JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2288-2292

Analisis Kebocoran Data ASN oleh TopiAx: Etika, Keamanan Siber, dan Perlindungan Data Pribadi

Della Putri Destyana[1], Farand Arja Kurniawan[2*], Tinesya Nur Azmiani[3], Violanda Junita Putri[4], Annisa Elfina Augustia[5]

[1-5]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1]dellaputridestyana3@gmail.com, [2*]farandarja50@gmail.com, [3]tinesyanur.azmiani24@gmail.com, [4]violandajntp@gmail.com, [5]annisa12elfina@gmail.com
(* : coressponding author)

Abstrak−Kasus kebocoran data Aparatur Sipil Negara (ASN) oleh kelompok peretas TopiAx pada tahun 2024 menimbulkan perhatian serius terhadap lemahnya sistem keamanan siber instansi pemerintah di Indonesia. Penelitian ini bertujuan untuk menganalisis aspek teknis dan etika dalam pengelolaan data publik, serta mengevaluasi sejauh mana penerapan prinsip keamanan informasi dan kepatuhan terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Metode penelitian yang digunakan adalah studi kasus deskriptif dengan pendekatan kualitatif, yang memanfaatkan data sekunder dari laporan BKN, publikasi media, serta kajian akademik terkait keamanan siber nasional. Hasil analisis menunjukkan bahwa kebocoran tersebut terjadi akibat kelemahan pada manajemen akses data dan rendahnya implementasi prinsip *privacy by design*. Selain itu, terdapat pelanggaran etika profesi teknologi informasi, khususnya dalam hal tanggung jawab pengelolaan dan perlindungan data publik. Penelitian ini menegaskan pentingnya tata kelola keamanan siber yang berkelanjutan, peningkatan kesadaran etis, serta pembentukan sistem perlindungan data terpadu antarinstansi. Temuan ini diharapkan dapat menjadi dasar evaluasi kebijakan keamanan informasi dan penguatan etika profesi di lingkungan pemerintahan Indonesia.

Kata Kunci: kebocoran data, ASN, keamanan siber, etika profesi IT, UU PDP

Abstract−*The data breach of Indonesia's Civil Servants (ASN) by the hacker group TopiAx in 2024 raised serious concerns about the vulnerability of government cybersecurity systems. This study aims to analyze both the technical and ethical aspects of public data management and to evaluate the implementation of information security principles in accordance with Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). The research employs a descriptive case study with a qualitative approach, utilizing secondary data from official BKN reports, media publications, and academic sources related to national cybersecurity. The findings indicate that the breach occurred due to weak access management and insufficient application of the* privacy by design *principle. Furthermore, the incident highlights ethical violations within the information technology profession, particularly in accountability and data protection responsibilities. This study emphasizes the need for sustainable cybersecurity governance, enhanced ethical awareness, and integrated data protection systems among government institutions. The results are expected to provide a reference for future policy evaluation and the reinforcement of professional ethics in Indonesia's public sector.*

Keywords: *data breach, civil servant, cybersecurity, IT ethics, PDP Law*

1. PENDAHULUAN

Kemajuan teknologi saat ini tidak bisa dipisahkan dari kehidupan masyarakat. Berbagai informasi yang terjadi di berbagai belahan dunia kini telah dapat langsung kita ketahui berkat kemajuan teknologi. Pada dasarnya teknologi diciptakan untuk memudahkan pekerjaan manusia. Saat ini teknologi sudah menjadi kebutuhan primer manusia. Bahkan teknologi sudah digunakan di semua segi kehidupan manusia (Hidayat *et al*., 2023) salah satunya di berbagai instansi pemerintahan. Namun, kemajuan ini juga diiringi dengan meningkatnya ancaman terhadap keamanan data dan pelanggaran etika profesi di bidang teknologi informasi. Salah satu kasus yang menyoroti isu ini adalah dugaan kebocoran data 4.759.218 milik Aparatur Sipil Negara (ASN) dari Satu Data ASN yang dikelola Badan Kepegawaian Negara (BKN) oleh kelompok peretas TopiAx pada tahun 2024 (Darmawan, 2024) yang mengungkap kerentanan sistem keamanan siber di Badan Kepegawaian Negara (BKN) dan menimbulkan kekhawatiran publik terkait perlindungan data pribadi pegawai negeri. Dalam kondisi kebocoran data, terdapat data dan/atau informasi yang dilihat, diakses dan disebarluaskan tanpa seizin pemilik data. Ditinjau dari subjek atau pelakunya, keboran data tidak selalu terjadi karena serangan peretas. Ancaman ini juga bisa terjadi karena ketidaksengajaan atau kelalaian pihak internal yang memiliki akses terhadap data (*insider*) (Sukmawan & Setyawan, 2023).

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2288-2292

Kebocoran tersebut memperlihatkan lemahnya manajemen keamanan informasi, terutama dalam hal pengendalian akses data, enkripsi, serta audit sistem secara berkala. Selain itu, dari sisi etika profesi teknologi informasi, kasus ini menunjukkan kurangnya tanggung jawab dalam memastikan keamanan dan privasi data publik yang dikelola oleh instansi pemerintah. Padahal, menurut Kode Etik Profesi IT dan prinsip *Information Security Governance*, pengelolaan data publik harus menjunjung tinggi integritas, kerahasiaan, dan akuntabilitas.

Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP**)** diharapkan menjadi landasan hukum yang kuat dalam menegakkan tanggung jawab etis dan teknis terhadap data pribadi warga negara. Namun, lemahnya implementasi dan koordinasi antarinstansi membuat perlindungan tersebut belum berjalan optimal.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis aspek keamanan siber, etika profesi IT, serta penerapan UU PDP dalam konteks kebocoran data ASN oleh TopiAx. Hasil penelitian diharapkan dapat memberikan kontribusi dalam penguatan tata kelola keamanan informasi di sektor publik dan peningkatan kesadaran etika profesi teknologi informasi di Indonesia.

2. METODE PENELITIAN

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode studi kasus dengan pendekatan kualitatif deskriptif**.** Pendekatan ini dipilih karena dianggap paling sesuai untuk menganalisis secara mendalam fenomena kebocoran data Aparatur Sipil Negara (ASN) oleh kelompok peretas TopiAx yang terjadi pada tahun 2024. Pendekatan kualitatif digunakan untuk menggali pemahaman mendalam mengenai aspek teknis keamanan siber serta dimensi etika profesi teknologi informasi yang terlibat dalam kasus ini

2.2 Sumber dan Teknik Pengumpulan Data

Data yang digunakan dalam penelitian ini merupakan data sekunder yang dikumpulkan melalui studi literatur. Sumber data meliputi laporan resmi dari Badan Kepegawaian Negara (BKN), publikasi dari Kementerian Komunikasi dan Informatika (Kominfo), pemberitaan dari media nasional, serta hasil penelitian akademik terdahulu yang relevan dengan isu keamanan data publik dan perlindungan data pribadi. Pengumpulan data dilakukan dengan cara menelusuri dokumen, artikel, dan laporan yang kredibel untuk mendapatkan informasi yang akurat dan mendukung analisis.

2.3 Teknik Analisis Data

Analisis data dilakukan melalui beberapa tahapan. Pertama, dilakukan identifikasi dan klasifikasi data untuk memetakan informasi berdasarkan aspek teknis, etika, dan hukum. Kedua, dilakukan analisis deskriptif guna memahami penyebab, pola serangan, serta dampak yang ditimbulkan oleh kebocoran data terhadap instansi pemerintah dan masyarakat. Ketiga, dilakukan evaluasi normatif dengan menilai sejauh mana praktik pengelolaan data yang dilakukan oleh instansi terkait telah sesuai dengan prinsip *Information Security Governance* dan ketentuan yang terdapat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

2.4 Validitas dan Keabsahan Data

Untuk memastikan keakuratan dan objektivitas hasil penelitian, dilakukan triangulasi sumber, yaitu dengan membandingkan dan memverifikasi data yang diperoleh dari berbagai sumber berbeda seperti dokumen resmi, pemberitaan media, dan publikasi akademik. Teknik ini digunakan agar analisis yang dihasilkan tidak bersifat bias dan tetap valid secara akademis. Dengan metode ini, penelitian diharapkan mampu memberikan gambaran yang komprehensif mengenai kelemahan tata kelola keamanan data ASN, serta mengidentifikasi bentuk pelanggaran etika profesi teknologi informasi dalam kasus kebocoran data oleh kelompok TopiAx.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2288-2292

3. ANALISA DAN PEMBAHASAN

3.1 Analisis Teknis Kebocoran Data ASN oleh TopiAX

Kasus kebocoran data Aparatur Sipil Negara (ASN) yang diduga dilakukan oleh kelompok peretas TopiAx pada 10 Agustus 2024 menjadi salah satu insiden siber terbesar di sektor pemerintahan Indonesia (Dani Aswara, 2024). Berdasarkan laporan yang beredar di berbagai media dan hasil analisis komunitas keamanan digital, kebocoran ini melibatkan jutaan data pegawai ASN yang mencakup identitas pribadi, nomor induk pegawai, serta riwayat kepegawaian. Dari sisi teknis, serangan ini diduga memanfaatkan celah keamanan pada sistem manajemen data milik Badan Kepegawaian Negara (BKN) yang belum menerapkan prinsip *zero trust architecture* dan belum mengadopsi sistem enkripsi yang kuat dalam proses penyimpanan data.

Selain itu, lemahnya pengawasan terhadap akses pengguna internal serta kurangnya pembaruan sistem keamanan menyebabkan peretas dapat mengeksploitasi celah autentikasi dan melakukan pengambilan data secara masif. Faktor lain yang turut memperparah kondisi ini adalah rendahnya penerapan kebijakan keamanan informasi yang berkelanjutan dan belum adanya audit keamanan siber yang dilakukan secara rutin. Hal ini memperlihatkan bahwa aspek tata kelola keamanan informasi di instansi pemerintah masih belum optimal, khususnya dalam memastikan integritas, ketersediaan, dan kerahasiaan data publik.

3.2 Analisis Etika Profesi Teknologi Informasi

Dari perspektif etika profesi, kasus kebocoran data ASN ini menunjukkan adanya pelanggaran terhadap prinsip dasar etika teknologi informasi, yaitu tanggung jawab, kejujuran, dan keadilan dalam mengelola serta melindungi data publik. Para profesional di bidang IT yang terlibat dalam pengelolaan sistem BKN seharusnya memiliki kewajiban moral dan profesional untuk menjaga kerahasiaan data dan mencegah akses tidak sah. Namun, lemahnya kesadaran etis dan kurangnya pengawasan internal menjadi faktor yang memperbesar risiko pelanggaran etika tersebut.

Menurut *Kode Etik Profesi IT Indonesia* (APTIKOM, 2010), setiap praktisi teknologi informasi harus menjamin keamanan dan privasi pengguna sistem. Dalam kasus ini, kegagalan untuk menerapkan prinsip *confidentiality* dan *accountability* mengindikasikan pelanggaran terhadap etika profesional. Selain itu, tindakan peretasan yang dilakukan oleh kelompok TopiAx juga termasuk pelanggaran etika berat dalam ranah siber, karena menyerang sistem pemerintah yang berisi data publik sensitif. Dengan demikian, kasus ini memperlihatkan dua sisi pelanggaran etika sekaligus: kelalaian dari pihak pengelola sistem, dan tindakan tidak etis dari pihak peretas.

3.3 Evaluasi terhadap Penerapan UU Perlindungan Data Pribadi

Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi2. Setiap orang berhak atas perlindungan data pribadinya. UU PDP mewajibkan setiap penyelenggara sistem elektronik, termasuk lembaga pemerintah, untuk memastikan kerahasiaan, keutuhan, dan ketersediaan data pribadi yang dikelolanya (Nurcahyani & Wiraguna, 2025). Namun, implementasinya pada saat kasus kebocoran data ASN terjadi masih belum optimal. BKN sebagai pengelola data publik seharusnya telah menyesuaikan kebijakan internalnya dengan standar perlindungan data pribadi, termasuk penunjukan pejabat perlindungan data (*Data Protection Officer*), mekanisme pelaporan insiden, serta prosedur mitigasi risiko kebocoran.

Analisis menunjukkan bahwa belum adanya mekanisme respons insiden yang terintegrasi menyebabkan keterlambatan dalam mendeteksi dan menanggapi kebocoran. Selain itu, koordinasi antarinstansi seperti BKN, Kominfo, dan Badan Siber dan Sandi Negara (BSSN) juga masih lemah, sehingga proses penanganan insiden menjadi tidak efisien. Dari sudut pandang hukum, hal ini menunjukkan bahwa penerapan UU PDP masih bersifat formal dan belum sepenuhnya dijalankan secara operasional di sektor publik.

3.4 Implikasi Terhadap Tata Kelola Keamanan Siber Pemerintah

Kasus ini menjadi pembelajaran penting bagi instansi pemerintah bahwa keamanan siber tidak hanya bersifat teknis, tetapi juga mencakup dimensi etika dan hukum. Diperlukan integrasi antara kebijakan keamanan informasi, peningkatan kompetensi sumber daya manusia, serta penegakan etika profesi di lingkungan pengelolaan data publik. Pemerintah perlu mengadopsi

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2288-2292

kerangka kerja seperti *ISO/IEC 27001 Information Security Management System (ISMS)* sebagai standar pengelolaan keamanan data yang berkelanjutan. Selain itu, peningkatan budaya keamanan digital dan kesadaran etika perlu dijadikan prioritas agar kebocoran serupa tidak kembali terjadi di masa mendatang.

4. KESIMPULAN

Kasus dugaan kebocoran data Aparatur Sipil Negara (ASN) oleh kelompok peretas TopiAx menunjukkan bahwa tata kelola keamanan siber di lingkungan pemerintahan Indonesia masih menghadapi berbagai kelemahan mendasar, baik dari sisi teknis, etika, maupun regulasi. Dari aspek teknis, kebocoran ini disebabkan oleh lemahnya pengamanan sistem, rendahnya penerapan prinsip *zero trust*, serta kurangnya pembaruan dan audit keamanan informasi secara berkala. Faktor-faktor tersebut memperlihatkan bahwa sistem pengelolaan data publik belum sepenuhnya menerapkan prinsip integritas, kerahasiaan, dan ketersediaan informasi yang seharusnya menjadi dasar dalam setiap pengelolaan data digital.

Dari perspektif etika profesi teknologi informasi, kasus ini menggambarkan kegagalan dalam menegakkan tanggung jawab moral dan profesionalitas dalam melindungi data publik. Praktisi teknologi informasi di lembaga pemerintahan seharusnya memegang prinsip kejujuran, tanggung jawab, dan keadilan dalam setiap tindakan pengelolaan sistem informasi. Pelanggaran etika tidak hanya dilakukan oleh pihak peretas, tetapi juga dapat terjadi akibat kelalaian pengelola sistem dalam menjaga privasi dan keamanan data publik. Hal ini menegaskan pentingnya penguatan kesadaran etika digital di lingkungan kerja, khususnya pada sektor pemerintahan.

Sementara itu, dari sisi hukum dan kebijakan, implementasi Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) masih belum berjalan efektif. Ketiadaan mekanisme tanggap insiden yang terstruktur, kurangnya koordinasi antar lembaga seperti BSSN dan Kominfo, serta belum adanya *Data Protection Officer* di instansi publik menjadi bukti bahwa penerapan UU PDP masih berada pada tahap awal dan belum menyentuh aspek operasional.

Secara keseluruhan, studi ini menegaskan bahwa upaya memperkuat keamanan siber nasional tidak dapat hanya bergantung pada perangkat teknologi, tetapi harus dibarengi dengan tata kelola yang baik, penegakan etika profesi, serta penerapan regulasi yang konsisten. Pemerintah perlu meningkatkan kapasitas sumber daya manusia di bidang keamanan digital, memperkuat koordinasi antarinstansi, serta membangun budaya kesadaran keamanan data di seluruh sektor publik. Dengan demikian, kebocoran data serupa dapat diminimalkan di masa depan, dan kepercayaan publik terhadap sistem pemerintahan digital dapat kembali terjaga.

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penelitian dan penulisan jurnal ini dapat diselesaikan dengan baik. Penulis juga menyampaikan terima kasih yang sebesar-besarnya kepada dosen pembimbing, rekan-rekan sejawat yang telah memberikan bimbingan, dukungan, serta masukan berharga selama proses penelitian ini berlangsung.

Ucapan terima kasih juga penulis tujukan kepada para peneliti, yang karya ilmiahnya menjadi rujukan penting dalam penyusunan jurnal ini. Tidak lupa, penulis berterima kasih kepada keluarga dan teman-teman yang senantiasa memberikan dukungan moral dan semangat.

Penulis berharap hasil penelitian ini dapat memberikan kontribusi nyata bagi pengembangan ilmu pengetahuan di bidang teknologi informasi, khususnya dalam aspek keamanan siber dan etika pengelolaan data publik di Indonesia.

REFERENCES

Aswara, D. (2024). Kaleidoskop 2024: 6 Serangan Siber Besar di Indonesia. https://www.tempo.co/hukum/kaleidoskop-2024-6-serangan-siber-besar-di-indonesia-1188275

Darmawan. (2024). Geger Data 4,7 Juta ASN Bocor dan Dijual Rp 159 Juta. https://wantimpres.go.id/id/newsflows/geger-data-47-juta-asn-bocor-dan-dijual-rp-159-juta/

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2288-2292

Hidayat M, W., Musdira, N., Rasyid, N., Khairi S, S., (2023). Analisis Ancaman Terhadap Keamanan Data Pribadi pada Email. *Jurnal Pendidikan Terapan, 1*(2), 7-12. DOI:10.61255/jupiter.v1i2.73

Nurcahyani, R. E. K., & Wiraguna, S. A. (2025). Tanggung Jawab Hukum Pelindungan Data ASN dalam Sistem Pemerintahan Berbasis Elektronik di Indonesia. *Jurnal Kajian Hukum Dan Kebijakan Publik, 2*(2), 1115-1120. DOI: https://doi.org/10.62379/wxf6a077

Sukmawan, D. I., & Setyawan, D. P. (2023). Hacker, Fear, and Harm: Data Breaches and National Security . *Global Strategis, 17*(1), 153–182. https://doi.org/10.20473/jgs.17.1.2023.153-182.