Madani: Jurnal Ilmiah Multidisiplin
Volume 3, Nomor 11, December 2025, P. 384-388
E-ISSN: 2986-6340

DOI: https://doi.org/10.5281/zenodo.17958901

Strategi Perlindungan Data dan Pengendalian Risiko Keamanan Informasi dalam Infrastruktur Digital Nasional

Data Protection Strategy and Information Security Risk Control in National Digital Infrastructure

Windi Antika[1], Muhammad Irwan Padli Nasution[2]
Program Studi Manajemen, Fakultas Ekonomi Dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara, Indonesia
E-mail: [1]wa7812786@gamil.com, [2]irwannst@uinsu.ac.id

Abstrak

Perkembangan teknologi informasi yang sangat cepat telah mengubah cara pemerintah, dunia usaha, dan masyarakat dalam mengelola serta mendistribusikan data. Digitalisasi layanan publik membawa efisiensi tinggi, tetapi di sisi lain juga membuka celah bagi ancaman terhadap keamanan informasi dan privasi individu. Dalam konteks pembangunan infrastruktur digital nasional, isu keamanan siber dan perlindungan data pribadi menjadi sangat penting karena berhubungan langsung dengan stabilitas nasional, kedaulatan data, serta kepercayaan publik terhadap sistem digital pemerintah. Artikel ini bertujuan untuk menganalisis strategi perlindungan data dan pengendalian risiko keamanan informasi yang relevan bagi Indonesia di tengah meningkatnya serangan siber dan kebocoran data. Metode yang digunakan adalah pendekatan kualitatif deskriptif melalui telaah literatur terhadap kebijakan nasional, standar internasional seperti ISO/IEC 27001 dan NIST Framework, serta hasil penelitian terkait keamanan siber di sektor publik. Hasil analisis menunjukkan bahwa perlindungan data yang efektif harus berlandaskan pada sinergi antara kebijakan hukum, penerapan teknologi keamanan informasi, manajemen risiko siber, dan peningkatan literasi digital masyarakat. Selain itu, penguatan tata kelola data, pembentukan lembaga keamanan siber yang terintegrasi, dan kolaborasi lintas sektor menjadi faktor penentu dalam membangun ketahanan digital nasional. Penerapan strategi ini tidak hanya meningkatkan keamanan data, tetapi juga memperkuat kepercayaan masyarakat dan daya saing Indonesia dalam ekonomi digital global.
Kata kunci: *keamanan informasi, perlindungan data pribadi, manajemen risiko siber, infrastruktur digital nasional, tata kelola keamanan*

Abstract

The rapid advancement of information technology has fundamentally transformed how governments, businesses, and societies manage and distribute data. Digitalization of public services provides significant efficiency, yet it also introduces vulnerabilities related to information security and individual privacy. Within the context of national digital infrastructure development, cybersecurity and data protection have become critical issues that directly affect national stability, data sovereignty, and public trust in digital governance systems. This article aims to analyze data protection strategies and information security risk control mechanisms relevant to Indonesia amid the rising frequency of cyberattacks and data breaches. The research employs a qualitative descriptive approach through literature review, examining national policies, international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework, and previous studies on cybersecurity in public institutions. The findings reveal that effective data protection requires synergy among legal frameworks, implementation of advanced information security technologies, cyber risk management practices, and the enhancement of digital literacy within society. Furthermore, the establishment of integrated cybersecurity governance and cross-sector collaboration between the government, private entities, and the public is crucial for building sustainable national digital resilience. Implementing these strategies not only strengthens data security but also increases public trust and Indonesia's competitiveness in the global digital economy.
Keywords: *Information security, personal data protection, cyber risk management, national digital infrastructure, security governance*
Article Info
Received date: 25 November 2025 Revised date: 30 November 2025 Accepted date: 12 December 2025

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan mendasar terhadap cara manusia berinteraksi, bekerja, dan mengelola informasi. Di era digital saat ini, data

menjadi aset strategis yang memiliki nilai ekonomi tinggi dan menjadi fondasi bagi berbagai aktivitas sosial, ekonomi, maupun pemerintahan. Transformasi digital yang pesat di Indonesia mendorong pemerintah, lembaga publik, dan sektor swasta untuk memanfaatkan infrastruktur digital sebagai sarana peningkatan efisiensi dan pelayanan publik. Namun, di balik kemajuan tersebut, muncul pula tantangan serius berupa meningkatnya ancaman terhadap keamanan informasi dan perlindungan data pribadi yang jika tidak dikelola dengan baik dapat menimbulkan risiko besar terhadap stabilitas nasional.

Dalam beberapa tahun terakhir, Indonesia menghadapi berbagai kasus kebocoran data yang melibatkan lembaga publik maupun swasta. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN, 2023), terdapat peningkatan signifikan dalam jumlah serangan siber dan pelanggaran data pribadi. Kondisi ini menunjukkan bahwa sistem keamanan informasi nasional masih belum sepenuhnya tangguh dalam menghadapi ancaman digital yang semakin kompleks. Kebocoran data bukan hanya menimbulkan kerugian finansial, tetapi juga mengancam kepercayaan publik terhadap institusi digital, serta membuka celah bagi kejahatan siber lintas negara.

Sebagai respons terhadap kondisi tersebut, pemerintah telah menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai dasar hukum untuk memperkuat tata kelola keamanan data di Indonesia. Undang-undang ini menegaskan pentingnya tanggung jawab penyelenggara sistem elektronik dalam menjaga keamanan dan kerahasiaan data pengguna. Namun, efektivitas implementasinya masih menghadapi berbagai kendala, mulai dari lemahnya kesadaran organisasi terhadap pentingnya keamanan informasi hingga keterbatasan infrastruktur dan sumber daya manusia di bidang keamanan siber.

Selain aspek hukum, tantangan lain yang dihadapi adalah kurangnya integrasi antar lembaga dan minimnya koordinasi dalam pengelolaan risiko keamanan informasi. Banyak institusi yang belum memiliki sistem manajemen keamanan informasi (*Information Security Management System* / ISMS) yang sesuai dengan standar internasional seperti ISO/IEC 27001:2013. Akibatnya, mekanisme pengendalian risiko dan mitigasi ancaman siber belum berjalan optimal. Dalam konteks infrastruktur digital nasional, kelemahan ini berpotensi menghambat upaya pemerintah dalam mewujudkan transformasi digital yang aman, inklusif, dan berkelanjutan.

Dengan demikian, penelitian ini bertujuan untuk menganalisis strategi perlindungan data dan pengendalian risiko keamanan informasi dalam konteks infrastruktur digital nasional. Melalui pendekatan deskriptif kualitatif berbasis studi literatur, penelitian ini berupaya menggali upaya strategis yang dapat memperkuat sistem keamanan informasi Indonesia, baik dari aspek kebijakan, teknologi, maupun pengembangan sumber daya manusia. Hasil penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan kebijakan publik dan praktik tata kelola keamanan informasi yang lebih efektif, adaptif, serta sejalan dengan kebutuhan keamanan digital nasional di era transformasi global.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur (library research). Pendekatan ini dipilih karena topik keamanan informasi dan perlindungan data bersifat multidimensi, mencakup aspek kebijakan, teknologi, serta manajemen risiko, sehingga analisis kualitatif lebih tepat digunakan untuk memahami hubungan antar variabel tersebut secara kontekstual. Data penelitian diperoleh melalui penelusuran sumber-sumber sekunder yang relevan, seperti jurnal ilmiah, buku akademik, dokumen resmi pemerintah, serta standar internasional di bidang keamanan informasi, termasuk ISO/IEC 27001:2013 dan NIST Cybersecurity Framework (2018).

Prosedur penelitian dilakukan dalam beberapa tahap. Pertama, peneliti mengidentifikasi permasalahan utama terkait keamanan data nasional dan risiko siber yang sering terjadi di Indonesia. Kedua, dilakukan proses pengumpulan data dengan meninjau literatur dan kebijakan yang dikeluarkan oleh lembaga pemerintah seperti Badan Siber dan Sandi Negara (BSSN) dan Kementerian Komunikasi

dan Informatika (Kominfo). Ketiga, seluruh data dianalisis menggunakan teknik analisis isi (*content analysis*), yaitu dengan menafsirkan makna, pola, dan kesesuaian antar konsep perlindungan data, kebijakan hukum, serta penerapan tata kelola keamanan informasi.

Selain itu, peneliti juga melakukan analisis komparatif antara kebijakan perlindungan data di Indonesia dengan praktik terbaik (*best practices*) di tingkat internasional untuk mengidentifikasi kesenjangan dan peluang perbaikan. Validitas data dijaga dengan menggunakan teknik triangulasi sumber, yakni membandingkan berbagai referensi yang memiliki kredibilitas tinggi dari sumber akademik dan lembaga resmi. Hasil analisis kemudian disusun secara sistematis untuk menghasilkan rekomendasi strategis yang dapat memperkuat perlindungan data dan pengendalian risiko keamanan informasi pada infrastruktur digital nasional.

HASIL

Hasil penelitian ini menunjukkan bahwa upaya perlindungan data dan pengendalian risiko keamanan informasi di Indonesia masih menghadapi berbagai tantangan struktural dan teknis. Berdasarkan analisis terhadap kebijakan pemerintah, laporan Badan Siber dan Sandi Negara (BSSN), serta studi literatur terkait, ditemukan bahwa tingkat kesiapan keamanan siber nasional masih berada pada tahap penguatan dasar. Sebagian besar lembaga publik telah memiliki kebijakan internal terkait keamanan informasi, namun implementasinya belum sepenuhnya mengikuti standar internasional seperti ISO/IEC 27001:2013. Hanya sebagian kecil instansi yang telah menerapkan sistem manajemen keamanan informasi secara terukur dan berkelanjutan.

Selain itu, hasil kajian memperlihatkan bahwa kebocoran data yang terjadi dalam dua tahun terakhir disebabkan oleh lemahnya kontrol akses, penggunaan sistem digital yang belum terenkripsi dengan baik, serta rendahnya literasi keamanan digital di kalangan pengguna dan pengelola data. Berdasarkan data BSSN (2024), serangan siber terhadap lembaga publik meningkat lebih dari 40% dibandingkan tahun sebelumnya, dengan pola serangan yang semakin kompleks seperti *phishing*, *malware injection*, dan *ransomware*. Hal ini menunjukkan bahwa ancaman terhadap keamanan data nasional tidak hanya bersifat teknis, tetapi juga sistemik, yang melibatkan faktor manusia, kelembagaan, dan kebijakan publik.

Lebih lanjut, hasil studi juga menemukan bahwa tingkat koordinasi antar lembaga dalam pengelolaan keamanan siber masih belum optimal. Terdapat tumpang tindih kewenangan antara lembaga pemerintah yang berperan dalam keamanan informasi, seperti BSSN, Kementerian Komunikasi dan Informatika, serta lembaga sektor privat. Minimnya integrasi sistem dan pertukaran informasi antar lembaga menyebabkan penanganan insiden keamanan siber sering terlambat dan kurang efektif. Oleh karena itu, dibutuhkan strategi nasional yang lebih terpadu untuk memperkuat perlindungan data pribadi dan keamanan infrastruktur digital nasional.

PEMBAHASAN

Hasil penelitian ini mengindikasikan bahwa strategi perlindungan data di Indonesia memerlukan pendekatan yang lebih komprehensif, tidak hanya dari aspek regulasi tetapi juga dalam peningkatan kesadaran dan kapasitas kelembagaan. Temuan ini sejalan dengan penelitian oleh Putra dan Rahman (2022) yang menekankan pentingnya tata kelola keamanan informasi berbasis risiko dalam lembaga publik. Namun, penelitian ini menambahkan dimensi penting bahwa efektivitas strategi perlindungan data sangat bergantung pada sinergi antara kebijakan pemerintah, kesiapan teknologi, dan literasi digital masyarakat. Dalam konteks nasional, penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan langkah maju, namun implementasinya masih menghadapi kendala dalam hal pengawasan dan penegakan hukum.

Dari perspektif manajemen risiko, penelitian ini menunjukkan bahwa pengendalian risiko keamanan informasi perlu diarahkan pada penguatan *preventive control* dan *detective control*. Langkah-langkah seperti penerapan enkripsi data, autentikasi berlapis, serta audit keamanan berkala dapat menjadi dasar strategi mitigasi risiko yang lebih efektif. Selain itu, perlu adanya peningkatan kompetensi sumber daya manusia di bidang keamanan siber agar lembaga publik dan swasta memiliki kemampuan deteksi dini terhadap potensi serangan. Pendekatan ini sejalan dengan model *Defense in Depth* yang digunakan secara global untuk melindungi aset informasi dari berbagai lapisan ancaman.

Dalam konteks yang lebih luas, hasil penelitian ini memperkuat pandangan bahwa keberhasilan strategi perlindungan data bergantung pada kolaborasi multi-stakeholder antara pemerintah, sektor swasta, akademisi, dan masyarakat. Penguatan literasi keamanan digital di masyarakat juga menjadi faktor krusial dalam menciptakan budaya keamanan informasi yang berkelanjutan. Oleh karena itu, kebijakan nasional perlu diarahkan tidak hanya pada aspek teknologi dan regulasi, tetapi juga pada pembentukan ekosistem digital yang aman, tangguh, dan adaptif terhadap perkembangan ancaman global. Dengan demikian, strategi perlindungan data dan pengendalian risiko keamanan informasi dapat menjadi pondasi utama bagi keberlanjutan transformasi digital nasional.

SIMPULAN

Penelitian ini menegaskan bahwa strategi perlindungan data dan pengendalian risiko keamanan informasi memiliki peran sentral dalam menjaga ketahanan infrastruktur digital nasional. Hasil kajian menunjukkan bahwa meskipun Indonesia telah memiliki dasar hukum melalui UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, penerapan di lapangan masih menghadapi kendala berupa lemahnya kesadaran organisasi, keterbatasan sumber daya manusia, serta belum optimalnya koordinasi antar lembaga. Ancaman siber yang terus meningkat juga menunjukkan bahwa sistem keamanan informasi nasional memerlukan pendekatan yang lebih adaptif dan terintegrasi.

Dengan demikian, upaya penguatan keamanan informasi harus diarahkan pada tiga fokus utama: pertama, peningkatan efektivitas kebijakan dan tata kelola keamanan berbasis risiko; kedua, penguatan infrastruktur teknologi melalui penerapan sistem keamanan berlapis dan audit berkala; dan ketiga, pengembangan literasi serta kompetensi sumber daya manusia di bidang keamanan digital. Strategi yang sinergis antara pemerintah, sektor swasta, dan masyarakat akan menjadi kunci dalam membangun ekosistem digital yang aman, tangguh, dan berkelanjutan.

REFERENSI

Badan Siber dan Sandi Negara. (2023). *Laporan Tahunan Keamanan Siber Indonesia 2023*. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2024). *Statistik Insiden Keamanan Siber Nasional Tahun 2024*. Jakarta: BSSN.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information Security Management Systems — Requirements*. Geneva: ISO.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Strategi Nasional Keamanan Siber dan Perlindungan Data Pribadi*. Jakarta: Kominfo.

Nurdin, M. (2023). Penguatan tata kelola keamanan informasi di sektor publik Indonesia. *Jurnal Sistem Informasi dan Keamanan Digital*, 11(2), 155–167.

Putra, A. R., & Rahman, T. (2022). Tata kelola keamanan informasi berbasis risiko di lembaga pemerintah Indonesia. *Jurnal Teknologi Informasi dan Manajemen*, 9(1), 45–58.

Rahmawati, D., & Hidayat, F. (2021). Literasi keamanan digital dan tantangan perlindungan data pribadi di Indonesia. *Jurnal Komunikasi dan Informasi Digital*, 7(3), 210–222.

Simanjuntak, E., & Pratama, A. (2022). Implementasi kebijakan perlindungan data pribadi dalam sistem digital nasional. *Jurnal Kebijakan Publik dan Transformasi Digital*, 5(1), 1–13.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 242.

World Economic Forum. (2023). *Global Cybersecurity Outlook 2023*. Geneva: World Economic Forum.