network Security in the Context of Big Data for Higher Education Institutions," *The Frontiers of Society, Science and Technology*, vol. 5, no. 13, 2023, doi: 10.25236/FSST.2023.051301.
- [9] A. Alammery, M. Alshaikh, and A. R. Pratama, "Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic," *PeerJ Comput. Sci.*, vol. 8, p. e1021, Jul. 2022, doi: 10.7717/peerj-cs.1021.

- [10] A. Adamova, T. Zhukabayeva, M. Zhartybayeva, and L. Zhumabayeva, "Assessing the knowledge and practices of internet of things security and privacy among higher education students," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 15, no. 4, p. 4074, Aug. 2025, doi: 10.11591/ijece.v15i4.pp4074-4086.
- [11] A. R. Pratama, F. M. Firmansyah, and F. Rahma, "Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality," *PeerJ Comput. Sci.*, vol. 8, p. e918, Mar. 2022, doi: 10.7717/peerj-cs.918.
- [12] I. G. A. Sukariana Yasa, I. M. E. Listartha, and I. M. A. Pradnyana, "MEASUREMENT OF INFORMATION SECURITY AND PRIVACY AWARENESS USING THE MULTIPLE CRITERIA DECISION ANALYSIS (MCDA) METHOD," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 4, pp. 759–768, Aug. 2023, doi: 10.52436/1.jutif.2023.4.4.692.
- [13] S. S. Kaleli, "Measuring Digital Data Security Awareness: The Case of Higher Education Institution," *Journal of Studies in Advanced Technologies*, vol. 2, no. 2, pp. 108–119, 2024, doi: 10.63063/jsat.1591281.
- [14] Q. An, W. C. H. Hong, X. Xu, Y. Zhang, and K. Kolletar-Zhu, "How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates," *Int. J. Inf. Secur.*, vol. 22, no. 2, pp. 305–317, Apr. 2023, doi: 10.1007/s10207-022-00637-z.
- [15] M. M. Chumaera, Safitri, and M. A. Ayu, "Assessing Students' Information Security Awareness through the Knowledge, Attitude, and Behavior Model," in *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED)*, IEEE, Jul. 2022, pp. 1–6. doi: 10.1109/ICCED56140.2022.10010455.
- [16] Nur Qoulun Tsakila and Muhammad Irwan Padli Nasution, "Perlindungan Data Privasi dalam Sistem Database Digital: Regulasi, Tinjauan Etika, dan Strategi Teknis," *Maeswara : Jurnal Riset Ilmu Manajemen dan Kewirausahaan*, vol. 3, no. 3, pp. 01–11, May 2025, doi: 10.61132/maeswara.v3i3.1750.
- [17] Ilman Maulana Kholis, "Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia," *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, vol. 4, no. 2, pp. 275–299, Jun. 2025, doi: 10.14421/t5sfe747.
- [18] Tania Tresna Kurnia and Ade Mahmud, "Perlindungan Hukum Data Pribadi Terhadap Korban Kejahatan Akses Ilegal dan Upaya Pencegahannya," *Bandung Conference Series: Law Studies*, vol. 5, no. 2, Jul. 2025, doi: 10.29313/bcsls.v5i2.18503.
- [19] R. Sadillah Ahmad, D. A. Puspaningtyas, and M. N. K. Al Ismariy, "Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital," *The Juris*, vol. 9, no. 1, pp. 15–23, Jun. 2025, doi: 10.56301/juris.v9i1.1307.
- [20] Devi Anjheli, "Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP," *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, vol. 4, no. 1, pp. 165–189, May 2025, doi: 10.14421/990epf27.