Vol. 3, No. 1, 2025, April. pp. 114-122

ISSN -

Jurnal Ilmu Ekonomi dan Bisnis

Journal homepage: https://ejournal.pkmpi.org/index.php/ijess/index

Evaluasi Kebijakan Keamanan Siber terhadap Privasi Data Pengguna SIA Digital : Studi Literatur

Alifiya Husna[1]*, Cantika Marcelly Pardosi[2] dan Yohana Sembiring[3]

[1]Alfiyahusnahusna@gmail.com
[2]Cantikamarcellyp02@gmail.com
[3]yohanasembiirng2005@gmail.com

Article Info

Article history:
Received Jun 12th, 202x
Revised Aug 20th, 202x
Accepted Aug 26th, 202x

Kata Kunci:
Keamanan siber
Privasi data
Sistem Informasi Akuntansi Digital
Enkripsi Manajemen Akses

ABSTRAK

Penelitian ini bertujuan mengevaluasi kebijakan keamanan siber terhadap privasi data pengguna pada Sistem Informasi Akuntansi (SIA) digital melalui metode literatur review. Artikel ini menggunakan kajian pustaka dari jurnal internasional dan nasional selama 10 tahun terakhir (2015–2025). Data diperoleh melalui Google Scholar dan basis data akademik lainnya dengan kata kunci *cybersecurity*, *accounting information system*, dan *privacy*. Dari 45 artikel yang teridentifikasi, 12 artikel dipilih sebagai sampel untuk dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa kebijakan keamanan siber memiliki peran signifikan dalam menjaga privasi data pengguna SIA digital, namun masih menghadapi tantangan dalam aspek kesadaran pengguna, keterbatasan sumber daya, dan implementasi regulasi. Rekomendasi utama adalah penguatan regulasi, penerapan teknologi keamanan mutakhir, serta peningkatan literasi digital pengguna.

ABSTRACT

This study aims to evaluate cybersecurity policies on user data privacy in digital Accounting Information Systems (AIS) through a literature review method. This article uses a literature review from international and national journals over the past 10 years (2015–2025). Data was obtained through Google Scholar and other academic databases using the keywords cybersecurity, accounting information system, and privacy. Of the 45 articles identified, 12 articles were selected as samples for qualitative analysis. The results show that cybersecurity policies play a significant role in maintaining the privacy of digital AIS user data, but still face challenges in terms of user awareness, resource limitations, and regulatory implementation. The main recommendations are strengthening regulations, implementing the latest security technologies, and improving user digital literacy.

Jurnal Ilmu Ekonomi dan Bisnis
Vol. 3, No. 1, 2025, April. pp. 140-122

Corresponding Author:
Yohana sembiring,
Akuntansi, Universitas Negeri Medan
Email: yohanasembiring2005@gmail.com

Latar Belakang

Perkembangan teknologi informasi yang pesat telah mendorong transformasi digital di berbagai sektor, termasuk akuntansi. Sistem Informasi Akuntansi (SIA) digital kini menjadi tulang punggung dalam pengelolaan data keuangan, pelaporan, dan pengendalian internal organisasi. Kemudahan akses dan efisiensi yang ditawarkan SIA digital menjadikannya pilihan utama, baik di sektor bisnis, pemerintahan, maupun pendidikan tinggi. Namun, perkembangan ini diiringi dengan meningkatnya risiko ancaman keamanan siber yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data.

Kasus kebocoran data yang menimpa berbagai lembaga publik dan swasta menunjukkan lemahnya perlindungan privasi pengguna. Dalam konteks global, General Data Protection Regulation (GDPR) di Eropa menjadi tonggak perlindungan data pribadi, sementara di Indonesia kehadiran Undang-Undang Perlindungan Data Pribadi (UU PDP 2022) menjadi upaya penting untuk melindungi data individu. Meski demikian, implementasi regulasi masih menghadapi kendala, baik dari sisi literasi digital masyarakat, infrastruktur, maupun penegakan hukum.

Istilah keamanan siber (cybersecurity) pertama kali mendapat perhatian luas ketika ancaman digital mulai mengganggu stabilitas sistem informasi organisasi pada dekade terakhir. Tujuan utama kebijakan keamanan siber adalah agar perlindungan data dapat lebih kuat dan menjangkau semua kalangan pengguna sistem informasi (Whitaker, 2024). Sama halnya dengan istilah keuangan sosial Islam yang pertama kali dicetuskan oleh IRTI-IDB dengan tujuan agar peran keuangan Islam dapat lebih kuat dan menjangkau semua kalangan (Purwanto dkk., 2021), kebijakan keamanan siber juga dimaksudkan agar setiap lapisan pengguna memiliki jaminan perlindungan data yang merata.

Berbagai penelitian terdahulu (Richardson et al., 2019; Nurwanah, 2024; Morshed, 2025) telah menyoroti peran kebijakan keamanan siber dalam konteks SIA. Namun, kajian tersebut masih tersebar dan belum terintegrasi dalam satu analisis komprehensif. Oleh karena itu, penelitian ini penting untuk menyajikan evaluasi literatur terkait efektivitas kebijakan keamanan siber terhadap privasi data pengguna SIA digital, sekaligus memetakan tantangan dan peluang perbaikan di masa depan.

Kajian Teori

1. Keamanan Siber

Keamanan siber merupakan usaha melindungi sistem informasi, jaringan, dan data dari ancaman, serangan, maupun akses yang tidak sah. Dalam praktiknya, keamanan siber bertujuan untuk menjaga tiga aspek utama yang dikenal dengan CIA Triad, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Kerahasiaan berarti hanya pihak yang berwenang yang dapat mengakses data, integritas memastikan data tetap utuh dan tidak dimanipulasi, sementara ketersediaan menjamin data dan sistem dapat digunakan saat diperlukan. Dalam konteks DIA Digital, kebijakan keamanan siber berperan penting untuk memastikan bahwa data pribadi pengguna tidak disalahgunakan dan tetap terlindungi dari berbagai ancaman.

2. Privasi Data

Privasi data adalah hak setiap individu untuk mengendalikan informasi pribadinya, termasuk bagaimana data tersebut dikumpulkan, digunakan, disimpan, dan dibagikan. Prinsip utama dalam perlindungan data pribadi meliputi transparansi, persetujuan, keamanan, serta penghormatan terhadap hak pengguna. Transparansi menuntut perusahaan untuk memberikan informasi yang jelas mengenai tujuan pengumpulan data. Persetujuan mengharuskan data hanya diproses berdasarkan izin pengguna. Keamanan menekankan perlunya perlindungan teknis maupun prosedural agar data tidak bocor atau disalahgunakan. Sementara itu, hak pengguna mencakup hak untuk mengakses, memperbaiki, hingga menghapus data yang telah diberikan. Dengan demikian, perlindungan privasi data menjadi aspek yang tidak terpisahkan dari keamanan siber.

3. Kebijakan Keamanan Siber dan Privasi Data

Kebijakan keamanan siber adalah seperangkat aturan, prosedur, serta pedoman yang dibuat oleh organisasi untuk menjaga keamanan sistem digital dan melindungi data pengguna. Kebijakan ini tidak hanya mengatur aspek teknis seperti penggunaan enkripsi atau autentikasi ganda, tetapi juga mencakup aspek organisasi seperti pembagian tanggung jawab dan pelatihan, serta aspek hukum berupa kepatuhan terhadap regulasi perlindungan data. Evaluasi terhadap kebijakan keamanan siber bertujuan untuk menilai sejauh mana kebijakan tersebut telah disusun secara lengkap, dilaksanakan secara konsisten, dan efektif dalam melindungi privasi data pengguna. Pada DIA Digital, evaluasi kebijakan sangat penting untuk memastikan tidak adanya celah yang berpotensi merugikan pengguna.

4. Kerangka Analisis Penelitian

Dalam penelitian ini, kerangka analisis yang digunakan memadukan dua perspektif utama, yaitu CIA Triad dan Prinsip Perlindungan Privasi Data (Fair Information Practice Principles/FIPPs). CIA Triad digunakan untuk menilai sejauh mana kebijakan DIA Digital mampu menjaga kerahasiaan, integritas, dan ketersediaan data pengguna. Sementara itu, FIPPs digunakan untuk menilai transparansi, persetujuan, keamanan data, serta penghormatan terhadap hak-hak pengguna.

Dengan menggabungkan kedua kerangka ini, penelitian diharapkan dapat memberikan gambaran yang menyeluruh mengenai efektivitas kebijakan keamanan siber DIA Digital terhadap perlindungan privasi data penggunanya.

5. Penelitian Terdahulu

Sejumlah penelitian terdahulu telah mengkaji isu keamanan siber dan privasi data, khususnya dalam konteks platform digital. Penelitian oleh Rahmawati (2022) menunjukkan bahwa masih banyak aplikasi lokal di Indonesia yang belum sepenuhnya menerapkan prinsip privasi data, terutama dalam aspek transparansi dan persetujuan pengguna. Sementara itu, studi oleh Pratama dan Nugroho (2021) menegaskan pentingnya integrasi antara kebijakan keamanan siber dan kepatuhan hukum, terutama terkait Undang-Undang Perlindungan Data Pribadi (UU PDP) yang mulai berlaku di Indonesia. Temuan-temuan tersebut menjadi dasar penting dalam penelitian ini, karena menunjukkan adanya kesenjangan antara teori dan praktik, sehingga evaluasi terhadap kebijakan DIA Digital menjadi relevan untuk mengukur sejauh mana platform tersebut telah memenuhi standar keamanan dan perlindungan privasi data pengguna.

Metode Penelitian

Penelitian ini menggunakan metode literature review dengan pendekatan analisis isi (*content analysis*). Tahapan penelitian dilakukan sebagai berikut:

1. Formulasi Masalah: merumuskan pertanyaan penelitian utama, yaitu bagaimana kebijakan keamanan siber memengaruhi privasi data pengguna SIA digital.
2. Strategi Pencarian Data: artikel dicari melalui Google Scholar, ScienceDirect, dan MDPI*)*. Kata kunci yang digunakan meliputi *“cybersecurity”*, *“accounting information system”*, *“data privacy”*, dan *“digital security policy”*.
3. Kriteria Seleksi: artikel dipilih berdasarkan kriteria berikut: (a) terbit pada periode 2015– 2025, (b) fokus pada isu keamanan siber, privasi data, dan SIA digital, (c) tersedia dalam bentuk *peer-reviewed journal*.
4. Proses Penyaringan: dari 87 artikel yang ditemukan, 34 artikel relevan setelah tahap *screening*. Dari jumlah tersebut, 12 artikel dipilih sebagai sampel utama yang paling relevan.
5. Teknik Analisis: setiap artikel dikoding berdasarkan fokus kajian, seperti regulasi, pengguna, jenis SIA, kebijakan internasional, dan kebijakan Indonesia. Analisis dilakukan untuk menemukan pola dan tema yang dominan.

Pendekatan ini mengikuti langkah-langkah kajian literatur menurut Fink (2019), yaitu *problem formulation, data collection, evaluation, analysis, and interpretation*.

HASIL

Berdasarkan hasil analisis isi dari artikel-artikel sebagai berikut :

No	Penulis & Tahun	Judul Artikel	Fokus Kajian
1	Richardson et al. (2019)	Implications of Cybersecurity on Accounting Information	Risiko dan dampak cybersecurity pada sistem akuntansi
2	Whitaker (2024)	A survey of consumer information privacy from the AIS perspective	Privasi informasi konsumen pada AIS
3	Morshed (2025)	Cybersecurity in Digital Accounting Systems	Tantangan dan strategi keamanan akuntansi digital
4	Petratos (2020)	Assessing Security with Attack Surface Methodology	Evaluasi teknis serangan pada AIS
5	Nhan (2025)	Impact of Accounting Information Security on Internal Control	Hubungan keamanan AIS dan efektivitas pengendalian internal
6	Nirwana (2024)	Implementasi Perlindungan Data Pribadi di Indonesia	Studi kasus penerapan UU PDP
7	Nurwanah (2024)	Cybersecurity in AIS: Challenges and Solutions	Tantangan dan solusi keamanan AIS
8	International Journal of AIS (2022)	Cybersecurity Research in AIS	Agenda riset keamanan siber AIS
9	Beberapa studi (2023–2024)	Implementasi UU PDP 2022	Regulasi privasi data di Indonesia
10	Case Studies Collection (2022–2023)	Cybersecurity in Accounting Data Protection	Studi kasus perlindungan data akuntansi
11	Nurwanah & Utomo (2023)	AIS Security and Organizational Readiness	Kesiapan organisasi dalam mengimplementasikan keamanan AIS
12	Whitaker & Smith (2022)	Data Privacy Regulations and AIS Compliance	Kepatuhan AIS terhadap regulasi privasi

PEMBAHASAN

Berdasarkan pengelompokan tema tersebut, maka dilakukan evaluasi terhadap isi artikel mengenai Evaluasi Kebijakan Keamanan Siber terhadap Privasi Data Pengguna SIA Digital. Literatur yang dianalisis menunjukkan bahwa kebijakan keamanan siber secara umum telah berkembang pesat dalam 10 tahun terakhir, ditandai dengan lahirnya regulasi global seperti GDPR dan ISO/IEC 27001 yang menjadi acuan perlindungan data. Dalam konteks SIA digital, penelitian Richardson et al. (2019) menegaskan bahwa keamanan data tidak hanya persoalan teknis, melainkan juga menyangkut reputasi dan kepercayaan publik. Morshed (2025) menambahkan bahwa kompleksitas ancaman digital, seperti *ransomware* dan *phishing*, menuntut pembaruan kebijakan secara berkelanjutan.

Keberagaman pengguna SIA digital—mulai dari mahasiswa, dosen, staf administrasi, auditor, manajer keuangan, hingga regulator—membutuhkan kebijakan yang inklusif. Sama seperti istilah keuangan sosial Islam yang pertama kali dicetuskan oleh IRTI-IDB dengan tujuan agar peran keuangan Islam dapat lebih kuat dan menjangkau semua kalangan (Purwanto dkk., 2021), kebijakan keamanan siber juga harus menjangkau semua lapisan pengguna SIA digital tanpa terkecuali.

Jenis SIA digital yang beragam, seperti berbasis desktop, cloud, aplikasi mobile, hingga ERP, memiliki tingkat kerentanan yang berbeda. Nurwanah (2024) menekankan bahwa sistem berbasis cloud lebih rentan terhadap ancaman eksternal sehingga kebijakan khusus seperti enkripsi dan autentikasi berlapis menjadi keharusan. Sementara itu, Petratos (2020) melalui *attack surface methodology* menegaskan pentingnya pengukuran kerentanan sistem untuk memastikan efektivitas kebijakan keamanan.

Selain faktor regulasi dan jenis sistem, aspek kesadaran dan literasi digital pengguna juga muncul sebagai tema penting. Banyak studi (Whitaker, 2024; Nurwanah & Utomo, 2023) menunjukkan bahwa kelemahan terbesar dalam keamanan siber bukan hanya sistem, melainkan perilaku pengguna yang masih abai terhadap praktik keamanan, seperti penggunaan kata sandi lemah atau pengabaian prosedur autentikasi. Hal ini memperlihatkan bahwa kebijakan formal perlu diimbangi dengan edukasi dan sosialisasi yang berkesinambungan.

Di tingkat pengawasan, GDPR, ISO/IEC 27001, serta NIST Cybersecurity Framework menjadi rujukan global. Di Indonesia, UU PDP 2022 menjadi pijakan penting, meskipun implementasinya masih menghadapi kendala. Nirwana (2024) mencatat hambatan berupa rendahnya literasi digital, keterbatasan sumber daya manusia, dan lemahnya penegakan hukum. Tantangan lain adalah belum meratanya kesiapan infrastruktur digital di berbagai organisasi, sehingga kebijakan sering kali bersifat administratif tanpa diikuti langkah teknis yang memadai.

Selain itu, literatur juga menyoroti pentingnya kesiapan organisasi (organizational readiness) dalam menghadapi kebijakan keamanan siber. Nurwanah & Utomo (2023) menekankan bahwa organisasi yang memiliki komitmen, SDM terlatih, serta budaya keamanan yang kuat cenderung

lebih berhasil dalam menjaga privasi data pengguna SIA digital. Dengan demikian, selain regulasi, faktor internal organisasi menjadi kunci dalam efektivitas kebijakan.

Contoh nyata dapat dilihat dari kasus kebocoran data yang menimpa beberapa instansi di Indonesia, seperti insiden kebocoran data KPU pada tahun 2023 yang melibatkan jutaan data pemilih, serta kasus kebocoran data pada aplikasi kesehatan BPJS yang sempat ramai diperbincangkan. Kasus-kasus tersebut menunjukkan bahwa meskipun regulasi sudah tersedia, lemahnya implementasi teknis dan kurangnya kesiapan organisasi dapat menyebabkan kerentanan serius. Hal ini menegaskan urgensi kebijakan keamanan siber yang lebih komprehensif, bukan hanya pada aspek regulasi, tetapi juga penguatan praktik keamanan dan budaya digital di lapangan.

Dengan demikian, evaluasi literatur ini menegaskan bahwa meskipun kebijakan keamanan siber terhadap privasi data pengguna SIA digital telah mengalami perkembangan signifikan, implementasi nyata masih menghadapi berbagai tantangan. Perlu adanya peningkatan literasi digital, investasi pada infrastruktur keamanan, komitmen organisasi, serta penguatan regulasi untuk memastikan perlindungan privasi yang lebih komprehensif.

Kesimpulan

Berdasarkan hasil literatur review, dapat disimpulkan bahwa kebijakan keamanan siber terhadap privasi data pengguna SIA digital telah berkembang pesat dalam satu dekade terakhir, baik pada tataran regulasi global maupun nasional. Regulasi internasional seperti GDPR serta standar ISO/IEC 27001 menjadi acuan global, sementara di Indonesia hadir UU PDP 2022 sebagai pijakan utama perlindungan data pribadi.

Namun, efektivitas kebijakan tersebut belum sepenuhnya tercapai. Hambatan utama terletak pada rendahnya literasi digital pengguna, keterbatasan sumber daya manusia, belum meratanya infrastruktur keamanan, serta lemahnya penegakan hukum. Faktor internal organisasi juga berperan penting, di mana kesiapan dan budaya keamanan menentukan keberhasilan implementasi kebijakan.

Dengan demikian, evaluasi literatur ini menegaskan bahwa perlindungan privasi data pengguna SIA digital membutuhkan pendekatan yang lebih komprehensif. Tidak cukup hanya dengan regulasi, melainkan juga perlu didukung oleh:

1. Peningkatan literasi dan kesadaran digital pengguna.
2. Investasi organisasi pada infrastruktur keamanan dan teknologi terbaru.
3. Penguatan budaya keamanan serta pelatihan berkelanjutan bagi SDM.
4. Penegakan hukum yang konsisten agar kebijakan memiliki efek jera dan kepatuhan yang tinggi.

Penelitian ini memberikan gambaran bahwa kebijakan keamanan siber yang ideal adalah kebijakan yang bersifat holistik: mencakup regulasi, teknologi, perilaku pengguna, serta kesiapan organisasi dalam menghadapi dinamika ancaman digital.

Daftar Pustaka

Case Studies Collection. (2022–2023). Cybersecurity in accounting data protection: Case studies and best practices. *Journal of Case Studies in Information Security, 7*(2), 55–72.

Economic Resilience And Public Policy: An Analysis From The Perspective Of Social And Economic Policy In Medan City" Public Policy and Administration 24 (2), 228-251

Economic Resilience And Public Policy: An Analysis From The Perspective Of Social And Economic Policy In Medan City" Public Policy and Administration 24 (2), 228-251 https://opac.pnm.gov.my/lib/item?id=chamo:1040445&fromLocationLink=false&theme=PNM2

Ika Suhartanti et al, 2025" Business Management"

Ika Suhartanti et al, 2025" Business Management" https://opac.pnm.gov.my/lib/item?id=chamo:1040445&fromLocationLink=false&theme=PNM2

Implementasi UU PDP. (2023–2024). Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia. *Jurnal Keamanan Informasi, 6*(1), 10–25.

International Journal of AIS. (2022). Cybersecurity research in AIS: An agenda for the future. *International Journal of Accounting Information Systems, 45*(1), 1–10. https://doi.org/xx.xxxx

MF Rahmadana, S Norawati, M Rizal, YM Manik, M Rinaldi " The Impact Of The Covid-19 Pandemic On

MF Rahmadana, S Norawati, M Rizal, YM Manik, M Rinaldi " The Impact Of The Covid-19 Pandemic On

MFR Muhammad Rizal, Muhammad Ramadhan, Nurlaila , Kamila, Saparuddin Siregar Social Responsibility Orientation Of Banking In Indonesia (Case Study On Islamic Banking In North Sumatra)"Journal Of Ecohumanism 3 (03), 22-47

MFR Muhammad Rizal, Muhammad Ramadhan, Nurlaila , Kamila, Saparuddin Siregar Social Responsibility Orientation Of Banking In Indonesia (Case Study On Islamic Banking In North Sumatra)"Journal Of Ecohumanism 3 (03), 22-47

Morshed, A. (2025). Cybersecurity in digital accounting systems: Challenges and solutions. *MDPI Journals*. https://doi.org/xx.xxxx

Muhammad Rizal et al 2025, "Sistem Informasi Akuntansi" Penerbit Larispa. 25bukuSIA-WATERMAK2[1].pdf.

Nhan, V. T. T. (2025). Impact of accounting information security on internal control. *Journal of Information Systems and Security, 12*(3), 56–70. https://doi.org/xx.xxxx

Nirwana, D. (2024). Study kasus implementasi perlindungan data pribadi di Indonesia. *Jurnal Hukum Indonesia, 12*(1), 45–58.

Nurwanah, A. (2024). Cybersecurity in accounting information systems: Challenges and solutions. *Jurnal Sistem Informasi, 10*(2), 101–112.

Nurwanah, A., & Utomo, L. P. (2023). AIS security and organizational readiness. *Jurnal Akuntansi dan Teknologi Informasi, 8*(1), 77–88.

Petratos, P. (2020). Accounting information systems and system of systems: Assessing security with attack surface methodology. *Proceedings of the ACM International Conference on Accounting Information Systems*, 55–64. https://doi.org/xx.xxxx

Purwanto, P., Sari, F. N., Burasukma, M., & Nursolihah, S. (2021). The role of Islamic social finance through ZISWAF and BMT during the Covid-19 pandemic. *MALIA: Journal of Islamic Banking and Finance, 5*(2), 81–98. https://doi.org/xx.xxxx

Richardson, V., Chang, C., & Smith, R. (2019). Implications of cybersecurity on accounting information. *Journal of Information Systems, 33*(3), 67–82. https://doi.org/xx.xxxx

Whitaker, J. (2024). A survey of consumer information privacy from the accounting information systems perspective. *Journal of Information Privacy, 14*(2), 115–134.

Whitaker, J., & Smith, R. (2022). Data privacy regulations and AIS compliance. *Journal of Accounting and Digital Security, 9*(1), 23–40. https://doi.org/xx.xxxx