E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 7 No 12 Tahun 2025

ANALISIS RISIKO DAN STRATEGI PERLINDUNGAN PRIVASI DATA DALAM PENGELOLAAN *BIG DATA*

Sri Anggraini[1], Muhammad Irwan Padli Nasution[2]
[1,2]Program Studi Manajemen, Fakultas Ekonomi dan Bisnis Islam,
Universitas Islam Negeri Sumatera Utara
[1]anggrainisri577@gmail.com, [2]irwannst@uinsu.ac.id

Abstrak

Di era digital, ditandai dengan perkembangan cepat teknologi informasi, tantangan baru telah muncul dalam melindungi perlindungan data, terutama ketika mengelola data besar. Volume data yang terus meningkat dengan aktivitas digital membuat informasi pribadi rentan terhadap berbagai bentuk pelanggaran, seperti kebocoran data dan penyalahgunaan informasi. Tujuan dari penelitian ini adalah untuk menganalisis berbagai risiko perlindungan data yang muncul dalam pengelolaan data besar dan untuk mengembangkan strategi perlindungan data yang efektif dan relevan untuk era digital. Metode yang digunakan adalah penelitian studi pustaka dengan pendekatan kualitatif dengan meninjau berbagai jurnal, peraturan hukum dan sumber-sumber informasi yang relevan terkait lainnya. Hasil penelitian ini menunjukkan bahwa risiko privasi dari mengendalikan sistem keamanan, kesadaran pengguna yang rendah, dan implementasi peraturan belum terbesar. Oleh karena itu, strategi teknis seperti enkripsi, kontrol akses, dan audit sistem berkala diperlukan. Ini didukung oleh peraturan seperti Undang-Undang Data Pribadi. Singkatnya, strategi perlindungan data untuk pengembangan teknologi harus dapat beradaptasi dan dapat mampu memberikan perlindungan individu dan organisasi pengelolaan *big data*.
Kata kunci: *Big data*, Perlindungan Data Pribadi, Strategi Perlindungan, Risiko Data, Kebocoran Data.

Abstract

In the digital age, characterized by the rapid development of information technology, new challenges have emerged in protecting data protection, especially when managing big data. The ever-increasing volume of data with digital activities makes personal information vulnerable to various forms of breaches, such as data leakage and information misuse. The purpose of this study is to analyze the various data protection risks that arise in managing big data and to develop an effective and relevant data protection strategy for the digital era. The method used is desk research with a qualitative approach by reviewing various journals, legal regulations and other relevant sources of information. The results of this study show that privacy risks from controlling security systems, low user awareness, and regulatory implementation have not been the greatest. Therefore, technical strategies such as encryption, access control, and periodic system

Article History:
Received: May 2025
Reviewed: May 2025
Published: May 2025

Plagirism Checker No 234
Prefix DOI :
10.8734/Kohesi.v1i2.365

audits are necessary. This is supported by regulations such as the Personal Data Act. In summary, data protection strategies for technological development must be adaptable and can be able to provide individual and organizational protection of big data management.
***Keywords**: Big data, Personal Data Protection, Protection Strategy, Data Risk, Data Leakage.*

PENDAHULUAN

Di era digital modern, Kemajuan dalam teknologi informasi di era digital saat ini telah menciptakan ledakan data dalam jumlah besar, yang dikenal sebagai *big data*. *Big data* merupakan sekumpulan data yang sangat besar dan kompleks yang tidak dapat ditangani dengan baik dengan sistem manajemen basis data konvensional atau aplikasi pemrosesan data biasa (Maryanto, 2017). Teknologi *big data* adalah sekumpulan sistem atau alat yang dimaksudkan untuk mengolah data yang sangat besar. Selain konsep 6V, ciri khas utama *big data* terdiri dari tiga elemen awal: *volume*, *velocity*, dan *variety*. Volume menunjukkan jumlah data yang sangat besar, *velocity* menunjukkan seberapa cepat data dibuat dan diakses, dan *variety* menunjukkan berbagai format data(Winarsih, 2020).

Big data umumnya dipahami sebagai kumpulan informasi dengan perbedaan besar, cepat, dan kompleks. Karena itu, untuk menghasilkan wawasan dan membantu proses pengambilan keputusan, pendekatan pengolahan data yang inventif diperlukan. Memahami sifat *big data* sangat bergantung pada enam atribut yang dikenal sebagai 6V: *Volume, Velocity, Variety, Value*, *Veracity*, dan *Variability* (Munawar et al., 2020). Fenomena ini berdampak besar pada banyak sektor, termasuk bisnis, pendidikan, dan pelayanan publik. Meskipun pengelolaan *big data* memiliki banyak manfaat, itu juga memiliki banyak tantangan, terutama dalam hal menjaga privasi dan keamanan data pribadi.

Agar pengelolaan *big data* berjalan dengan baik, diperlukan penerapan teknologi khusus dan strategi analitik yang tepat. Hal ini dibutuhkan agar data dapat membantu pengambilan keputusan yang efektif dan meningkatkan efisiensi operasional perusahaan (Maryanto, 2017). Seiring dengan penggunaan *big data*, perlindungan data pribadi menjadi semakin penting. Tanpa persetujuan yang jelas dari individu tersebut, data sering dikumpulkan, diproses, dan dievaluasi. Seperti dari penelitian terdahulu menurut (Hasibuan & Nasution, 2023) menyebutkan bahwa dalam praktiknya *big data* sering mengaburkan perbedaan antara data publik dan privat. Ini pada akhirnya dapat mengancam hak konsumen dalam konteks ekonomi digital.

Contoh kebocoran data berskala besar, seperti peretasan Bjorka, menunjukkan kelemahan sistem perlindungan data Indonesia dan dapat mengurangi kepercayaan masyarakat terhadap institusi publik di lembaga yang relevan (Akbar et al., 2024). Di samping itu, survei yang dilakukan (Aliefa et al., 2025) menemukan bahwa orang masih kurang relatif rendah menyadari pentingnya melindungi data pribadi. Sementara itu, peraturan saat ini belum cukup untuk mencegah kebocoran dan penyalahgunaan data. Karena kemungkinan penyalahgunaan hak informasi pribadi semakin meningkat, kesadaran masyarakat harus ditingkatkan (Disemadi et al., 2023). Kasus kebocoran data yang menyeret PDNS 2 Surabaya menjadi contoh nyata bahwa masalah tersebut bukan hanya masalah teknis; itu juga menunjukkan bahwa budaya keamanan siber di kantor pemerintah kurang efektif (Adristi & Ramadhani, 2024). Salah satu kasus yang menunjukkan pentingnya masalah ini adalah kebocoran data Bank Indonesia, yang menunjukkan bahwa industri keuangan juga bisa menjadi sasaran (Naufal & Azmi, 2024).

Risiko ini meningkat seiring dengan karakteristik *big data* seperti volume yang besar, kecepatan tinggi, keragaman format, nilai informasi, dan keakuratan data, yang membuat perlindungan data sensitif menjadi lebih kompleks. Salah satu masalah utama adalah kemungkinan akses ilegal, manipulasi, atau bahkan kebocoran data. Selain itu, kurangnya pemahaman pengguna tentang pentingnya privasi akan memperburuk situasi, terutama jika tidak melakukan evaluasi rutin dari algoritma yang digunakan, dan para pengguna tidak mengabaikan proses validasi dan memfilter data. Untuk meminimalkan risiko ini, strategi seperti generalisasi data, enkripsi, anonimisasi, kesadaran yang lebih tinggi, dan membentuk keamanan siber untuk pengguna data.

Berdasarkan pendahuluan di atas, tujuan dari penelitian ini adalah untuk mengevaluasi berbagai bahaya yang terkait dengan privasi data yang muncul selama proses pengelolaan *big data*, serta untuk mengembangkan strategi perlindungan yang dapat digunakan dengan benar. Penelitian ini diharapkan dapat membantu memperluas pemahaman dan memperkuat upaya untuk melindungi data pribadi saat teknologi digital berkembang dengan menggunakan metodologi studi kepustakaan dan analisis kualitatif literatur yang relevan.

METODE PENELITIAN

Dalam artikel ini, metode penelitian yang digunakan adalah penelitian literatur dan menggunakan pendekatan kualitatif. Penelitian ini meninjau jurnal ilmiah, peraturan hukum yang berlaku, dan sumber lain untuk mendapatkan informasi yang relevan tentang risiko dan strategi perlindungan privasi data dalam pengelolaan *Big data*. Data yang digunakan dalam penelitian ini dari berbagai sumber seperti jurnal akademik, artikel, laporan penelitian. Penulis juga mengumpulkan studi kasus dari temuan penelitian terdahulu yang dapat diakses di *Google Scholar*, *Researchgate*, dan *Website* jurnal lainnya. Metode ini dipilih untuk mendapatkan pemahaman menyeluruh tentang masalah dan solusi yang terkait dengan perlindungan privasi data di era *Big data*.

HASIL DAN PEMBAHASAN

Big data mengacu pada pengumpulan data yang sangat besar yang tersedia dalam berbagai format dan diproduksi dengan kecepatan tinggi (Winarsih, 2020). Meskipun pengelolaan *big data* menawarkan banyak keuntungan di era digital saat ini, juga menawarkan sejumlah tantangan, khususnya dalam hal perlindungan data pribadi. Berdasarkan temuan dari beberapa referensi dan penelitian terdahulu, beberapa risiko yang paling sering muncul termasuk kebocoran data, penyalahgunaan dan kegagalan sistem keamanan yang digunakan untuk melindungi data.

Dalam sebuah studi kasus berjudul "Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan", insiden kebocoran data di Bank Indonesia menjadi contoh nyata dari tingginya risiko yang menyertai pengelolaan *big data*. Akibat kelemahan sistem keamanan, berbagai jenis kejahatan siber seperti *ransomware*, *phishing*, pencurian identitas, dan *cyber espionage* terus berkembang pesat. Tidak adanya perlindungan yang memadai, seperti enkripsi data secara *real time*, otentikasi ganda, dan sistem pemantauan ancaman yang responsif, membuat situasi menjadi lebih buruk.

Salah satu faktor utama di balik kebocoran data adalah dukungan yang lemah dari halaman hukum dan teknologi oleh manajer data dan publik sebagai pengguna basis data. Ini lebih buruk karena banyak orang tidak tahu tentang pentingnya menjaga data pribadi dan banyak yang tidak tahu tentang undang-undang seperti Undang-Undang Perlindungan Data Pribadi (UU PDP). Sebaliknya, kurangnya inovasi untuk mengatasi modus kejahatan siber yang terus berkembang merupakan hambatan besar untuk membangun ekosistem digital yang aman. Oleh karena itu, strategi perlindungan data yang komprehensif dan terorganisir harus digunakan

untuk mengimbangi ketergantungan besar masyarakat dan organisasi pada sistem digital (Naufal & Azmi, 2024).

Perbankan menggunakan berbagai strategi untuk menjaga data pelanggan aman dan rahasia. Salah satunya adalah teknologi enkripsi, yang mengamankan data dalam bentuk kode yang tidak dapat dibaca *(ciphertext*), yang hanya dapat diakses oleh pihak yang memiliki otorisasi. Karena terkait langsung dengan tiga komponen utama keamanan data: kerahasiaan, integritas, dan otentikasi, teknologi ini menjadi sangat penting bagi industri perbankan. Untuk memastikan bahwa informasi sensitif seperti data keuangan dan identitas pribadi nasabah hanya dapat diakses oleh individu tertentu. Sementara itu, integritas memastikan bahwa data tetap utuh dan belum diubah selama proses penyimpanan atau transmisi, sehingga informasi yang diterima tetap akurat dan dapat dipercaya.

Di sisi lain, fungsi otentikasi dapat memverifikasi identitas pihak yang terlibat dalam pertukaran data dan mencegah penyalahgunaan identitas dan akses ilegal. Selain menjaga keamanan internal, enkripsi membantu bisnis perbankan memenuhi peraturan seperti GDPR dan PCI DSS, yang mengharuskan perlindungan data pelanggan yang optimal. Bank yang mematuhi peraturan ini tidak hanya menghindari sanksi hukum dan kerugian finansial, tetapi juga meningkatkan kepercayaan masyarakat terhadap sistem perbankan. Oleh karena itu, di tengah meningkatnya ancaman siber yang semakin kompleks dari waktu ke waktu, enkripsi menjadi bagian penting dari sistem pertahanan digital bank. Dengan menggunakan kriptografi, teknologi *blockchain* digunakan untuk mencatat setiap jenis transaksi secara aman dalam blok-blok yang saling terhubung dan sulit untuk diubah.

Sebuah blok akan dibuat setelah setiap transaksi telah divalidasi, dan kemudian dihubungkan ke blok sebelumnya melalui *hash*, sejenis sidik jari digital yang mewakili isi blok. Karena jaringan penambang memverifikasi setiap transaksi dan banyak komputer secara terdesentralisasi memprosesnya, metode ini menjadikan *blockchain* sebagai sistem pencatatan yang sangat andal. Data yang disimpan dalam *blockchain* telah sepenuhnya terenkripsi, sehingga hanya dapat ditambahkan tanpa mengubahnya. Hal ini meminimalkan kemungkinan penipuan atau manipulasi dalam riwayat transaksi dan Ini dapat mempertahankan integritas sejarah transaksi. Selain itu, *blockchain* memberikan sistem audit yang transparan yang memungkinkan siapa pun untuk melacak riwayat transaksi, termasuk dalam pelacakan aset digital.

Kelebihan-kelebihan tersebut menunjukkan bahwa *blockchain* memiliki potensi besar untuk mengubah model bisnis, terutama di sektor jasa keuangan. Teknologi ini tidak hanya meningkatkan efisiensi operasional, tetapi juga menyederhanakan proses seperti mengidentifikasi pelanggan, mempercepat proses evakuasi, dan kesimpulan tentang transaksi keuangan. Pihak perbankan dapat mengambil berbagai tindakan tambahan selain menerapkan enkripsi dan teknologi *blockchain* untuk mengurangi kemungkinan kebocoran data dan memastikan bahwa data nasabah tetap aman. Salah satunya adalah rutin melakukan audit keamanan. Tujuannya adalah untuk menilai seberapa baik kebijakan yang digunakan untuk melindungi data, serta memastikan bahwa prosedur dan sistem yang ada memenuhi persyaratan keamanan yang ditetapkan.

Bank disarankan harus memberikan pelatihan kepada seluruh staf tentang pentingnya menjaga data dan privasi. Dengan pemahaman yang baik, karyawan diharapkan dapat memenuhi tugas menjaga kerahasiaan data pelanggan. Di sisi lain, juga merupakan aspek penting dari pelanggan untuk mendapatkan penjelasan yang jelas tentang bagaimana data dikumpulkan, digunakan, disimpan, dan dilindungi, termasuk haknya untuk melindungi data pribadi. Bank harus menjadi prioritas utama untuk mematuhi peraturan yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), yang mewajibkan lembaga keuangan untuk menjaga kerahasiaan dan keamanan data nasabah.

Selain itu, bank juga harus memiliki rencana tanggap darurat untuk kasus kebocoran data. Ini termasuk mengirimkan pemberitahuan kepada pelanggan yang terkena dampak dan mengambil tindakan untuk mencegah kejadian serupa terjadi lagi. Selain itu, data pelanggan harus disimpan dengan aman dan terbatas pada waktu yang diperlukan. Bank harus menghapus data secara aman dan menyeluruh setelah tidak digunakan untuk mencegah penyalahgunaan (Jacqueline et al., 2025).

Selama pengembangan teknologi yang semakin jaringan, perlindungan privasi data kini menjadi masalah global yang sangat penting di tengah perkembangan teknologi yang semakin terhubung. Setiap negara memiliki kebijakan dan rencana untuk melindungi data pribadi warganya. Ini karena ancaman kebocoran data, penyalahgunaan data, dan serangan siber semakin meningkat. Dalam kebanyakan kasus, pendekatan untuk melindungi data pribadi mencakup berbagai komponen, seperti peraturan, pembentukan lembaga pengawas, dan penerapan metode teknis dan instruksional yang disesuaikan dengan kemajuan teknologi dan masyarakat. Untuk mengatasi masalah ini, negara seperti Singapura, Amerika Serikat, dan Malaysia telah membuat rencana khusus. Di bawah ini adalah ringkasan metode yang digunakan oleh ketiga negara untuk melindungi privasi data, yang dapat digunakan sebagai referensi dalam membuat kebijakan perlindungan data di tingkat nasional dan internasional:

1. Undang-undang Perlindungan Data Pribadi (PDPA) 2012 di Singapura mengatur pendekatan utama untuk perlindungan data pribadi. Undang-undang ini mencakup aturan tentang pengumpulan, penggunaan, pembukaan, akses, koreksi, dan penyimpanan data pribadi. *Personal Data Protection Commission* (PDPC) bertanggung jawab atas pengawasan dan penegakan peraturan ini. Selain itu, Singapura menekankan transparansi dengan mempublikasikan kasus pelanggaran di situs PDPC. Tindakan ini bertujuan untuk memberi tahu orang dan lembaga tentang pentingnya pengelolaan data yang baik, serta memberikan efek jera melalui penerapan denda dan sanksi administratif.
2. Amerika Serikat belum memiliki atap federal hukum yang secara khusus mengatur perlindungan data pribadi. Penanganan perlindungan data lebih lanjut dikendalikan oleh *Federal Trade Commission* (FTC), tetapi tidak ada pengaturan khusus untuk perlindungan data pribadi Anda. Menurut skandal *Cambridge Analytica*, kurangnya hukum federal ini telah menjadi sorotan dan telah memicu tekanan publik untuk membentuk undang -undang yang melindungi data pribadi negara.
3. Malaysia akan mengambil alih undang-undang *Personal Data Protection Act* 2010 (PDPA), dengan fokus pada pemrosesan data pribadi yang terkait dengan transaksi komersial. Undang-undang tersebut mengatur hak pihak yang terlibat, prinsip -prinsip pengumpulan dan pemrosesan data, dan pembentukan *Department of Personal Data Protection* (JPDP) sebagai otoritas pengawas. Malaysia juga memiliki keamanan siber di Malaysia, sebuah agen teknis dari Kementerian Sains dan Teknologi dan Inovasi yang memperkuat aspek teknis melindungi data pribadi (Daniswara & Rahman, 2018).

KESIMPULAN

Di era digital saat ini, mengelola *big data* menjadi tantangan tersendiri karena melibatkan privasi dan keamanan data pribadi selain volume dan kecepatan data. Analisis penelitian terdahulu ini menunjukkan bahwa masih ada kemungkinan kebocoran dan penyalahgunaan data, terutama karena sistem keamanan yang tidak kuat, kesadaran pengguna yang rendah, dan kurangnya penerapan UU Perlindungan Data Pribadi (UU PDP). Penggunaan teknologi *blockchain*, autentikasi ganda, enkripsi data, dan audit berkala harus menjadi bagian dari pendekatan teknis yang efektif sebagai strategi melindungi data. Penelitian ini membahas secara menyeluruh berbagai risiko bahaya yang muncul saat mengelola *big data* dan berbagai cara yang dapat digunakan untuk melindungi privasi data. Di sisi lain, pendekatan edukasi kepada masyarakat juga penting agar lebih sadar akan pentingnya memelihara data pribadi.

Untuk membuat ekosistem digital yang aman, regulasi yang jelas dan peraturan pengawasan yang ketat dilakukan oleh lembaga terkait harus diperkuat. Studi ini juga menunjukkan bahwa perlindungan privasi data bukan hanya tugas pemerintah atau lembaga, tetapi juga kesadaran pengguna, penyedia layanan, dan organisasi secara keseluruhan. Singapura dan Malaysia adalah negara lain yang sudah menggunakan perlindungan data. Dalam pengelolaan *big data*, perlindungan data melibatkan kesadaran publik, tanggung jawab hukum, dan etika digital. Oleh karena itu, kerja sama antara teknologi, hukum, dan edukasi adalah kunci yang sangat penting untuk mengatasi tantangan perlindungan privasi di era *big data*.

DAFTAR PUSTAKA

Adristi, F. I., & Ramadhani, E. (2024). "Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya". *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, *2*(6), 196–212.

Akbar, M., Syahril, F., Hasan, H., & Hasan, N. (2024). "Dampak Kebocoran Data Bjorka pada Kepatuhan Wajib Pajak: Perspektif Akuntansi Keperilakuan". September, 109–115.

Aliefa, F., Khairul, S., Mulyadi, D., & Nurhasbiyah, I. (2025). "Konstruksi Sosial: Jurnal Penelitian Ilmu Sosial Survey Mengenai Kebocoran Data di Era Digital". *5*(1), 7–16.

Daniswara, F., & Rahman, F. (2018). "Perlindungan Data Pribadi: Studi Komparasi terhadap Praktik di Singapura, Amerika Serikat, dan Malaysia". *Center For Digital Society*, *31*, 24.

Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, M. (2023). "Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?" *Sang Sewagati Journal*, *1*(2), 67–90.

Hasibuan, M., & Nasution, M. I. P. (2023). "Perlindungan Privasi Konsumen Dalam Penggunaan Big data Di Ekonomi Digital". *JUEB: Jurnal Ekonomi Dan Bisnis*, *2*(2), 83–87. https://doi.org/10.57218/jueb.v2i2.692

Jacqueline, A., Gunardi, S., Moody, L., & Syailendra, R. (2025). "Perlindungan Kepada Nasabah Bank Terhadap Kebocoran Data (Studi Kasus Kebocoran Data pada Bank Indonesia)". *2*(1), 107–114.

Maryanto, B. (2017). "Big data dan Pemanfaatannya Dalam Berbagai Sektor". *Media Informatika*, *16*(2), 14–19.

Munawar, Z., Kom, M., & Putri, N. I. (2020). "Keamanan Jaringan Komputer Pada Era Big data". *Jurnal Sistem Informasi-J-SIKA*, *02*(01), 14–20.

Naufal, M., & Azmi, A. (2024). "Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan". *1*(6), 448–458.

Winarsih, I. (2020). "Proteksi Privasi *Big data* Dalam Media Sosial". *Jurnal Audience*, *3*(1), 1–33. https://doi.org/10.33633/ja.v3i1.3722