Vol. 4, No. 2, 2026, pp 01-10 ISSN 3123-7444

Jurnal Ilmu Ekonomi dan Bisnis

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

Analisis Etika Sistem Informasi pada Kasus Kebocoran Data PDN 2024: Studi Literatur

Adelsiza Zenoni Harianja[1], Hesly Irawanda Naibaho[2]
[12]adelsizaharianja@gmail.com
[12]Universitas Negeri Medan

Article Info

Article history:
Received Jun 12th, 2026
Revised Aug 20th, 2026
Accepted Jun 26th, 2026

Kata Kunci:
Etika Sistem Informasi
Kebocoran Data
Pusat Data Nasional

ABSTRAK

Perkembangan transformasi digital di Indonesia mendorong peningkatan penggunaan sistem informasi dalam pelayanan publik, termasuk melalui pembangunan Pusat Data Nasional (PDN). Namun, meningkatnya penggunaan teknologi juga diikuti oleh tingginya ancaman keamanan siber. Penelitian ini bertujuan untuk menganalisis kasus kebocoran data PDN 2024 dari perspektif etika sistem informasi. Penelitian menggunakan metode studi literatur. Hasil penelitian menunjukkan bahwa kasus PDN tidak hanya menunjukkan kelemahan teknis dalam keamanan siber, tetapi juga memperlihatkan pelanggaran etika berupa rendahnya perlindungan privasi data, lemahnya perlindungan hak kepemilikan data, serta menurunnya aksesibilitas layanan publik. Kesimpulannya, bahwa penguatan tata kelola sistem informasi, peningkatan keamanan siber, dan perlindungan data yang efektif diperlukan untuk mendukung transformasi digital yang aman dan berkelanjutan di Indonesia.

ABSTARCT

The development of digital transformation in Indonesia has increased the use of information systems in public services, including through the establishment of the National Data Center (Pusat Data Nasional/PDN). However, the growing dependence on digital technology has also been accompanied by increasing cybersecurity threats. This study aimed to analyze the 2024 PDN data breach case from the perspective of information systems ethics. This study employed a literature review method with a qualitative descriptive approach. The findings indicated that the PDN incident did not only reveal technical weaknesses in cybersecurity but also demonstrated ethical failures, including inadequate data privacy protection, weak protection of data ownership rights, and reduced accessibility of public services. This study concluded that strengthening information system governance, enhancing cybersecurity, and implementing effective data protection are essential to support secure and sustainable digital transformation in Indonesia.

Corresponding Author:
Adelsiza Zenoni Harianja, Hesly Irawanda Naibaho
Universitas Negeri Medan
Email: adelsizaharianja@gmail.com

Latar Belakang

Perkembangan teknologi informasi telah mendorong pemerintah Indonesia untuk melakukan transformasi digital dalam berbagai sektor pelayanan publik. Sistem informasi digunakan untuk meningkatkan efisiensi, integrasi data, dan kualitas pelayanan kepada masyarakat. Salah satu upaya pemerintah dalam mendukung transformasi digital tersebut adalah pembangunan Pusat Data Nasional (PDN) yang berfungsi sebagai pusat penyimpanan dan pengelolaan data berbagai instansi pemerintah. Namun, semakin berkembangnya penggunaan teknologi digital juga diikuti dengan meningkatnya ancaman keamanan siber. Berdasarkan data Badan Siber dan Sandi Negara (BSSN), total trafik anomali siber di Indonesia selama tahun 2023 mencapai 403.990.813 anomali. Selain itu, ditemukan 1.011.209 aktivitas ransomware dan 4.001.905 aktivitas *Advanced Persistent Threat* (APT) yang menunjukkan tingginya ancaman terhadap keamanan sistem digital nasional.

Tingginya ancaman siber tersebut membuktikan bahwa keamanan informasi menjadi tantangan besar dalam pengelolaan sistem informasi di Indonesia. Penelitian mengenai statistik kejahatan siber tahun 2024 menunjukkan bahwa Indonesia mengalami peningkatan signifikan pada kasus phishing, ransomware, dan penipuan digital. Pada tahun 2024 tercatat sekitar 26,7 juta aktivitas phishing dan 514 ribu serangan ransomware yang menyerang berbagai sektor, termasuk lembaga pemerintahan. Selain itu, tingkat kekhawatiran masyarakat terhadap penipuan online meningkat dari 10,3% pada tahun 2023 menjadi 32,5% pada tahun 2024. Data tersebut menunjukkan bahwa ruang digital kini menjadi area yang sangat rentan terhadap kejahatan siber dan kebocoran data.

Salah satu kasus keamanan siber terbesar di Indonesia pada tahun 2024 adalah serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) yang terjadi pada 20 Juni 2024. Serangan tersebut menyebabkan gangguan pada berbagai layanan publik nasional, termasuk layanan imigrasi dan administrasi pemerintahan lainnya. Berdasarkan hasil identifikasi Badan Siber dan Sandi Negara, serangan tersebut dilakukan menggunakan ransomware Brain Cipher, yaitu pengembangan dari LockBit 3.0. Selain itu, ditemukan adanya upaya penonaktifan fitur keamanan Windows Defender sejak 17 Juni 2024 yang menyebabkan aktivitas berbahaya dapat masuk ke sistem. Bahkan, laporan lain menyebutkan bahwa sekitar 210 instansi pemerintah terdampak akibat gangguan pada PDNS tersebut.

Penelitian terdahulu mengenai kasus kebocoran data Pusat Data Nasional tahun 2024 menunjukkan bahwa permasalahan utama tidak hanya terletak pada aspek teknis keamanan siber, tetapi juga pada tata kelola dan tanggung jawab dalam pengelolaan sistem informasi pemerintah. Penelitian oleh (Adristi & Ramadhani, 2024) menjelaskan bahwa serangan terhadap PDNS 2 Surabaya memperlihatkan lemahnya budaya keamanan siber dalam sistem pemerintahan Indonesia, terutama dalam kesiapan mitigasi risiko dan perlindungan data digital. Penelitian tersebut menyoroti bahwa rendahnya kesadaran keamanan siber dapat memperbesar dampak serangan terhadap layanan publik dan kepercayaan masyarakat. Selain itu, penelitian (Bua & Idris, 2025) menyatakan bahwa kebocoran data nasional tahun 2024 menunjukkan perlunya penguatan kebijakan keamanan siber dan evaluasi tata kelola sistem digital pemerintah agar mampu menghadapi ancaman ransomware dan serangan siber modern. Sementara itu, penelitian (Fatimah Asrianti et al., 2025) menegaskan bahwa kasus kebocoran data pada PDN Kominfo memperlihatkan pentingnya penerapan keamanan cloud yang lebih ketat dalam era digitalisasi pemerintahan.

Kasus kebocoran data dan serangan ransomware terhadap PDN tidak hanya menjadi persoalan teknis, tetapi juga berkaitan erat dengan etika sistem informasi. Etika sistem informasi menekankan pentingnya tanggung jawab organisasi dalam menjaga keamanan, kerahasiaan, dan integritas data pengguna. Pemerintah sebagai pengelola data publik memiliki kewajiban moral untuk melindungi data masyarakat dari ancaman penyalahgunaan dan kebocoran. Apabila sistem keamanan tidak dikelola dengan baik hingga menyebabkan terganggunya layanan publik dan berpotensi membahayakan data masyarakat, maka hal tersebut dapat dianggap sebagai bentuk kelalaian etis dalam pengelolaan sistem informasi. Oleh karena itu, penelitian ini penting dilakukan untuk menganalisis aspek etika sistem informasi pada kasus kebocoran data PDN 2024 melalui metode studi literatur agar dapat memberikan pemahaman mengenai dampak, bentuk pelanggaran

etika, serta upaya pencegahan yang perlu dilakukan dalam pengelolaan sistem informasi di Indonesia.

Pengertian Sistem Informasi

Sistem informasi merupakan suatu sistem yang memiliki peran penting dalam membantu organisasi maupun instansi pemerintahan dalam mengelola data dan menghasilkan informasi yang dibutuhkan untuk mendukung kegiatan operasional serta pengambilan keputusan. Dalam perkembangannya, sistem informasi tidak hanya berkaitan dengan teknologi komputer, tetapi juga melibatkan manusia, prosedur kerja, komunikasi, dan pengelolaan data yang saling terintegrasi.

Menurut O'Brien, sistem informasi adalah kombinasi dari setiap unit yang dikelola oleh manusia (*people*), perangkat keras (*hardware*), perangkat lunak (*software*), jaringan komputer dan komunikasi data (*communication*), serta basis data (*database*) yang berfungsi untuk mengumpulkan, mengolah, dan menyebarkan informasi dalam suatu organisasi. Sementara itu, menurut (Laudon & Laudon, 2018), sistem informasi merupakan sekumpulan komponen yang saling berhubungan untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi guna mendukung pengendalian, koordinasi, analisis, dan pengambilan keputusan dalam organisasi.

Selain itu, Joperson dalam Harumy (Fadilah et al., 2020) menyatakan bahwa sistem informasi adalah suatu sistem yang dirancang dalam perusahaan untuk memenuhi kebutuhan pengelolaan transaksi sehari-hari, mendukung kegiatan operasional dan manajerial, serta menyediakan laporan yang dibutuhkan oleh pihak-pihak tertentu di luar organisasi. Pendapat lain dikemukakan oleh Jhon F. Nash yang menjelaskan bahwa sistem informasi merupakan gabungan dari manusia, fasilitas atau alat teknologi, media, prosedur, dan pengendalian yang dirancang untuk mengatur komunikasi penting, memproses transaksi tertentu secara rutin, membantu manajemen serta pengguna internal dan eksternal, dan menyediakan dasar yang tepat dalam pengambilan keputusan.

Dalam era digital, sistem informasi memiliki peran penting dalam meningkatkan efisiensi kerja, mempercepat arus informasi, serta membantu organisasi maupun pemerintah dalam memberikan pelayanan yang lebih efektif kepada masyarakat. Penerapan sistem informasi tidak hanya digunakan pada sektor bisnis, tetapi juga telah menjadi bagian penting dalam tata kelola pemerintahan, terutama dalam pengelolaan data publik dan pelayanan berbasis digital. Dalam konteks pemerintahan digital, sistem informasi menjadi fondasi utama dalam pengelolaan data nasional karena mampu mengintegrasikan data antarinstansi sehingga pelayanan publik dapat dilakukan secara lebih cepat dan terstruktur. Namun, semakin besarnya ketergantungan terhadap sistem informasi juga meningkatkan risiko keamanan siber apabila sistem tidak dilengkapi dengan perlindungan dan pengelolaan keamanan yang baik.

Berdasarkan beberapa pengertian tersebut, dapat disimpulkan bahwa sistem informasi merupakan suatu kombinasi antara manusia, teknologi, prosedur, jaringan komunikasi, dan basis data yang saling terintegrasi untuk mengumpulkan, mengolah, menyimpan, dan mendistribusikan informasi guna mendukung kegiatan operasional, pengendalian, serta pengambilan keputusan dalam suatu organisasi atau instansi. Sistem informasi juga menjadi bagian penting dalam mendukung efektivitas pelayanan dan pengelolaan data di era digital.

Metode Penelitian

Metode studi literatur merupakan metode penelitian yang dilakukan dengan mengumpulkan dan menganalisis berbagai referensi tertulis untuk memperoleh pemahaman yang lebih mendalam mengenai suatu fenomena atau permasalahan tertentu. Menurut (Snyder, 2019), *literature review* berfungsi untuk mengidentifikasi, mengevaluasi, dan menginterpretasikan hasil penelitian terdahulu sehingga dapat memberikan dasar teoritis yang kuat dalam suatu penelitian.

Penelitian ini menggunakan metode studi literatur (literature review) dengan pendekatan deskriptif kualitatif. Metode studi literatur dipilih karena penelitian berfokus pada pengumpulan, pengkajian, dan analisis berbagai sumber tertulis yang berkaitan dengan kasus kebocoran data Pusat Data Nasional tahun 2024 serta etika sistem informasi. Data dalam penelitian ini diperoleh dari jurnal ilmiah, artikel penelitian, berita resmi, dokumen pemerintah, dan sumber akademik lain yang relevan dengan topik penelitian. Pendekatan deskriptif digunakan untuk menjelaskan secara sistematis fenomena kebocoran data PDN serta dampaknya terhadap keamanan informasi dan etika pengelolaan data digital.

Teknik pengumpulan data dilakukan melalui penelusuran berbagai sumber literatur menggunakan database akademik seperti Google Scholar, Garuda Kemdikbud, dan jurnal nasional terkait keamanan siber serta sistem informasi. Literatur yang digunakan dipilih berdasarkan kesesuaian tema, tahun publikasi, dan relevansi dengan kasus kebocoran data PDN 2024. Selanjutnya, data dianalisis menggunakan teknik analisis deskriptif dengan mengidentifikasi permasalahan, dampak, serta aspek etika sistem informasi yang muncul dalam kasus tersebut. Hasil analisis kemudian disusun untuk memperoleh pemahaman mengenai bentuk pelanggaran etika, tanggung jawab pengelola sistem informasi, dan upaya pencegahan terhadap kebocoran data di Indonesia.

Hasil dan Pembahasan

Kronologi Kasus Kebocoran Data PDN 2024

Kasus Kebocoran Data Pusat Data Nasional (2024) merupakan salah satu kasus kebocoran data terbesar dalam sejarah Indonesia. Data 1,3 miliar penduduk Indonesia diduga bocor dan diperjualbelikan di dark web. Data yang bocor mencakup Nomor Induk Kependudikan (NIK), nama lengkap, alamat, dan informasi pribadi lainnya. Kasus ini menunjukkan lemahnya sistem keamanan infrastruktur digital pemerintah. Beberapa platform e-commerce besar di Indonesia juga mengalami kebocoran data pengguna yang mencakup informasi nama, alamat email, nomor telepon, dan riwayat transaksi. Data tersebut kemudian diperjualbelikan secara ilegal dan digunakan untuk penipuan. Banyak aplikasi pinjaman online ilegal yang menyalahgunakan akses ke data pribadi pengguna, termasuk kontak telepon, foto, dan lokasi. Data ini kemudian digunakan untuk intimidasi dan penagihan yang melanggar privasi. Temuan ini sejalan dengan penelitian (Simanullang et al., 2026) yang mengidentifikasi berbagai celah keamanan dalam sistem informasi rumah sakit yang dapat menyebabkan kebocoran data pasien.

Peristiwa ini semakin memperlihatkan bahwa pengelolaan sistem informasi pemerintah masih memiliki kelemahan pada aspek tata kelola keamanan (IT governance) dan manajemen risiko siber. Menurut Badan Siber dan Sandi Negara (2024), serangan terhadap PDN melibatkan teknik ransomware yang mampu melumpuhkan sistem dan membuka peluang eksfiltrasi data. Hal ini menunjukkan bahwa kesiapan sistem dalam menghadapi ancaman siber tingkat tinggi masih belum optimal. Fenomena kebocoran data juga tidak hanya terjadi pada sektor pemerintahan. Beberapa platform e-commerce besar di Indonesia pernah mengalami kebocoran data pengguna yang mencakup informasi nama, alamat email, nomor telepon, dan riwayat transaksi. Data tersebut kemudian diperjualbelikan secara ilegal dan digunakan untuk berbagai modus kejahatan siber seperti phishing, social engineering, dan penipuan digital. Menurut laporan (Association of Certified Fraud Examiners, 2024), data pribadi yang bocor menjadi salah satu sumber utama meningkatnya kasus penipuan berbasis rekayasa sosial di era digital.

Selain itu, maraknya aplikasi pinjaman online ilegal turut memperparah risiko penyalahgunaan data pribadi. Aplikasi tersebut meminta akses ke kontak telepon, foto, lokasi, dan berbagai data sensitif lainnya yang kemudian disalahgunakan sebagai alat intimidasi saat proses penagihan. Praktik ini menunjukkan lemahnya pengawasan terhadap aplikasi digital serta rendahnya kesadaran masyarakat terhadap pentingnya perlindungan data pribadi. Kondisi ini memperlihatkan bahwa pelanggaran etika sistem informasi tidak hanya terjadi karena kelemahan teknologi, tetapi juga karena kurangnya regulasi yang ditegakkan secara efektif. Temuan ini sejalan dengan penelitian (Simanullang et al., 2026) yang mengidentifikasi berbagai celah keamanan dalam sistem informasi

rumah sakit yang dapat menyebabkan kebocoran data pasien. Penelitian tersebut menekankan bahwa kelemahan sistem sering kali berasal dari kurangnya audit keamanan, minimnya standar pengamanan, serta rendahnya kesadaran pengelola sistem terhadap risiko kebocoran data.

Dengan demikian, rangkaian kasus kebocoran data di berbagai sektor ini menunjukkan pola yang sama, yaitu lemahnya tata kelola keamanan sistem informasi, kurangnya pengawasan, serta belum optimalnya penerapan prinsip etika dalam pengelolaan data digital. Kebocoran data tidak lagi dapat dipandang sebagai insiden teknis semata, tetapi merupakan indikasi kegagalan sistemik dalam pengamanan informasi dan manajemen risiko di era transformasi digital.

Analisis Etika Sistem Informasi

Berdasarkan analisis data yang dilakukan, ditemukan beberapa kategori utama pelanggaran etika IT yang terjadi di Indonesia periode 2020-2024. Kategorisasi ini menggunakan framework PAPA (Privacy, Accuracy, Property, Accessibility) dari Mason sebagai dasar analisis.

Privacy (Privasi) dilanggar karena data masyarakat yang seharusnya dijaga kerahasiaannya berada dalam kondisi rentan akibat lemahnya sistem keamanan. Dalam konteks sistem informasi pemerintahan, privasi bukan hanya isu teknis, tetapi juga menyangkut kepercayaan publik (public trust). Ketika negara mengumpulkan, menyimpan, dan mengelola data pribadi warga, maka negara memiliki kewajiban moral yang sangat tinggi untuk menjamin bahwa data tersebut tidak disalahgunakan, diakses tanpa izin, ataupun bocor ke pihak yang tidak berwenang. Kegagalan menjaga privasi ini menunjukkan bahwa prinsip kehati-hatian (due care) dan perlindungan maksimal (due diligence) belum diterapkan secara optimal. Pemerintah sebagai pengelola data publik memiliki tanggung jawab moral dan hukum sesuai dengan Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022 untuk memastikan perlindungan data pribadi melalui pengamanan teknis, administratif, dan kebijakan yang memadai.

Accuracy (Akurasi) terdampak karena gangguan sistem berpotensi menyebabkan kerusakan, perubahan, atau kehilangan data penting yang dapat memengaruhi keakuratan informasi layanan publik. Dalam etika sistem informasi, akurasi berkaitan dengan integritas data (data integrity), yaitu jaminan bahwa data tetap utuh, benar, dan tidak mengalami manipulasi. Serangan ransomware yang mengenkripsi sistem berisiko menyebabkan inkonsistensi data, hilangnya histori data, atau bahkan perubahan data tanpa terdeteksi. Hal ini dapat berdampak pada kesalahan pengambilan keputusan administrasi publik, seperti kesalahan data kependudukan, keimigrasian, atau layanan sosial lainnya. Ketika akurasi data terganggu, maka kualitas layanan publik juga ikut menurun dan berpotensi merugikan masyarakat.

Property (Hak Kepemilikan) berkaitan dengan kepemilikan data oleh masyarakat. Data pribadi pada hakikatnya adalah milik individu, sedangkan pemerintah hanya bertindak sebagai pengelola (data controller). Kebocoran atau akses ilegal terhadap data menunjukkan bahwa hak kepemilikan informasi tidak dijaga secara optimal. Dalam perspektif etika, hal ini menunjukkan bahwa kontrol atas data individu berpindah ke pihak yang tidak berhak, sehingga merampas hak individu atas informasi pribadinya. Pelanggaran terhadap aspek property ini juga membuka peluang terjadinya eksploitasi data untuk kepentingan kejahatan siber, penipuan, atau penyalahgunaan identitas.

Accessibility (Hak Akses) juga terganggu karena layanan publik tidak dapat diakses oleh masyarakat akibat sistem yang lumpuh. Dalam sistem informasi pemerintahan, aksesibilitas berarti masyarakat memiliki hak untuk mendapatkan layanan secara cepat, tepat, dan berkelanjutan. Ketika sistem tidak dapat diakses, maka hak masyarakat atas layanan digital tidak terpenuhi. Ini menunjukkan kegagalan dalam menjaga ketersediaan sistem (availability), yang merupakan salah satu pilar utama keamanan informasi selain confidentiality dan integrity. Lumpuhnya layanan imigrasi dan administrasi lainnya menjadi bukti nyata bahwa aspek aksesibilitas belum diprioritaskan melalui perencanaan sistem cadangan (backup system) dan disaster recovery plan yang memadai.

Kasus ini memperlihatkan bahwa kelemahan dalam pengamanan sistem informasi dapat dikategorikan sebagai bentuk kelalaian etis (ethical negligence) dalam tata kelola teknologi informasi pemerintahan. Kelalaian ini bukan hanya karena kurangnya teknologi, tetapi juga karena kurangnya kesadaran etis, pengawasan, manajemen risiko, serta budaya keamanan siber di lingkungan

pengelola sistem. Dengan demikian, permasalahan kebocoran data PDN 2024 tidak hanya dapat dilihat sebagai kegagalan teknis, tetapi juga sebagai kegagalan dalam menerapkan prinsip-prinsip etika sistem informasi secara menyeluruh dalam pengelolaan data publik.

Dampak Kebocoran Data

Kebocoran data nasional, seperti insiden yang terjadi pada Pusat Data Nasional (PDN) tahun 2024, menimbulkan berbagai dampak serius yang berdampak luas pada aspek ekonomi, sosial, hingga psikologis masyarakat. Dampak ini tidak hanya bersifat langsung seperti kerugian finansial, tetapi juga berdampak jangka panjang terhadap kepercayaan publik dan stabilitas sistem digital nasional. Kebocoran data nasional membuka peluang besar bagi pelaku kejahatan siber untuk melakukan berbagai tindak kriminal seperti pemerasan, penipuan, hingga penyalahgunaan identitas. Data yang bocor sering kali berisi informasi sensitif seperti nomor induk kependudukan, data keuangan, hingga rekam jejak digital individu.

Dampak ekonomi dari kebocoran data sangat signifikan. Perusahaan dan lembaga pemerintah yang menjadi korban harus mengeluarkan biaya besar untuk pemulihan sistem, investigasi, serta kompensasi kepada individu yang terdampak. Selain itu, masyarakat yang datanya bocor berisiko menjadi korban penipuan daring (phishing), pemerasan, hingga pencurian identitas yangdapat merugikan secara finansial dan psikologis. Studi Syahril et al. (2024) bahkan menemukan bahwa kebocoran data dapat memengaruhi perilaku ekonomi masyarakat, termasuk menurunnya kepatuhan terhadap sistem perpajakan akibat hilangnya rasa aman dan percaya pada pemerintah.

Salah satu dampak paling nyata dari kebocoran data nasional adalah penurunan tingkat kepercayaan masyarakat terhadap pemerintah dan penyelenggara layanan digital. Kepercayaan publik merupakan modal sosial yang sangat penting dalam pembangunan sector digital. Ketika masyarakat merasa bahwa data pribadinya tidak aman mereka akan enggan menggunakan layanan digital pemerintah, bahkan bisa beralih ke jalur informal atau menghindari penggunaan layanan sama sekali. (Bua & Idris, 2025) menyoroti bahwa krisis kepercayaan ini dapat berdampak domino pada berbagai sektor termasuk menurunnya kepatuhan pajak, keengganan masyarakat untuk berbagi data, hingga resistensi terhadap program digitalisasi pemerintah.

Upaya Pencegahan dan Solusi

Untuk mengatasi permasalahan kebocoran data, diperlukan upaya komprehensif dari berbagai pihak. Penguatan regulasi dan penegakan hukum menjadi prioritas utama. Pemerintah perlu memastikan UU Perlindungan Data Pribadi diimplementasikan secara efektif dengan sosialisasi, pengawasan, dan penegakan sanksi yang tegas. Menetapkan standar minimum keamanan informasi yang wajib diterapkan oleh semua organisasi yang mengelola data pribadi. Meningkatkan kemampuan aparat penegak hukum dalam menangani kejahatan siber dan pelanggaran etika IT. Memperkuat peran lembaga pengawas seperti Kominfo dan membentuk otoritas independen untuk perlindungan data pribadi.

Peningkatan kesadaran dan literasi digital dapat dilakukan melalui kampanye masif tentang pentingnya keamanan data dan etika IT kepada masyarakat. Memasukkan materi etika IT dalam kurikulum pendidikan formal dari tingkat dasar hingga perguruan tinggi. Mengembangkan program sertifikasi etika IT untuk profesional teknologi informasi. Mendorong organisasi untuk memberikan pelatihan reguler tentang etika dan keamanan IT kepada karyawan.

Penelitian (Manurung et al., 2023) menunjukkan bahwa pelatihan dan edukasi tentang keamanan website dapat meningkatkan kesadaran akan pentingnya perlindungan data. Peningkatan kapasitas teknis meliputi mendorong organisasi untuk meningkatkan investasi pada infrastruktur dan sistem keamanan informasi. Menerapkan standar internasional seperti ISO 27001 untuk manajemen keamanan informasi. Menerapkan prinsip keamanan sejak tahap perancangan sistem, bukan sebagai tambahan di akhir. Melakukan audit keamanan secara rutin untuk mengidentifikasi dan memperbaiki celah keamanan.

(Ashar, 2022) dalam penelitiannya menunjukkan pentingnya penggunaan metode ISSAF dan OWASP dalam menganalisis keamanan web server untuk mengidentifikasi dan memperbaiki

celah keamanan. Penguatan tanggung jawab korporat mencakup setiap organisasi harus memiliki kebijakan etika IT yang jelas dan mengikat. Menunjuk petugas khusus yang bertanggung jawab atas perlindungan data pribadi. Menerbitkan laporan transparansi tentang pengelolaan data dan insiden keamanan. Menyediakan saluran yang aman bagi karyawan dan pengguna untuk melaporkan pelanggaran etika. Kolaborasi multi-stakeholder sangat diperlukan dengan membangun kerjasama antara pemerintah dan sektor swasta dalam meningkatkan keamanan siber nasional. Melibatkan perguruan tinggi dalam penelitian dan pengembangan solusi keamanan informasi. Memberdayakan organisasi masyarakat sipil untuk mengawasi dan mengadvokasi perlindungan data pribadi. Berkolaborasi dengan negara lain dalam pertukaran informasi dan best practices tentang etika IT.

Kesimpulan

Berdasarkan hasil studi literatur mengenai kasus kebocoran data Pusat Data Nasional (PDN) tahun 2024, dapat disimpulkan bahwa insiden tersebut tidak hanya menunjukkan kelemahan pada aspek teknis keamanan siber, tetapi juga mencerminkan adanya permasalahan etika dalam pengelolaan sistem informasi di sektor pemerintahan. Serangan ransomware yang menyebabkan terganggunya layanan publik serta meningkatnya risiko penyalahgunaan data menunjukkan bahwa sistem perlindungan informasi nasional masih belum dikelola secara optimal dalam menghadapi ancaman digital yang semakin kompleks.

Melalui analisis menggunakan konsep PAPA (Privacy, Accuracy, Property, Accessibility), ditemukan bahwa kasus PDN mengandung pelanggaran pada aspek privasi karena kegagalan menjaga kerahasiaan data masyarakat, aspek akurasi akibat potensi terganggunya integritas data, aspek hak kepemilikan karena lemahnya perlindungan terhadap data pribadi sebagai hak individu, serta aspek aksesibilitas karena terhambatnya layanan publik yang bergantung pada sistem digital. Kondisi tersebut menunjukkan bahwa keamanan informasi tidak dapat dipandang hanya sebagai persoalan teknologi, tetapi juga berkaitan dengan tanggung jawab moral, tata kelola, dan akuntabilitas penyelenggara sistem elektronik.

Oleh karena itu, diperlukan upaya yang lebih komprehensif melalui penguatan regulasi perlindungan data, peningkatan budaya keamanan siber, penerapan standar keamanan informasi, audit sistem secara berkala, serta peningkatan literasi digital bagi masyarakat dan pengelola sistem. Selain itu, kolaborasi antara pemerintah, sektor swasta, akademisi, dan masyarakat menjadi faktor penting dalam membangun ekosistem digital yang aman, etis, dan mampu menjaga kepercayaan publik terhadap transformasi digital di Indonesia.

Daftar Pustaka

Adristi, F., & Ramadhani, E. (2024). *Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (Pdns 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber Dan Dimensi Budaya Nasional Hofstede*. *02*(06), 196–212. Https://Journal.Uii.Ac.Id/Selma/Index

Amalia, R., Kasmiati, N., Yorismanto, Y., Hartono, B., & Daut, A. G. (2025). Etika Dalam Penggunaan Jaringan Untuk Sistem Informasi Rumah Sakit. *Riggs: Journal Of Artificial Intelligence And Digital Business*, *4*(2), 5262–5268. Https://Doi.Org/10.31004/Riggs.V4i2.1419

Anhar, A., Munip, A., & Haeran. (2025). Optimalisasi Pelayanan Sistem Informasi Administrasi Di Kua Geragai Tanjung Jabung Timur. *Swakarya: Jurnal Penelitian Sosial Dan Pemberdayaan Masyarakat*, *3*(2). Https://Afeksi.Id/Journal3/Index.Php/Swakarya

Ashar, R. (2022). Analisis Keamanan Open Website Menggunakan Metode Owasp Dan Issaf. *Jurnal Informasi Dan Teknologi*, *4*(4), 211–218. Https://Doi.Org/10.37034/Jsisfotek.V4i4.233

Association Of Certified Fraud Examiners. (2024). *Occupational Fraud 2024: A Report To The Nations*.

Badan Siber dan Sandi Negara. (2024). Laporan investigasi insiden kebocoran data Pusat Data Nasional. Jakarta: BSSN.

Bua, I. T., & Idris, N. I. (2025). Analisis Kebijakan Keamanan Siber Di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024. *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, *2*(2), 100–114. Https://Doi.Org/10.62383/Desentralisasi.V2i2.653

Fadilah, S. C., Rianto, H., & Hartati, T. (2020). Implementasi Framework Code Iginter Menggunakan Metode Waterfall Pada Sistem Informasi Penjualan Pt. Supreme Jaya Abadi. *Jisicom (Journal Of Information System, Informatics And Computing)*, *4*(1), 134–140. Http://Journal.Stmikjayakarta.Ac.Id/Index.Php/Jisicom

Fatimah Asrianti, N., Ghaza Alghazali, M., Yulistianti Putri, I., Dio Nurul Awalia, A., Teknik Informatika Dan Komputer, J., Teknik, F., Negeri Makassar Jl Bonto Langkasa, U., Banta-Bantaeng, K., Rapocini, K., & Makassar, K. (2025). Kasus Kebocoran Data Pada Pusat Data Nasional Kominfo: Pentingnya Keamanan Cloud Di Era Digitalisasi. *Innovation In Computer Education Journal*, *1*(1), 24–33. Https://Journal.Unm.Ac.Id/Index.Php/Icej/Article/View/7740/4852

Laudon, K. J., & Laudon, J. P. (2018). *Management Information Systems: Managing The Digital Firm (15th Ed.)* (15th Ed.). Pearson Education .

Manurung, J., Sihombing, A. P. E., & Pandiangan, B. (2023). Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat. *Jurnal Pengabdian Masyarakat Nauli*, *2*(1), 1–7. Https://Www.Ejournal.Marqchainstitute.Or.Id/Index.Php/Nauli/Article/Download/103/92

Simanullang, M. J., Setiawan Aritonang, A., & Sinaga, F. M. (2026). Analisis Keamanan Data Pasien Pada Sistem Informasi Manajemen Rumah Sakit (Simrs). *Jurnal Desain Dan Analisis Teknologi (Jddat)*, *5*(1), 44–50. Http://Journal.Aptikomkepri.Org/Index.Php/Jddat44jurnaldesaindananalisisteknologi

Snyder, H. (2019). Literature Review As A Research Methodology: An Overview And Guidelines. *Journal Of Business Research*, *104*, 333–339. Https://Doi.Org/10.1016/J.Jbusres.2019.07.039

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. Https://Doi.Org/10.38043/Jah.V6i1.4484

Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022. (2022). Perlindungan Data Pribadi. Pemerintah Republik Indonesia.

Utami, M., & Rizal, M. (2026). Factors That Influence The Value Of Regional Government Financial Reporting Information In North Sumatra Province. *International Journal of Islamic, Economic and Finance (IJIEF)*, *3*(1), 40-56.