*Jurnal Manajemen Pendidikan* *Volume 14, No. 01, 2026, halaman 227 – 233*
*https://journal.unpak.ac.id/index.php/jmp* *e-SSN: 2614-3313 ; p-ISSN: 2302-0296*
*Penerbit: Sekolah Pascasarjana, Universitas Pakuan*

# KEBOCORAN DATA PUBLIK DAN ETIKA TI DALAM TATA KELOLA SERTA RESILIENSI SIBER BPJS-PDN 2024

Audita Najwa Khalidah [a*)], Ragil [a)], Raka Prabu Wikrama Yudianto[a)],
Dylan Saputra [a)], Mugi Sugiharto Tramajie [a)], Yunita [a)]

[a)] *Universitas Bina Sarana Informatika, Jakarta, Indonesia*

[*)]*e-mail korespondensi: 19220376@bsi.ac.id*

*Article history: received 01 December 2025; revised 12 December 2025; accepted 31 Januari 2026* *DOI : https://doi.org/10.33751/jmp.v14i1.13504*

**Abstrak.** Transformasi digital pelayanan publik di Indonesia menghadapi tantangan serius terkait keamanan data dan etika profesional TI. Penelitian ini membandingkan tata kelola dan resiliensi siber pada dua insiden kebocoran data publik: BPJS Kesehatan (2021) dan Pusat Data Nasional/PDN (2024), serta meninjau penerapan etika profesional TI. Dengan pendekatan kualitatif komparatif melalui studi pustaka terhadap laporan resmi dan literatur ilmiah lima tahun terakhir, ditemukan bahwa kedua insiden memiliki kelemahan serupa, seperti keterbatasan sistem backup, lemahnya pengawasan vendor, dan rendahnya kesadaran etika. BPJS Kesehatan dinilai lebih baik dalam tata kelola dan koordinasi dengan BSSN, sedangkan PDN menunjukkan mitigasi dan akuntabilitas publik yang lemah. Penelitian menyimpulkan bahwa penguatan etika profesional TI, perbaikan tata kelola keamanan, dan pembentukan lembaga pengawas independen yang memastikan implementasi konsisten UU Perlindungan Data Pribadi merupakan langkah penting untuk meningkatkan resiliensi siber nasional.

**Kata Kunci:** BPJS Kesehatan, Etika Profesional TI, Kebocoran Data, Pusat Data Nasional.

***Public Data Leakage and IT Ethics in Cyber Governance and Resilience BPJS-PDN 2024***

***Abstract***. *Digital transformation in Indonesia's public service sector faces significant challenges related to data security and IT professional ethics. This study compares cybersecurity governance and cyber resilience in two major public data breach incidents: BPJS Kesehatan (2021) and the National Data Center/PDN (2024), while examining the application of IT professional ethics. Using a qualitative comparative approach through literature review of official reports and scientific publications from the last five years, the findings show shared weaknesses in both incidents, including limited backup systems, weak vendor oversight, and low ethical awareness. BPJS Kesehatan demonstrates stronger governance and better coordination with the National Cyber and Crypto Agency (BSSN), whereas PDN shows weak mitigation efforts and limited public accountability. The study concludes that strengthening IT professional ethics, improving cybersecurity governance, and establishing an independent oversight body to ensure consistent implementation of the Personal Data Protection Law are essential for enhancing national cyber resilience.*

***Keywords:*** *cybersecurity governance, data breach, IT professional ethics, BPJS Kesehatan, National Data Center*

## I. PENDAHULUAN

Transformasi digital yang berlangsung pesat di Indonesia telah meningkatkan efisiensi pelayanan publik, namun juga membawa risiko signifikan terkait keamanan data dan kerentanan sistem informasi. Berbagai lembaga pemerintah kini mengandalkan sistem digital untuk mengelola data masyarakat, sehingga insiden kebocoran data memiliki dampak yang semakin luas (Magnusson et al., 2025). Kondisi ini menuntut penerapan tata kelola keamanan informasi dan etika profesional teknologi informasi (TI) secara konsisten. Namun, perluasan infrastruktur digital tersebut juga meningkatkan risiko serangan siber, kebocoran data, dan pelanggaran etika profesional, terutama karena lemahnya tata kelola keamanan informasi di banyak instansi pemerintah (Aryanti, 2025). Secara global, tata kelola keamanan informasi di sektor publik memerlukan integrasi strategi, kebijakan, dan mekanisme pengawasan untuk mengendalikan risiko siber secara menyeluruh dan berkelanjutan (Magnusson et al., 2025).

Dalam beberapa tahun terakhir, Indonesia menghadapi dua insiden besar kebocoran data yang menimbulkan keprihatinan publik, yaitu kebocoran data BPJS Kesehatan pada tahun 2021 serta serangan *ransomware* pada Pusat Data Nasional (PDN) tahun

2024. Kedua peristiwa tersebut menunjukkan bahwa perlindungan data publik masih belum optimal, baik dari sisi kesiapan infrastruktur maupun kepatuhan terhadap standar keamanan (Suci Anugrah et al., 2025). Selain itu, persoalan etika profesional TI juga terlihat melalui kelalaian dalam menjaga kerahasiaan data, penyalahgunaan akses, serta kurangnya akuntabilitas dalam pelaporan insiden (Suci Anugrah et al., 2025). Kebocoran data BPJS Kesehatan memperlihatkan celah dalam pengelolaan basis data peserta, sementara insiden PDN 2024 mengungkap lemahnya mekanisme pencadangan, ketergantungan pada satu pusat data, serta belum matangnya *respons* insiden pemerintah (Asiyanti & Agussalim Agussalim, 2024; Kayode-Bolarinwa, 2025).

Ketidaksiapan lembaga pemerintah dalam menghadapi ancaman siber sejalan dengan berbagai studi yang menegaskan rendahnya implementasi standar keamanan seperti ISO/IEC 27001, *privacy-by-design*, autentikasi berlapis, dan audit keamanan berkala (Sinaga & Taan, 2024). Penelitian sebelumnya juga menunjukkan bahwa pelanggaran etika dan lemahnya tata kelola saling berkaitan: ketika etika personal dan profesional tidak ditegakkan, maka standar keamanan teknis cenderung tidak diikuti (Fransciko Pritama et al., 2024).

Selain aspek etika, sejumlah penelitian menyoroti pentingnya tata kelola yang lebih adaptif. Kerangka seperti *SCRUM-based risk management* dapat meningkatkan keandalan dan kesigapan lembaga publik dalam menghadapi insiden siber (Prio Pamungkas et al., 2024). Di sisi lain, perkembangan *cloud governance* berbasis CIA (*Confidentiality, Integrity, Availability*) memberikan pendekatan baru yang menekankan integrasi *risk assessment* dengan kebijakan keamanan informasi (Rahmika et al., 2025).

Dari sisi regulasi, berbagai studi menekankan bahwa ketidakjelasan standar dan lemahnya penerapan kebijakan turut meningkatkan kerentanan data publik. Regulasi yang ada belum sepenuhnya diimplementasikan, terutama terkait audit keamanan, penunjukan pejabat pelindungan data, dan penerapan prinsip-prinsip keamanan informasi (Siti Maesaroh, 2025).

Meskipun penelitian terdahulu membahas aspek keamanan, etika, dan tata kelola secara terpisah, masih terdapat kesenjangan dalam kajian yang mengintegrasikan ketiga aspek tersebut secara komprehensif untuk menganalisis kebocoran data publik di Indonesia. Berbeda dengan penelitian sebelumnya yang mengkaji aspek keamanan, etika, atau tata kelola secara terpisah, penelitian ini mengintegrasikan ketiga aspek tersebut untuk memberikan pemahaman yang lebih komprehensif mengenai faktor penyebab kelemahan keamanan data pada kasus BPJS Kesehatan dan PDN 2024.

Berdasarkan latar belakang tersebut, penelitian ini berupaya mengkaji bagaimana penerapan etika profesional TI tercermin dalam kasus kebocoran data BPJS Kesehatan dan insiden pada Pusat Data Nasional (PDN) tahun 2024, bagaimana tata kelola keamanan data diterapkan dalam kedua lembaga tersebut, serta bagaimana tingkat resiliensi siber mereka terlihat melalui proses penanganan dan pemulihan insiden.

Tujuan penelitian ini adalah menganalisis secara komparatif penerapan etika profesional TI, tata kelola keamanan data, dan tingkat resiliensi siber pada kasus kebocoran data BPJS Kesehatan dan PDN 2024, serta memberikan rekomendasi yang dapat digunakan untuk meningkatkan perlindungan data publik dan keamanan siber nasional.

***Etika Profesional Teknologi Informasi***

Etika profesional TI mencakup integritas, akuntabilitas, dan tanggung jawab dalam pengelolaan data digital. Pelanggaran etika seperti penyalahgunaan akses, tidak menjaga kerahasiaan data, dan minimnya transparansi merupakan faktor yang memperbesar risiko kebocoran data (Suci Anugrah et al., 2025). Penelitian (Fransciko Pritama et al., 2024) menunjukkan bahwa kegagalan etika profesional sering kali menjadi akar masalah insiden keamanan, terutama ketika pegawai TI tidak mengikuti prosedur pengamanan standar.

***Tata Kelola Keamanan Informasi***

Tata kelola keamanan informasi merupakan elemen penting dalam memastikan konsistensi kebijakan, kontrol risiko, serta perlindungan data di sektor publik. (Sinaga & Taan, 2024) menekankan bahwa sebagian besar instansi pemerintah masih belum memenuhi standar seperti ISO/IEC 27001:2022, khususnya terkait pengendalian akses, audit teknis, dan dokumentasi keamanan. Pada skala global, tata kelola keamanan informasi sektor publik membutuhkan integrasi antara kebijakan, proses, dan metrik formal untuk memastikan efektivitas perlindungan data (Magnusson et al., 2025).

Beberapa lembaga daerah di Indonesia mulai mengembangkan mekanisme tata kelola mandiri, termasuk pemetaan proses, manajemen risiko internal, dan penyusunan kebijakan keamanan data yang lebih sistematis (Ridzqi Fauzi et al., 2025). Selain itu, implementasi pendekatan *SCRUM-based governance* sebagaimana disarankan (Prio Pamungkas et al., 2024) terbukti meningkatkan fleksibilitas dan kepatuhan dalam pemutakhiran kontrol keamanan.

***Keamanan Data dan Infrastruktur Digital***

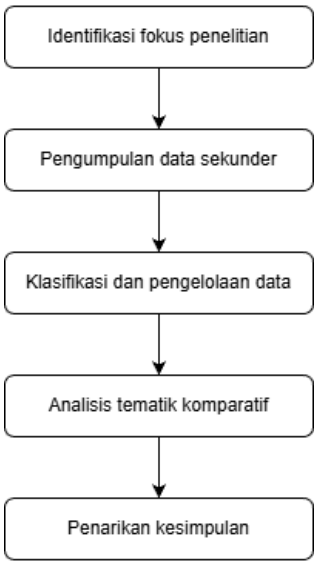
Pertumbuhan penggunaan layanan digital mendorong kebutuhan keamanan data yang lebih baik, terutama pada sistem telematika dan layanan publik yang menyimpan banyak data sensitif. Dalam konteks ini, analisis (Syailendra Putra et al., 2024) menunjukkan bahwa aspek legal dan teknis harus berjalan beriringan untuk melindungi privasi dan mengurangi risiko eksposur data. Sementara itu, kerangka *cloud governance* berbasis CIA memberikan pemahaman lebih komprehensif dalam menilai risiko serta meminimalkan potensi serangan (Rahmika et al., 2025).

***Kebijakan dan Diplomasi Siber Nasional***

Pada tingkat nasional, tata kelola keamanan siber membutuhkan koordinasi antar lembaga dan penguatan regulasi. (Chotimah, 2019) menjelaskan bahwa diplomasi siber Indonesia masih menghadapi tantangan koordinasi kelembagaan dan lemahnya kapabilitas operasional, yang berdampak pada mitigasi insiden siber di sektor publik. Hal ini menunjukkan bahwa tata kelola keamanan tidak hanya dimaknai secara teknis, tetapi juga memerlukan kerangka kelembagaan yang kuat dan responsif terhadap ancaman siber.

## II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif komparatif dengan metode studi pustaka (*library research*). Pendekatan ini dipilih karena penelitian berfokus pada analisis perbandingan antara dua kasus kebocoran data publik dengan berfokus pada penerapan etika profesional teknologi informasi (TI), tata kelola keamanan data, dan resiliensi siber pada lembaga pemerintah.



Gambar 1. Tahap Penelitian

***Jenis dan Pendekatan Penelitian***

Jenis penelitian ini adalah deskriptif-komparatif dengan pendekatan kualitatif. Menurut (Fadli, 2021; Isik, 2025) penelitian kualitatif digunakan untuk memahami makna dan konteks suatu fenomena melalui analisis mendalam data dari setting alami, wawancara, observasi, dan dokumen relevan, dengan menekankan pengalaman dan persepsi partisipan. Dalam konteks ini, penelitian membandingkan dua kasus kebocoran data publik BPJS Kesehatan (2021) dan Pusat Data Nasional (PDN, 2024) untuk mengidentifikasi perbedaan dan persamaan dalam tata kelola data, etika profesional TI, dan resiliensi siber.

***Objek dan Sumber Data***

Objek penelitian mencakup dua lembaga publik yang mengalami insiden kebocoran data berskala nasional di Indonesia. Kasus pertama adalah kebocoran data BPJS Kesehatan tahun 2021 dengan estimasi 279 juta data penduduk yang terungkap dan diperjualbelikan. Kasus kedua adalah serangan *ransomware LockBit 3.0* terhadap Pusat Data Nasional (PDN) tahun 2024 yang menyebabkan gangguan layanan digital ratusan instansi pemerintah. Data yang digunakan merupakan data sekunder, diperoleh dari dokumen resmi Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), BPJS Kesehatan, dan regulasi relevan seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain itu, penelitian ini memanfaatkan artikel ilmiah terindeks nasional dan internasional periode 2021–2025, laporan penelitian, media daring kredibel (Kompas, Katadata, CNN Indonesia), serta standar internasional seperti ACM Code of Ethics (2018) dan ISO/IEC 38505-1 (2017) terkait tata kelola data.

***Teknik Pengumpulan Data***

Data dikumpulkan melalui analisis dokumen dan kajian literatur, mencakup kronologi insiden, kebijakan pengelolaan data, mekanisme respons dan pemulihan, serta aspek etika dan tata kelola lembaga publik. Data kemudian dikategorikan ke dalam tiga tema: etika profesional TI, tata kelola keamanan data, dan resiliensi siber.

***Teknik Analisis Data***

Analisis dilakukan secara tematik komparatif, meliputi reduksi data, klasifikasi ke dalam tema utama, perbandingan antar kasus BPJS dan PDN, serta penarikan kesimpulan yang mengaitkan etika TI, tata kelola, dan resiliensi siber. Pendekatan ini memungkinkan pemahaman holistik terhadap dinamika kebocoran data dan praktik tata kelola di lembaga publik.

## III. HASIL PENELITIAN

***Gambaran Umum Kasus Kebocoran Data Publik***

Peningkatan serangan siber terhadap lembaga pemerintah memperlihatkan bahwa keamanan data publik di Indonesia berada pada kondisi yang semakin kritis. Laporan Tahunan BSSN (2024) mencatat peningkatan serangan hingga 31% dibanding tahun

sebelumnya, dan 38% di antaranya menargetkan sektor pemerintahan. Persentase tersebut menunjukkan bahwa sistem digital pemerintah masih memiliki kelemahan signifikan dalam melindungi data dan infrastruktur strategis.

Dua kasus terbesar dalam empat tahun terakhir kebocoran data BPJS Kesehatan (2021) dan serangan *ransomware* terhadap Pusat Data Nasional (PDN, 2024) merupakan bukti paling jelas dari lemahnya perlindungan data negara. Kebocoran data BPJS melibatkan lebih dari 279 juta data penduduk mencakup NIK, alamat, dan informasi kesehatan, yang kemudian diperjualbelikan di forum daring. Sebaliknya, insiden PDN 2024 tidak hanya mengakibatkan kebocoran data, tetapi juga menyebabkan lumpuhnya layanan digital ratusan instansi pemerintah karena serangan *ransomware LockBit 3.0*. Dampaknya sangat sistemik mengingat PDN merupakan pusat pertukaran data nasional yang menopang berbagai layanan digital pemerintah.

Dampak kedua insiden ini juga terlihat pada aspek non-teknis, terutama penurunan kepercayaan publik. Hasil survei Katadata Insight Center (2024) dan Kompas R&D (2023) menunjukkan tren penurunan konsisten setelah kedua peristiwa.

Tabel 1. Tingkat Kepercayaan Publik pada Keamanan Data Pemerintah (2021–2024)

| Tahun | Tingkat Kepercayaan (%) |
|---|---|
| 2021 | 58 |
| 2022 | 47 |
| 2023 | 42 |
| 2024 | 36 |

***Sumber:*** *(Maharani, 2021; Setyowati, 2024)*

Rendahnya kepercayaan ini mengindikasikan bahwa masyarakat menilai pemerintah belum mampu memenuhi prinsip transparansi dan akuntabilitas, khususnya dalam pelaksanaan etika profesional TI. Dengan demikian, gambaran umum ini menjadi dasar untuk menganalisis secara lebih mendalam penerapan tata kelola, etika profesional, dan resiliensi siber pada masing-masing lembaga.

***Analisis Tata Kelola Keamanan Data Publik***

Tata kelola keamanan data (data *governance*) merupakan fondasi utama dalam melindungi informasi sensitif. Berdasarkan analisis literatur (Firdaus & Wardhani, 2025), terdapat tiga kelemahan mendasar pada tata kelola keamanan BPJS dan PDN.

Pertama, audit keamanan belum dilakukan secara konsisten, terutama pada PDN yang tidak memiliki mekanisme pengawasan rutin. Kedua, manajemen risiko siber tidak terintegrasi sehingga respons terhadap insiden menjadi lambat dan tidak terarah. Ketiga, tanggung jawab kelembagaan tidak terstruktur, terutama pada PDN yang melibatkan banyak vendor tanpa kejelasan komando maupun koordinasi.

Tabel 2. Indikator Tata Kelola Keamanan Data Publik

| **Indikator** | **BPJS Kesehatan** | **PDN 2024** |
|---|---|---|
| Transparansi Kebijakan Data | Sedang | Rendah |
| Audit Keamanan Berkala | Cukup baik | Tidak ada |
| Manajemen Risiko Siber | Ada sebagian | Belum berjalan |
| Tanggung Jawab Lembaga | Jelas | Tumpang tindi |
| Perlindungan Privasi | Sedang | Lemah |

**Sumber:** Analisis berdasarkan BSSN (2024), (Firdaus & Wardhani, 2025; Nugraha et al., 2025)

BPJS Kesehatan telah melakukan beberapa upaya untuk memperkuat tata kelola keamanan data, seperti adanya audit keamanan berkala dan manajemen risiko yang parsial. Namun, langkah-langkah ini masih bersifat reaktif pascainsiden dan belum sepenuhnya terintegrasi ke dalam sistem tata kelola yang berkelanjutan. Sebaliknya, PDN 2024 menunjukkan kelemahan yang lebih signifikan, misalnya tidak adanya audit keamanan berkala, manajemen risiko yang tidak berjalan, serta tanggung jawab

lembaga yang tumpang tindih. Kondisi ini sejalan dengan temuan literatur yang menunjukkan bahwa sebagian besar lembaga publik di Indonesia belum mencapai tingkat maturity keamanan siber yang memadai (Marcal et al., 2025).

Secara keseluruhan, hasil analisis memperlihatkan bahwa tata kelola keamanan data di institusi publik belum mampu memberikan perlindungan yang konsisten terhadap risiko siber.

***Analisis Resiliensi Siber***

Resiliensi siber mengacu pada kemampuan lembaga mempertahankan kontinuitas layanan serta memulihkan sistem ketika terjadi insiden. Dalam konteks ini, BPJS dan PDN menunjukkan perbedaan yang sangat signifikan.

BPJS masih dapat mempertahankan operasional dasar meskipun mengalami kebocoran data, yang menunjukkan keberadaan mekanisme pemulihan tertentu. Meski demikian, langkah pemulihan ini belum menjamin keamanan data anggota secara menyeluruh untuk jangka panjang.

Sebaliknya, PDN mengalami kelumpuhan total karena tidak memiliki backup real-time dan tidak memiliki disaster recovery plan yang memadai. Hal ini mengindikasikan tingkat resiliensi yang sangat rendah pada infrastruktur yang seharusnya menjadi tulang punggung digital pemerintah.

*Tabel 3. Distribusi Serangan Siber terhadap Sektor Pemerintah (2019–2024)*

| | |
|---|---|
| Pemerintahan | 38% |
| Pendidikan | 21% |
| Kesehatan | 14% |
| Keuangan | 10% |
| Lainnya | 17% |

***Sumber:*** *Laporan Keamanan Siber BSSN (2024)*

Temuan ini konsisten dengan (Khudori & Lala, 2024) yang menyatakan bahwa resiliensi hanya dapat dicapai jika lembaga memiliki rencana pemulihan bencana yang terukur serta struktur komando yang jelas. Pada kasus PDN, kedua hal tersebut tidak terlihat.

***Etika Profesional Teknologi Informasi***

Etika profesional TI berperan penting dalam menjamin kerahasiaan, akurasi, dan integritas data publik. Sebagaimana disampaikan oleh (Coda Sofiq Indonesiawan et al., 2021), kebocoran data bukan hanya akibat kelemahan teknis, tetapi juga lahir dari lemahnya integritas moral dan pengawasan terhadap individu yang memiliki akses pada data..

Tabel 4. Dimensi Etika Profesional TI dalam Penanganan Kebocoran Data

| Dimensi Etika | BPJS Kesehatan | PDN 2024 |
|---|---|---|
| Integritas | Sedang | Rendah |
| Kompetensi | Cukup | Rendah |
| Tanggung Jawab | Baik | Kurang |
| Akuntabilitas | Cukup | Rendah |
| Transparansi | Kurang | Rendah |

**Sumber:** (Coda Sofiq Indonesiawan et al., 2021; Ingrida & Wibowo, 2024; Maulida & Utomo, 2023)

BPJS menunjukkan penerapan etika profesional yang relatif lebih baik melalui klarifikasi publik serta pelaksanaan audit pascainsiden. Sebaliknya, PDN dinilai lambat dalam menyampaikan informasi kepada publik dan minim transparansi selama proses penanganan insiden, sehingga memperburuk persepsi publik.

***Perbandingan Keseluruhan Kasus BPJS dan PDN***

Tabel 5. Perbandingan Utama BPJS Kesehatan dan PDN 2024

| Dimensi Etika | BPJS Kesehatan 2021 | PDN 2024 |
|---|---|---|
| Jenis Insiden | Kebocoran data pribadi | Serangan ransomware |

| | | |
|---|---|---|
| Dampak | Data bocor dijual online | Layanan digital lumpuh |
| Tata Kelola | Ada audit & koordinasi | Tidak ada audit rutin |
| Resiliensi | Cukup tinggi | Rendah |
| Etika Profesional | Kurang transparan | Kurang akuntabel |
| Respons Pemerintah | Cepat (BSSN & Kominfo) | Lambat dan parsial |

**Sumber:** Analisis Penulis (2025) berdasarkan data BSSN, Katadata,Kompas, dan jurnal terkait.

Perbandingan ini menunjukkan bahwa BPJS memiliki tingkat kematangan tata kelola yang lebih baik meskipun masih jauh dari ideal. Sebaliknya, PDN memperlihatkan kegagalan struktural yang menghambat proses pemulihan dan respons insiden secara efektif.

***Pembahasan Reflektif***

Analisis komparatif mengungkap bahwa akar persoalan kebocoran data publik tidak hanya terletak pada aspek teknis, tetapi juga pada ketidakterpaduan antara tata kelola, etika profesional TI, dan resiliensi siber. Ketiga aspek ini harus berjalan secara selaras agar mampu mencegah dan meminimalkan dampak insiden keamanan data.

BPJS Kesehatan menunjukkan koordinasi yang relatif lebih baik dan respons yang lebih cepat, meskipun masih terdapat kekurangan dalam aspek transparansi dan pengawasan internal. Sebaliknya, PDN 2024 memperlihatkan kelemahan sistemik yang mencakup tata kelola yang lemah, kesiapan teknis yang rendah, serta terbatasnya kemampuan pemulihan. Kondisi ini mempertegas bahwa tanpa tata kelola yang kuat dan penerapan etika TI yang konsisten, resiliensi siber tidak akan tercapai apa pun teknologi yang digunakan.

Hasil perbandingan ini menekankan bahwa kelemahan utama pengelolaan data publik di Indonesia terletak pada minimnya integrasi antara etika profesional TI, tata kelola, dan resiliensi siber. BPJS lebih cepat dalam menanggapi krisis, menunjukkan adanya kesadaran etika dan koordinasi kelembagaan yang lebih baik. Sebaliknya, PDN memperlihatkan kelemahan sistemik baik dari aspek teknis maupun moral. Temuan ini sejalan dengan (Nugraha et al., 2025) yang menyatakan bahwa "tantangan terbesar keamanan data publik bukan pada teknologi, melainkan pada integritas manusia yang mengelolanya." Dengan demikian, penerapan prinsip etika profesional TI menjadi elemen kunci dalam membangun sistem tata kelola data publik yang kuat dan resiliensi siber nasional yang berkelanjutan.

## IV. SIMPULAN

Berdasarkan analisis komparatif terhadap kasus kebocoran data BPJS Kesehatan tahun 2021 dan insiden serangan *ransomware* pada Pusat Data Nasional (PDN) tahun 2024, penelitian ini menunjukkan bahwa kelemahan etika profesional TI, ketidakterpaduan tata kelola keamanan data, serta rendahnya tingkat resiliensi siber merupakan faktor utama yang memperburuk dampak insiden kebocoran data publik di Indonesia. Hasil penelitian menunjukkan bahwa BPJS Kesehatan memiliki struktur tata kelola dan koordinasi yang relatif lebih baik, termasuk pelaksanaan audit pascainsiden serta mekanisme pemulihan layanan, meskipun transparansi dan penerapan prinsip *privacy-by-design* belum optimal. Sebaliknya, PDN 2024 memperlihatkan kegagalan tata kelola yang lebih mendasar, ditandai kurangnya audit keamanan berkala, lemahnya pengawasan vendor, tidak adanya sistem backup real-time, serta ketiadaan *disaster recovery plan* yang mengakibatkan kelumpuhan layanan digital pemerintah secara luas. Temuan ini sejalan dengan tinjauan pustaka yang menekankan pentingnya integritas etika profesional, penerapan standar keamanan seperti ISO/IEC 27001, serta perlunya manajemen risiko siber yang terstruktur untuk mendukung transformasi digital sektor publik. Dengan demikian, penelitian ini menegaskan bahwa penguatan etika profesional TI, peningkatan tata kelola keamanan data, dan pembangunan resiliensi siber yang berkelanjutan merupakan prasyarat penting bagi perlindungan data publik dan pemulihan kepercayaan masyarakat terhadap layanan digital pemerintah.

## V. REFERENSI

Aryanti, D. R. (2025). Cybersecurity Governance In Public Institutions : Managing Digital Risks And Resilience. Visioner: Jurnal Pemerintahan Daerah Di Indonesia, 17(3), 24–35. Https://Doi.Org/Https://Doi.Org/10.54783/Jv.V17i3.1424

Asiyanti, A. P. D., & Agussalim Agussalim. (2024). Strategi Manajemen Risiko Dan Keamanan Siber Dalam Ekonomi Digital: Tinjauan Literatur. Jurnal Penelitian Sistem Informasi (Jpsi), 2(4), 90–110. Https://Doi.Org/10.54066/Jpsi.V2i4.2562

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance And Indonesian Cyber Diplomacy By National Cyber And Encryption

Agency]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 10(2), 113–128. Https://Doi.Org/10.22212/Jp.V10i2.1447

Coda Sofiq Indonesiawan, R., Alroy, M., Laras Suci, T., & Rizky Prasetyo, B. (2021). Analisis Privasi Data Pengguna Dalam Instansi Bpjs Kesehatan Analysis Of User Data Privacy In Bpjs Kesehatan Institution. Prosiding Seminar Nasional Teknologi Dan Sistem Informasi, 1(1), 174–182.

Fadli, M. R. (2021). Memahami Desain Metode Penelitian Kualitatif. Humanika, 21(1), 33–54. Https://Doi.Org/10.21831/Hum.V21i1.38075

Firdaus, A., & Wardhani, D. F. (2025). Melindungi Privasi Di Era Digital: Keamanan Data Pribadi Di Indonesia. Inovasi Pembangunan: Jurnal Kelitbangan, 13(1).

Fransciko Pritama, Ekat Rueh Daya Leluni, Yovita, & Jadiaman Parhusip. (2024). Analisis Pelanggaran Etika Profesi Keamanan Siber (Studi Kasus Kebocoran Data Pajak Di Indonesia). Teknik: Jurnal Ilmu Teknik Dan Informatika, 4(2), 53–56. Https://Doi.Org/10.51903/Teknik.V4i2.585

Ingrida, N. V., & Wibowo, D. (2024). Digital Security In Human Security: A Case Study Of The Bjorka Hacking Incident. Politicos: Jurnal Politik Dan Pemerintahan, 4(1), 56–65. Https://Doi.Org/10.22225/Politicos.4.1.2024.56-65

Isik, O. (2025). Qualitative Research Approaches And Data Collection Methods: Understanding Meaning And Experience. Journal Of Humanities And Education Development, 7(6), 19–32. Https://Doi.Org/10.22161/Jhed.7.6.3

Kayode-Bolarinwa, G. (2025). Cybersecurity Awareness And Risk Management In The Public Sector. International Journal Of Intelligent Systems And Applications In Engineering, 13(1s), 146–152. Https://Ijisae.Org/Index.Php/Ijisae/Article/View/7609

Khudori, A., & Lala, A. (2024). Legal Implications Of Data Breach Cases In Indonesia: Challenges And Solutions In The Era Of Personal Data Protection. Indonesian Cyber Law Review, 1(1), 13–20. Https://Doi.Org/10.59261/Iclr.V1i1.1

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information Security Governance In The Public Sector: Investigations, Approaches, Measures, And Trends. International Journal Of Information Security, 24(4), 177. Https://Doi.Org/10.1007/S10207-025-01097-X

Maharani, T. (2021). Dugaan Kebocoran Data 279 Juta Wni, Bpjs Kesehatan Tempuh Langkah Hukum. Kompas. Https://Nasional.Kompas.Com/Read/2021/05/25/11140881/Dugaan-Kebocoran-Data-279-Juta-Wni-Bpjs-Kesehatan-Tempuh-Langkah-Hukum

Marcal, A., Tommy, S., Irwan Padli Nasution, M., Manajemen, P., & Ekonomi Dan Bisnis Islam, F. (2025). Evaluasi Manajemen Risiko Keamanan Siber Pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (Pdn). Jurnal Ilmiah Ekonomi Dan Manajemen, 3(6), 330–346. Https://Doi.Org/10.61722/Jiem.V3i6.5266

Maulida, O., & Utomo, H. (2023). Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (Bpjs) Kesehatan Atas Kebocoran Data Pribadi Pengguna Dalam Perspektif Hukum Pidana. Indonesian Journal Of Law And Justice, 1(2), 10. Https://Doi.Org/10.47134/Ijlj.V1i2.2011

Nugraha, D. A., Nurfitroh, R., Ul-Haq, N. D., Dika, R. P., & Lagontang, S. N. (2025). Kebocoran Data Bpjs Kesehatan: Ancaman Terhadap Keamanan Informasi Publik Di Era Digital. Integrative Perspectives Of Social And Science Journal, 2(03 Juli), 4685–4691.

Prio Pamungkas, R. Wisn., Saputra, I. E., Alfaridzy, M. D., Pramedya, D. F., & Nugraha, D. A. (2024). Meningkatkan Keamanan Dan Kepatuhan Melalui Tata Kelola It Dengan Metode Scrum Untuk Manajemen Resiko Ti Yang Lebih Fleksibel. Kohesi: Jurnal Sains Dan Teknologi, 5(11), 167–186. Https://Doi.Org/Https://Doi.Org/10.3785/Kohesi.V5i11.9065

Rahmika, A. R., Muhammad Akbar, Deni Luvi Jayanto, & Joshua Reska Bu'tu. (2025). Cloud Governance Frameworks: Cia-Based Security And Compliance. Journal Of Embedded Systems, Security And Intelligent Systems, 379–389. Https://Doi.Org/10.59562/Jessi.V6i3.9541

Ridzqi Fauzi, T., Salamah, U., & Hendrawan, H. (2025). Tata Kelola Keamanan Digital Siber Pemerintah Pada Diskominfo Kabupaten Garut. Jurnal Ilmu Multidisiplin, 4(1), 447–457. Https://Doi.Org/10.38035/Jim.V4i1.883

Setyowati, D. (2024). Fakta Pusat Data Nasional Down: Uang Tebusan, Ransomware, Lokasi, Efek. Katadata. Https://Katadata.Co.Id/Digital/Teknologi/667a509c1dbed/Fakta-Pusat-Data-Nasional-Down-Uang-Tebusan-Ransomware-Lokasi-Efek

Sinaga, R., & Taan, F. (2024). Penerapan Iso/Iec 27001:2022 Dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses Dan Kendala. Nuansa Informatika, 18(2), 46–54. Https://Doi.Org/10.25134/Ilkom.V18i2.205

Siti Maesaroh, R. (2025). Tantangan Keamanan Siber Dan Implikasinya Terhadap Hukum Kenegaraan: Tinjauan Atas Peran Negara Dalam Menjamin Ketahanan Digital. Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam, 4(2), 255–274.

Suci Anugrah, Muhammad Zaky Himawan, Nabila Raihana Qalby, & Evy Nurmiati. (2025). Pengaruh Etika Profesi Terhadap Keamanan Informasi Dalam Konteks Kebocoran Data Bsi (Bank Syariah Indonesia): Studi Literatur Sistematis. Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi, 11(2), 106–112. Https://Doi.Org/10.34010/Jtk3ti.V11i2.17033

Syailendra Putra, M. R., Purwanti, P. A., & Istisofani, A. S. (2024). Analisis Keamanan Data Dalam Telematika Hukum: Antara Privasi Dan Transparansi. Jurnal Akuntansi Hukum Dan Edukasi, 1(2), 633–642.