TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 272-277

Evaluasi Pembelajaran dari Kasus Kebocoran Data di Indonesia sebagai Negara dengan Data Breach Terbesar Ke-8 Dunia

Fariz Fadliansyah[1*], Muhammad Khusni Mubarok[2], Muhammad Dafa Aziz[3], Annisa Elfina Augustia[4]

[1-4]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1*]farizfadliansyah@gmail.com, [2]muhammadkhusni26@gmail.com, [3]mdaffaaziz497@gmail.com, [4]annisa12elfina@gmail.com
(* : coressponding author)

Abstrak−Indonesia menempati peringkat kedelapan dunia dalam jumlah kasus kebocoran data, mencerminkan kerentanan sistemik dalam tata kelola keamanan siber nasional. Penelitian ini bertujuan mengevaluasi pembelajaran dari insiden kebocoran data nyata untuk merumuskan solusi berbasis bukti. Melalui pendekatan kualitatif, dengan analisis dokumen, studi kasus, dan tinjauan literatur, penelitian mengidentifikasi akar permasalahan yang meliputi keterlambatan peraturan pelaksana Undang-Undang Perlindungan Data Pribadi, dominasi *human error* dalam insiden siber, serta infrastruktur teknis yang rentan akibat sentralisasi data tanpa proteksi berlapis. Evaluasi pasca-insiden menunjukkan minimnya transparansi, investigasi independen, dan mekanisme formal untuk mendokumentasikan pelajaran yang dapat ditindaklanjuti. Solusi yang diusulkan mencakup percepatan regulasi pelaksana, integrasi prinsip *privacy by design* dalam Sistem Pemerintahan Berbasis Elektronik, penguatan peran Badan Pengawas Perlindungan Data Pribadi, serta edukasi berbasis risiko nyata. Penelitian ini menekankan bahwa transformasi keamanan siber harus berakar pada pembelajaran kolektif agar setiap kebocoran data menjadi momentum membangun ekosistem digital yang tangguh dan terpercaya.

Kata Kunci: Kebocoran Data; Evaluasi Pembelajaran; UU Perlindungan Data Pribadi; *Human Error*; Keamanan Siber

Abstract−*Indonesia ranks eighth globally in data breach incidents, revealing systemic vulnerabilities in its national cybersecurity governance. This study evaluates lessons drawn from real data breach cases to formulate evidence-based solutions. Using a qualitative approach, document analysis, case studies, and literature review, the research identifies root causes including delays in implementing regulations for the Personal Data Protection Law, the prevalence of human error in cyber incidents, and vulnerable technical infrastructure due to centralized data management without layered protection. Post-breach evaluation reveals a lack of transparency, independent investigation, and formal mechanisms to document actionable lessons. Proposed solutions include accelerating implementing regulations, integrating privacy by design into Indonesia's Electronic-Based Government System, strengthening the Personal Data Protection Authority, and risk-based public education. The study emphasizes that cybersecurity transformation must be rooted in collective learning so that every data breach becomes an opportunity to build a resilient and trustworthy digital ecosystem.*

Keywords: *Data Breach; Learning Evaluation; Personal Data Protection Law; Human Error; Cybersecurity*

1. PENDAHULUAN

Transformasi digital telah menjadi pilar utama pembangunan nasional Indonesia, terutama melalui percepatan Sistem Pemerintahan Berbasis Elektronik (SPBE). Namun, integrasi teknologi dalam layanan publik juga membuka kerentanan terhadap ancaman keamanan siber. Badan Siber dan Sandi Negara (BSSN) mencatat 370,02 juta serangan siber pada 2022, meningkat 38,72% dari tahun sebelumnya (Alfi et al., 2023). Lebih mengkhawatirkan lagi, Indonesia menempati peringkat ke-8 dunia dalam jumlah kasus kebocoran data, dengan insiden besar seperti kebocoran 279 juta data BPJS Kesehatan dan 15 juta data nasabah Bank Syariah Indonesia yang mengungkap rapuhnya infrastruktur keamanan data nasional.

Kebocoran data tidak hanya menimbulkan kerugian finansial, tetapi juga mengikis kepercayaan publik dan mengancam hak privasi sebagai bagian dari *human security* (Prabowo et al., 2020). Sebagai respons, pemerintah mengesahkan Undang-Undang Perlindungan Data Pribadi

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 272-277

(PDP) No. 27 Tahun 2022, yang menjadi landasan hukum komprehensif pertama di bidang ini. Namun, implementasinya terhambat oleh keterlambatan peraturan pelaksana, kurangnya kapasitas SDM, dan rendahnya kesadaran keamanan siber.

Penelitian ini menawarkan solusi yang berakar pada refleksi kritis terhadap insiden kebocoran data yang terjadi di Indonesia, dengan tujuan mengubah krisis menjadi momentum transformasi kebijakan dan praktik keamanan siber. Solusi tersebut dirancang melalui pendekatan holistik yang mengintegrasikan penguatan regulasi, peningkatan kapasitas institusional, edukasi berbasis konteks riil, serta penguatan tata kelola data yang berorientasi pada perlindungan hak warga negara. Dengan memadukan pembelajaran dari kegagalan sistemik, mulai dari kerentanan teknis, faktor manusia, hingga kelemahan koordinasi kebijakan, penelitian ini bertujuan merumuskan rekomendasi yang tidak hanya responsif terhadap ancaman saat ini, tetapi juga proaktif dalam membangun ekosistem digital yang tangguh, transparan, dan berkelanjutan. Pendekatan ini diharapkan mampu memperkuat ketahanan digital nasional di tengah dinamika Revolusi Industri 4.0 yang terus berakselerasi.

2. METODE PENELITIAN

2.1 Pendekatan dan Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan desain studi kasus ganda (*multiple case study*) dan analisis kebijakan komparatif. Pendekatan ini dipilih karena memungkinkan peneliti untuk memahami secara mendalam akar permasalahan, konteks sosio-politik, serta dinamika implementasi kebijakan terkait kebocoran data di Indonesia. Metode ini selaras dengan prinsip *learning-based evaluation* yang menekankan refleksi kritis atas insiden nyata untuk merumuskan rekomendasi kebijakan berbasis bukti (Prasetyo et al., 2025).
Desain penelitian menggabungkan tiga komponen utama:

a. Analisis kasus nyata terhadap lima insiden kebocoran data besar di Indonesia (2020–2024).
b. Studi dokumen kebijakan terhadap UU Perlindungan Data Pribadi (PDP), UU ITE, dan regulasi turunannya.
c. Analisis framing media terhadap pemberitaan di portal berita nasional.

2.2 Teknik Pengumpulan Data

Penelitian ini mengandalkan data sekunder yang dikumpulkan secara sistematis dari dokumen hukum, laporan resmi, studi akademik, dan pemberitaan media. Sumber hukum meliputi UU Perlindungan Data Pribadi No. 27 Tahun 2022, UU ITE No. 11/2008 sebagaimana diubah oleh UU No. 19/2016, serta Permen Kominfo No. 20 Tahun 2016. Laporan dari Badan Siber dan Sandi Negara (BSSN) dan Kementerian Kominfo menyediakan data serangan siber serta temuan investigasi kasus kebocoran data, seperti BPJS Kesehatan, Bank Syariah Indonesia, Pusat Data Nasional, dan sistem ASN. Studi akademik nasional dan internasional digunakan untuk memperkaya analisis teoretis terkait *human error*, kesadaran keamanan informasi, dampak terhadap kepercayaan publik, dan pendekatan *human security*. Sementara itu, pemberitaan dari media seperti *Kompas.com*, *Tempo.co*, dan *CNN Indonesia* dianalisis untuk memahami narasi publik dan framing sosial atas insiden kebocoran data. Kombinasi sumber ini memungkinkan penelitian mengevaluasi kesenjangan antara regulasi, implementasi, dan dinamika ancaman siber kontemporer secara holistik dan multidisipliner.

2.3 Teknik Analisis Data

Teknik analisis data dalam penelitian ini menggunakan pendekatan tematik dan komparatif untuk mengungkap akar permasalahan, pola, dan dinamika kebijakan dalam kasus kebocoran data di Indonesia. Data dikelompokkan ke dalam kategori kunci, seperti kerentanan teknis, faktor manusia, kelemahan regulasi, respons institusional, dan dampak terhadap kepercayaan publik, lalu dikaji melalui kerangka perlindungan data pribadi, keamanan siber, dan perspektif *human security*. Validitas temuan dipastikan melalui triangulasi antara dokumen kebijakan, laporan insiden, studi akademik, dan pemberitaan media. Analisis juga membandingkan implementasi UU Perlindungan Data Pribadi dengan standar internasional seperti *GDPR* dan *NIST Cybersecurity Framework* guna

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 272-277

mengidentifikasi kesenjangan antara norma dan praktik. Temuan diperkaya dengan evaluasi *post-breach learning* untuk merumuskan rekomendasi yang proaktif, berkelanjutan, dan berbasis pembelajaran dari insiden nyata.

2.4 Validitas dan Etika Penelitian

Validitas data dijamin melalui triangulasi sumber, triangulasi metode, dan audit trail. Penelitian ini tidak melibatkan responden manusia secara langsung, sehingga tidak memerlukan persetujuan etik institusional. Namun, seluruh data yang digunakan bersifat publik dan dianalisis dengan menjunjung prinsip objektivitas, akuntabilitas, serta penghormatan terhadap privasi pihak-pihak yang terdampak.

3. ANALISA DAN PEMBAHASAN

3.1 Karakteristik dan Pola Kebocoran Data di Indonesia

Kebocoran data di Indonesia menunjukkan pola yang sistematis dan berulang, dengan ciri khas dominasi serangan ransomware, peretasan database pemerintah, dan penjualan data di forum gelap (*dark web*). Berdasarkan data dari Kementerian Komunikasi dan Informatika (2024) dan laporan BSSN (2022–2024), terdapat 124 kasus dugaan pelanggaran perlindungan data pribadi sejak 2019 hingga pertengahan 2024, dengan 111 di antaranya merupakan kebocoran data skala besar (Utami et al., 2025).

Tabel 1. Kasus Kebocoran Data Skala Nasional di Indonesia (2020–2024)

Tahun	Insiden	Jumlah Data	Jenis Ancaman	Sektor
2020	Tokopedia	91 juta	Peretasan & penjualan di dark web	E-commerce
2021	BPJS Kesehatan	279 juta	Eksploitasi API & kebocoran database	Kesehatan
2022	Bjorka (KPU)	105 juta	Peretasan & publikasi data pejabat	Pemerintahan
2023	Bank Syariah Indonesia	15 juta	Ransomware Lockbit 3.0	Keuangan
2024	Pusat Data Nasional (PDN)	5,8 juta	Ransomware & gangguan layanan publik	Infrastruktur Digital

Dari tabel tersebut, terlihat bahwa sektor pemerintahan menjadi target utama, dengan tiga dari lima insiden melibatkan data sensitif warga negara yang dikelola oleh instansi negara. Hal ini mengindikasikan kerentanan struktural dalam tata kelola data publik, terutama dalam hal sentralisasi data tanpa proteksi berlapis dan *backup* yang memadai.

3.2 Faktor Penyebab Kebocoran Data

3.2.1 Human Error sebagai Faktor Dominan

Data global menunjukkan bahwa human error merupakan faktor dominan dalam insiden keamanan siber, dengan kontribusi berkisar antara 24% hingga 95%, tergantung pada konteks organisasi dan sektor (Amoresano & Yankson, 2023). Meskipun tingkat pengetahuan keamanan

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 272-277

informasi di kalangan pegawai BMKG mencapai 88,06%, perilaku nyata hanya mencapai 80,74%, dengan skor terendah pada penggunaan perangkat mobile (73,19%) dan email (78,70%).

Untuk mengukur kesenjangan antara pengetahuan dan perilaku, penelitian ini mengadopsi model Knowledge–Attitude–Behavior (KAB) yang dirumuskan sebagai:

$$ISA\ Score = \frac{1}{3}$$

di mana:

K = skor pengetahuan (0–100%),

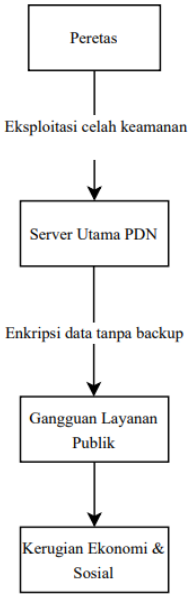
A = skor sikap (0–100%),

B = skor perilaku (0–100%).

Skor ISA rata-rata pegawai pemerintah adalah 83,56% (kategori tinggi). Namun, perilaku spesifik seperti penggunaan kata sandi lemah ("Admin#1234") dan keengganan mengaktifkan autentikasi dua faktor tetap menjadi celah utama.

3.2.2 Kerentanan Teknis dan Infrastruktur

Infrastruktur keamanan siber pemerintah masih mengandalkan sistem yang ketinggalan zaman (*outdated*), tanpa segmentasi jaringan, dan minim enkripsi end-to-end. Serangan ransomware terhadap PDN pada Juni 2024 berhasil karena tidak adanya sistem *failover* dan *backup* terdistribusi, sehingga ratusan instansi pemerintah lumpuh selama berhari-hari (Bua & Idris, 2025).



Gambar 1. Diagram Serangan Ransomware terhadap PDN (2024)

3.2.3 Keterlambatan Regulasi dan Penegakan Hukum

Meskipun Undang-Undang Perlindungan Data Pribadi (PDP) No. 27 Tahun 2022 telah disahkan, keterlambatan penyusunan peraturan pelaksananya menciptakan ketidakpastian hukum yang menghambat penerapan operasional di lapangan (Mahameru et al., 2023). Hingga 2025, banyak instansi masih belum memenuhi standar teknis minimum seperti enkripsi, audit keamanan berkala, dan pelaporan insiden dalam 72 jam sebagaimana diamanatkan Pasal 45 UU PDP. Ketidaksiapan ini diperparah oleh minimnya panduan teknis, kapasitas SDM, dan koordinasi

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 272-277

antarlembaga, sehingga implementasi UU PDP berisiko hanya menjadi formalitas administratif, bukan transformasi nyata dalam tata kelola keamanan data nasional.

3.3 Dampak Kebocoran Data terhadap Kepercayaan Publik dan Human Security

Kebocoran data tidak hanya berdampak teknis, tetapi juga mengancam "*vital core*" individu, yaitu kelangsungan hidup, mata pencaharian, dan martabat, sebagaimana didefinisikan dalam pendekatan human security (Prabowo et al., 2020). Sebanyak 79,5% responden menyatakan kekhawatiran terhadap keamanan data pribadi pasca-insiden Bjorka, dan 60,3% menilai UU PDP hanya "cukup efektif" dalam mencegah kebocoran. Lebih jauh, kebocoran data berdampak pada penurunan kepatuhan warga negara, termasuk keengganan membayar pajak karena hilangnya kepercayaan terhadap kemampuan negara melindungi data sensitif.

3.4 Evaluasi Pembelajaran Pasca-Insiden

Evaluasi pasca-insiden kebocoran data di Indonesia, seperti kasus BPJS Kesehatan (2021), Bjorka (2022), dan serangan ransomware terhadap Pusat Data Nasional (2024), menunjukkan bahwa respons pemerintah masih bersifat reaktif, bukan reflektif. Minimnya transparansi dalam pelaporan insiden, absennya investigasi yang benar-benar independen, serta tidak adanya mekanisme formal yang sistematis untuk mendokumentasikan dan menyebarkan pelajaran yang dapat diambil dari setiap kebocoran data, menyebabkan kesalahan yang sama terus berulang tanpa perbaikan mendasar. Akibatnya, kesalahan sistemik, seperti penggunaan kata sandi lemah, kurangnya autentikasi dua faktor, dan sentralisasi data tanpa *backup* terus berulang.

Pendekatan yang efektif setelah terjadi kebocoran data seharusnya mencakup serangkaian langkah terstruktur: dimulai dari investigasi yang independen dan mendalam untuk mengungkap akar permasalahan, dilanjutkan dengan penyampaian informasi yang terbuka dan jujur kepada publik mengenai apa yang terjadi, bagaimana dampaknya, serta langkah-langkah yang diambil. Temuan dari proses tersebut harus menjadi dasar bagi perbaikan menyeluruh, baik dalam aspek teknis, prosedural, maupun tata kelola, sehingga celah yang sama tidak terulang. Lebih dari itu, pelajaran yang diperoleh perlu dibagikan secara luas di antara berbagai instansi pemerintah dan pemangku kepentingan terkait, agar insiden serupa dapat dicegah di tempat lain. Tanpa mekanisme semacam ini, kerangka hukum yang telah dibangun, termasuk UU Perlindungan Data Pribadi No. 27 Tahun 2022, berisiko tidak memberikan dampak nyata dalam mengubah praktik pengelolaan data di lapangan. Oleh karena itu, diperlukan komitmen kolektif dan berkelanjutan dari berbagai pihak, termasuk lembaga keamanan siber, regulator, akademisi, dan masyarakat sipil, untuk mengubah setiap insiden kebocoran data bukan hanya sebagai krisis yang harus ditangani, melainkan sebagai momentum kritis untuk memperkuat fondasi ekosistem digital nasional yang aman, transparan, dan berkelanjutan.

4. KESIMPULAN

Kebocoran data di Indonesia, yang menempatkan negara ini sebagai peringkat ke-8 dunia dalam jumlah insiden data breach, merupakan cerminan dari kerentanan sistemik yang melibatkan faktor teknis, manusia, dan regulasi. Meskipun Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022 telah disahkan sebagai landasan hukum, keterlambatan peraturan pelaksana, rendahnya kesadaran keamanan siber, serta lemahnya infrastruktur teknis menghambat implementasi efektifnya. Evaluasi pasca-insiden menunjukkan bahwa respons selama ini masih reaktif, bukan reflektif, sehingga pelajaran dari kasus seperti BPJS Kesehatan, Bjorka, hingga serangan ransomware terhadap Pusat Data Nasional belum sepenuhnya dijadikan dasar perbaikan sistemik. Untuk membangun ketahanan digital nasional yang berkelanjutan, diperlukan pendekatan holistik yang mengintegrasikan penguatan regulasi, peningkatan kapasitas SDM, edukasi berbasis risiko nyata, dan kolaborasi lintas sektor, sehingga setiap kebocoran data tidak hanya menjadi

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 272-277

krisis, tetapi juga momentum transformasi menuju ekosistem digital yang aman, transparan, dan terpercaya.

UCAPAN TERIMA KASIH

Penulis mengucapkan puji dan syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat, hidayah, dan kemudahan yang diberikan sehingga penelitian ini dapat diselesaikan dengan baik. Ucapan terima kasih yang tulus disampaikan kepada Ibu Annisa Elfina Augustia, M.Kom., selaku pembimbing utama, atas bimbingan, arahan, masukan, serta kesabaran yang luar biasa selama proses penyusunan penelitian ini. Ucapan terima kasih juga disampaikan kepada seluruh pihak yang telah memberikan dukungan, masukan, dan semangat selama proses penyusunan penelitian ini, tanpa kontribusi dan kepercayaan dari Bapak/Ibu serta rekan-rekan sekalian, penelitian ini tidak akan mampu mencapai bentuk akhirnya seperti sekarang.

REFERENCES

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 1–11. https://doi.org/10.7454/jkskn.v6i2.10082

Amoresano, K., & Yankson, B. (2023). Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *HOLISTICA – Journal of Business and Public Administration*, *14*(1), 110–132. https://doi.org/10.2478/hjbpa-2023-0007

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

Emily, R., Lucius, D., John, A., & Elly, A. (2025). *Investigating the Effect of Data Breaches on Consumer Trust in Personalization Efforts*. https://www.researchgate.net/publication/388631365

Mahameru, D. E., Nurhalizah, A., Wildan, A., Badjeber, M. H., & Rahmadia, M. H. (2023). Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas di Indonesia. *Jurnal Esensi Hukum*, *5*(2), 115–131. https://journal.upnvj.ac.id/index.php/esensihukum/index

Prabowo, W. H., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. *Padjadjaran Journal of International Relations*, *1*(3), 218–239. https://doi.org/10.24198/padjir.v1i3.26194 Prasetyo, A., Aji, R. F., & Wibowo, W. S. (2025). Assessing Information Security Awareness Among Indonesian Government Employees: A Case Study of the Meteorology, Climatology, and Geophysics Agency. *Journal of Information Systems Engineering and Business Intelligence*, *11*(2), 126–142. https://doi.org/10.20473/jisebi.11.2.126-142

Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait dengan Kebocoran Data. *Jurnal Kewarganegaraan*, *6*(1), 976–982.

Utami, T. K., Suryanto, S. O., Putri, K. A., & Asriani, F. (2025). Personal Data Breach Cases In Indonesia : Perspective Of Personal Data Protection Law. *Journal Customary Law*, *2*(2), 21. https://doi.org/10.47134/jcl.v2i2.3742