



Institutional Dysfunction in Personal Data Protection: A Legal-Political Analysis Based on New Institutional Theory

Rengga Kusuma Putra¹, Yulia Agustin*², Latif Nurul Ihsan³, Zaki Ahmad Dafiqi⁴

¹ *Fakultas Hukum, Universitas Sains dan Teknologi Komputer Semarang, Jawa Tengah, Indonesia*

^{2,3,4} *Fakultas Syari'ah dan Hukum, UIN Sunan Kalijaga, Yogyakarta, Indonesia*

E-mail: yuliaagust2@gmail.com

Article Info	Abstract
Keywords: Personal Data Institutional Dysfunction Institutional Theory Legal Politics Data Breaches	<i>Indonesia is facing a personal data protection crisis, as cases of sensitive information leaks from various public institutions continue to increase. Although Law No. 27 of 2022 on Personal Data Protection has been enacted, recurring incidents, such as the hacking of eHAC, BPJS Kesehatan, PeduliLindungi, and ransomware attacks on the National Data Center, demonstrate a weak implementation at the institutional level. This research aims to identify and analyze the forms of institutional dysfunction in personal data protection in Indonesia. This research uses a qualitative approach with a descriptive-analytical design, relying on data from literature studies, documentation, online media news, and in-depth interviews with informants from government institutions, academics, and digital rights activists. The research findings indicate that there are three primary forms of institutional dysfunction: weak formal structures, a bureaucratic culture that is unresponsive, and limited technical capacity. The absence of independent oversight institutions, overlapping inter-agency authorities, and minimal public accountability exacerbate this situation. These findings are analyzed using the new institutional theory, which emphasizes the importance of internal norms and the logic of appropriateness in institutional behavior. This research contributes to filling the gap in digital law studies in Indonesia by highlighting the role of institutional culture and legal politics in explaining the failure of data protection. In conclusion, adequate personal data protection is not sufficient with formal regulations alone, but requires institutional reforms that address structural and cultural aspects, as well as the establishment of an independent supervisory authority that is adaptive to digital threats.</i>

DOI: <https://doi.org/10.51903/bkktev52>

Submitted: April 2025, Reviewed: May 2025, Accepted: June 2025

*Corresponding Author

I. PENDAHULUAN

Dalam dua dekade terakhir, transformasi digital telah mengubah cara negara, korporasi, dan individu mengelola informasi. Di tengah arus digitalisasi ini, data pribadi menjadi komoditas bernilai tinggi yang rawan disalahgunakan. Indonesia, sebagai salah satu negara dengan penetrasi internet tertinggi di Asia Tenggara (Yonatan, 2023), menghadapi tantangan besar dalam hal perlindungan data pribadi. Sejumlah kasus besar telah mencuat ke publik: kebocoran 279 juta data BPJS (Maharani & Meiliana, 2021),

peretasan sistem PeduliLindungi (Sagita, 2025), eksploitasi data pelanggan MyPertamina (Perdana, 2022), hingga serangan *ransomware* terhadap Pusat Data Nasional Sementara (Dewi, 2024).

Fenomena ini tidak hanya menimbulkan gangguan administratif, tetapi juga berisiko memperparah kerentanan sosial. Data pribadi yang bocor telah dimanfaatkan oleh pihak tak bertanggung jawab untuk kejahatan digital seperti pinjaman online ilegal (Aurellia, 2025), peretasan akun finansial (Kalsum, 2025), hingga pemalsuan identitas untuk judi online dan pencucian uang (Wahyuni, 2023). Dalam beberapa laporan investigatif, data hasil kebocoran bahkan dijual bebas di forum gelap (dark web) dalam bentuk paket lengkap: NIK, nama ibu kandung, nomor telepon, dan rekam medis (MetroTv, 2023). Hal ini menunjukkan bahwa dampak kebocoran data tidak lagi bersifat potensial, melainkan sudah nyata dan sistemik. Di sisi regulasi, pemerintah telah merespons dengan disahkannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Namun hingga pertengahan 2025, pelaksanaan UU ini belum menunjukkan efektivitas nyata (Hukom et al., 2025). Literatur sebelumnya telah banyak menyoroti pentingnya perlindungan data pribadi dalam konteks keamanan siber dan hak asasi manusia. Namun sebagian besar studi tersebut berfokus pada aspek teknis seperti enkripsi, keamanan sistem, atau kebijakan perusahaan teknologi (Kossay et al., 2025).

Penelitian hukum di Indonesia pun masih dominan pada pembahasan normatif peraturan dan belum banyak yang mengkaji praktik kelembagaan dalam pelaksanaan perlindungan data, misalnya kajian (Nurchayani & Wiraguna, 2025) yang membahas tanggung jawab hukum perlindungan data ASN dalam SPBE, (Kennedy, 2025) yang mengulas perkembangan hukum telematika secara umum, serta (Mahameru et al., 2023) yang menyoroti lemahnya koordinasi antar lembaga tetapi belum mengurai akar permasalahan secara sistematis. Padahal, seperti dijelaskan dalam teori institusional baru oleh March dan Olsen (1984), keberhasilan kebijakan publik tidak hanya ditentukan oleh isi regulasi, tetapi juga oleh nilai, norma, dan struktur kelembagaan yang mengimplementasikannya (Arda et al., 2025). Penelitian internasional menegaskan bahwa perlindungan data efektif memerlukan otoritas pengawas independen, pelaporan insiden yang cepat, dan prinsip pencegahan sejak desain sistem. Ringkasannya disajikan pada Tabel 1.

Tabel 1. Perbandingan Model Kelembagaan Perlindungan Data Internasional

Negara	Lembaga Pengawas	Karakteristik Utama	Rujukan
Singapura	PDPC (Personal Data Protection Commission)	Otoritas independen, respons cepat, menjadi model tata kelola data di Asia Tenggara	(Chan et al., 2024)
Jerman	BfDI (Federal Commissioner for Data Protection)	<i>Privacy by design</i> , audit regular GDPR	(Custers et al., 2018); (Ramiro, 2025).
Filipina	NPC (National Privacy Commission)	Pelaporan insiden 72 jam, partisipasi masyarakat sipil	(Datu et al., 2024);(Khan, 2025)

Dengan demikian, terdapat gap penelitian dalam melihat disfungsi kelembagaan secara kritis dan sistematis dalam konteks politik hukum perlindungan data pribadi di Indonesia. Penelitian ini mengisi kekosongan tersebut dengan menganalisis kegagalan kelembagaan melalui kerangka teori institusional

baru, yang melihat bahwa perilaku institusi tidak hanya ditentukan oleh aturan formal, tetapi juga oleh norma, nilai, dan logika kepantasan yang berlaku di dalamnya (Coates et al., 2023). Penelitian ini juga membandingkan kondisi tersebut dengan praktik global yang lebih mapan. Berdasarkan latar belakang tersebut, penelitian ini menjawab pertanyaan utama: Bagaimana bentuk disfungsi kelembagaan dalam perlindungan data pribadi di Indonesia dan bagaimana teori institusional baru dapat menjelaskan kegagalan tersebut? Apa perbandingannya dengan model kelembagaan di negara-negara lain yang telah menerapkan prinsip tata kelola data yang baik?

Tujuan dari penelitian ini adalah untuk mengkaji secara mendalam bentuk-bentuk disfungsi kelembagaan dalam perlindungan data pribadi di Indonesia, serta menganalisis praktik kelembagaan tersebut melalui pendekatan teori institusional baru. Penelitian ini juga bertujuan menyusun pemetaan respons institusional terhadap kebocoran data dan mengevaluasi kesiapan tata kelola kelembagaan dalam melaksanakan UU PDP. Kebaruan dari penelitian ini terletak pada pendekatan teoritik dan empiris yang digunakan untuk menilai kelembagaan hukum dalam perlindungan data, serta integrasi analisis politik hukum dengan kerangka institusional baru yang belum banyak digunakan dalam konteks Indonesia. Secara teoritis, penelitian ini memperkaya diskursus hukum dan kebijakan digital dengan pendekatan kelembagaan yang lebih mendalam. Secara praktis, penelitian ini memberikan kontribusi bagi penguatan tata kelola perlindungan data melalui desain kelembagaan yang responsif, akuntabel, dan sesuai dengan tantangan era digital.

II. METODOLOGI

A. Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan desain deskriptif-analitis untuk mengkaji disfungsi kelembagaan dalam perlindungan data pribadi di Indonesia. Fokus utama penelitian ini adalah menelusuri bagaimana kelembagaan negara seperti Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), dan lembaga pengatur lainnya berperan, atau justru gagal berperan, dalam mengimplementasikan Undang-Undang Perlindungan Data Pribadi (UU PDP). Penelitian ini bersifat normatif-empiris, yakni menggabungkan analisis terhadap norma hukum dengan realitas kelembagaan di lapangan. Pendekatan ini dipilih karena memungkinkan analisis yang lebih mendalam terhadap proses institusional yang tidak selalu tercermin secara eksplisit dalam teks regulasi.

Data dikumpulkan melalui studi pustaka atas peraturan perundang-undangan, dokumen kelembagaan, laporan media, serta sumber-sumber ilmiah yang relevan. Selain itu, wawancara mendalam dilakukan terhadap ±12 informan kunci yang dipilih berdasarkan keterlibatan langsung mereka dalam isu perlindungan data. Analisis data dilakukan dengan pendekatan teori institusional baru yang dikemukakan oleh James G. March dan Johan P. Olsen (Lhotta, 2024), yang menekankan bahwa perilaku lembaga tidak hanya dibentuk oleh aturan formal, tetapi juga oleh norma, nilai, dan logika kepantasan yang hidup di dalam institusi tersebut (Alam & Miah, 2024). Dengan kerangka ini, penelitian bertujuan untuk mengungkap akar struktural dari lemahnya perlindungan data pribadi, serta mengkaji

keterkaitan antara struktur kelembagaan, politik hukum, dan kegagalan implementasi regulasi di era digital.

B. Populasi dan Sampel

Populasi teoritis dalam penelitian ini mencakup lembaga negara, aktor pembuat kebijakan, pelaksana regulasi, serta pemangku kepentingan non-negara seperti lembaga swadaya masyarakat dan akademisi yang berfokus pada isu perlindungan data dan hak digital. Keseluruhan aktor dan institusi yang memiliki relevansi langsung dalam proses formulasi, implementasi, dan pengawasan kebijakan perlindungan data pribadi di Indonesia. Pemilihan populasi teoritis ini penting untuk memastikan bahwa analisis mencakup spektrum kepentingan yang mempengaruhi efektivitas regulasi data pribadi. Keberagaman aktor yang terlibat mencerminkan kompleksitas tata kelola data dalam konteks demokrasi digital dan birokrasi pemerintahan.

Sampel dalam penelitian ini ditentukan secara purposive atau bertujuan, yaitu dipilih berdasarkan keterkaitannya yang kuat dengan topik penelitian. Sampel lembaga meliputi antara lain: Kementerian Komunikasi dan Informatika (Kominfo), yang bertindak sebagai regulator utama; Badan Siber dan Sandi Negara (BSSN) sebagai pelaksana teknis keamanan siber; serta Komisi I DPR RI, yang memiliki peran dalam proses legislasi UU PDP. Di samping itu, penelitian ini juga dapat melibatkan organisasi masyarakat sipil seperti SAFEnet, ELSAM, atau akademisi dan peneliti yang aktif dalam isu privasi digital. Jumlah informan ditentukan hingga mencapai *saturation point* (titik jenuh informasi), diperkirakan pada kisaran 10-15 wawancara mendalam

C. Prosedur Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan melalui studi kepustakaan terhadap peraturan perundang-undangan yang relevan, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta literatur ilmiah, jurnal akademik, dan laporan lembaga yang membahas isu privasi digital dan kelembagaan negara. Selain itu, data dikumpulkan melalui analisis dokumen kelembagaan seperti laporan resmi, strategi nasional, risalah kebijakan, dan publikasi publik dari instansi terkait seperti Kominfo, BSSN, DPR, serta lembaga pengawasan lainnya. Untuk memperkaya konteks dan mendapatkan perspektif yang lebih mendalam, data juga diperoleh dari wawancara semi-terstruktur terhadap informan kunci. Seluruh data yang diperoleh diuji melalui triangulasi sumber dan metode untuk memastikan validitas dan reabilitas temuan.

D. Instrumen Penelitian

Instrumen yang digunakan dalam penelitian ini disesuaikan dengan pendekatan kualitatif dan bersifat fleksibel namun terarah. Instrumen utama berupa pedoman telaah dokumen yang difokuskan untuk mengidentifikasi struktur regulasi, pola kebijakan, serta peran kelembagaan dalam isu perlindungan data. Untuk wawancara, instrumen yang digunakan adalah daftar pertanyaan terbuka yang dikembangkan berdasarkan kerangka teori institusional baru, dengan fokus pada persepsi, praktik

kelembagaan, serta hambatan implementatif yang dihadapi oleh aktor-aktor terkait. Instrumen ini dirancang agar mampu menangkap dinamika relasi antara norma formal dan perilaku institusional, serta membuka ruang eksploratif bagi informan untuk mengungkapkan pandangan kritis terhadap efektivitas negara dalam menjamin hak atas privasi digital.

E. Prosedur Analisis Data

Analisis data dilakukan secara kualitatif melalui proses open coding, axial coding, dan kategorisasi tema untuk mengidentifikasi pola-pola yang berulang. Data dari dokumen hukum, kebijakan kelembagaan, dan hasil wawancara ditata secara sistematis untuk mengidentifikasi tema-tema utama yang berkaitan dengan hambatan struktural, norma institusional, serta dinamika politik dalam perlindungan data pribadi. Setiap temuan dianalisis menggunakan pendekatan teoritis institusional baru, guna mengungkap keterkaitan antara struktur organisasi, nilai-nilai internal lembaga, dan kegagalan dalam menjalankan fungsi perlindungan. Analisis juga melibatkan pembacaan kritis terhadap hubungan antaraktor dan konteks kebijakan yang melatarbelakangi lemahnya implementasi regulasi, sehingga dapat ditarik kesimpulan yang bersifat reflektif dan konseptual tentang disfungsi kelembagaan dalam sistem perlindungan data di Indonesia.

F. Pertimbangan Etis

Pertimbangan etis dalam penelitian ini menjadi aspek penting, terutama karena topik yang dikaji berkaitan dengan hak privasi, kerahasiaan informasi, dan kepercayaan terhadap lembaga negara. Seluruh proses pengumpulan data yang melibatkan manusia, seperti wawancara, dilakukan dengan menjunjung tinggi prinsip informed consent, di mana informan diberi penjelasan lengkap mengenai tujuan, ruang lingkup, dan penggunaan data yang diberikan, serta memiliki hak untuk menolak atau menghentikan partisipasi kapan pun. Identitas informan dijaga secara anonim dan data yang bersifat sensitif akan disimpan dengan perlindungan yang ketat untuk menghindari potensi pelanggaran etika. Keterbatasan penelitian diakui, terutama pada sifat kualitatif yang membuat generalisasi hasil terbatas dan minimnya data kuantitatif tentang dampak langsung bagi korban kebocoran data.

III. HASIL DAN DISKUSI

Hasil

A. Analisis Kelembagaan terhadap Krisis Perlindungan Data Pribadi di Indonesia

Temuan rinci disajikan dalam Tabel 2, yang menunjukkan lima bentuk utama disfungsi kelembagaan dalam perlindungan data pribadi di Indonesia, mulai dari lemahnya struktur formal hingga keterbatasan kapasitas teknis. Semua bentuk disfungsi tersebut berkontribusi terhadap lemahnya perlindungan data warga negara, baik dalam aspek pencegahan, deteksi, maupun respons terhadap insiden. Disfungsi ini tidak hanya berdampak pada sektor pemerintahan, tetapi juga memengaruhi kepercayaan publik terhadap institusi digital. Selain itu, kurangnya integrasi antar-lembaga memperparah ketidakefisienan dalam menangani pelanggaran data pribadi.

Tabel 2. Identifikasi Disfungsi Kelembagaan dalam Perlindungan Data Pribadi di Indonesia

No	Jenis Disfungsi Kelembagaan	Bentuk Kegagalan Institusional	Dampak terhadap Perlindungan Data Pribadi
1	Struktur Formal Lemah	Tidak adanya lembaga pengawas independen	Tidak ada otoritas tunggal untuk kontrol dan sanksi
2	Tumpang Tindih Kewenangan	Kominfo, BSSN, dan lembaga lain saling menunggu	Penanganan insiden lambat, koordinasi buruk
3	Budaya Birokrasi Prosedural	Fokus pada tanggung jawab administratif, bukan publik	Tidak ada mekanisme notifikasi korban
4	Norma Institusional Tidak Adaptif	Tidak ada SOP mitigasi kebocoran	Respon instansi tidak sistematis dan defensif
5	Kapasitas Teknis Terbatas	Ketergantungan pada vendor, kurang SDM siber	Tidak mampu deteksi dini atau merespons serangan

B. Ringkasan Insiden Kebocoran Data Pribadi di Indonesia (2019–2024)

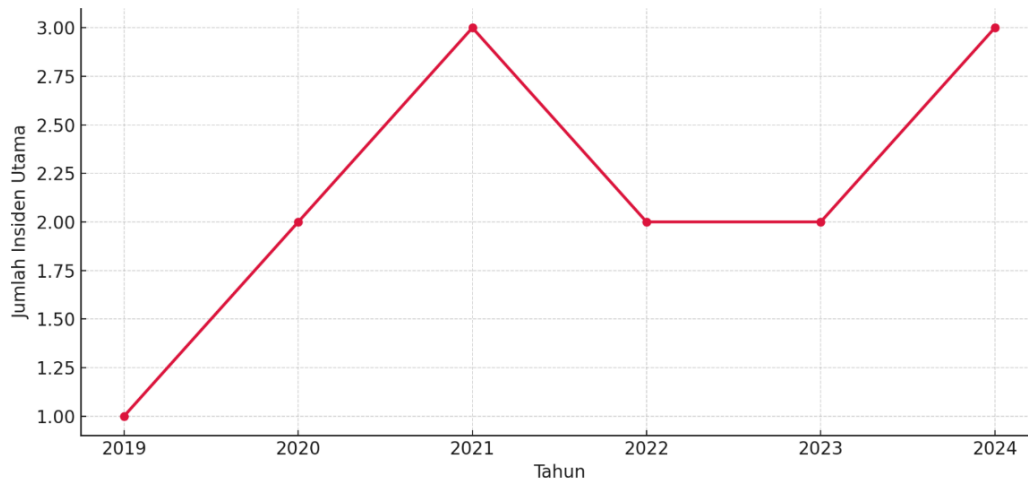
Sepanjang periode 2019 hingga 2024, Indonesia mengalami berbagai insiden kebocoran data pribadi berskala besar yang menyoroti kegagalan struktural dan lemahnya transparansi. Tabel 3 merangkum empat kasus kebocoran paling representatif yang menyoroti lemahnya pencegahan dan penegakan hukum. Kasus-kasus tersebut melibatkan berbagai instansi besar, termasuk lembaga pemerintah dan sektor swasta penyedia layanan publik. Tidak adanya sanksi tegas terhadap pelaku maupun institusi terkait memperlihatkan celah besar dalam sistem perlindungan data nasional.

Tabel 3. Ringkasan Kasus Kebocoran Data Pribadi di Indonesia (2019–2024)

No	Nama Kasus	Tahun	Lembaga Terkait	Jenis Data Bocor	Respons Institusi
1	BPJS Kesehatan	2021	BPJS, Kominfo	Data kependudukan dan kesehatan	Tidak ada notifikasi kepada korban
2	PeduliLindungi	2021	Kemenkes, Kominfo	Status vaksinasi, riwayat lokasi, identitas pengguna	Dibatasi pengakuan, tanggung jawab kabur
3	MyPertamina	2023	Pertamina, vendor swasta	Transaksi pelanggan dan akun digital	Penyangkalan awal, diikuti pengakuan terbatas
4	PDNS Kominfo	2024	Kominfo, BSSN	Infrastruktur server nasional, data teknis sistem	Belum pulih, evaluasi belum diumumkan

C. Tren Insiden Kebocoran Data Pribadi di Indonesia (2019–2024)

Tren insiden kebocoran data pribadi dalam enam tahun terakhir menunjukkan pola yang fluktuatif namun konsisten meningkat sejak 2019. Meskipun sempat menurun pada 2022, jumlah insiden besar kembali melonjak pada 2024, Gambar 1 menunjukkan kecenderungan ini dan mengindikasikan belum adanya perbaikan kelembagaan yang efektif. Peningkatan ini terjadi bersamaan dengan semakin luasnya penggunaan sistem digital dalam layanan publik dan komersial. Hal ini menunjukkan bahwa pertumbuhan infrastruktur digital tidak dibarengi dengan penguatan mekanisme keamanan data yang memadai.



Gambar 1. Tren Insiden Kebocoran Data Pribadi di Indonesia (2019–2024)

D. Persepsi Aktor Kunci terhadap Kegagalan Institusional

Wawancara dengan beragam aktor kunci mulai dari birokrat, akademisi, praktisi keamanan siber, hingga aktivis digital menggambarkan adanya konsensus bahwa kelembagaan negara belum mampu menjamin perlindungan data pribadi secara sistemik. Mayoritas informan menyoroti ketiadaan lembaga pengawas independen, lemahnya sanksi dalam UU PDP, serta nihilnya kewajiban pemberitahuan kepada korban kebocoran data. Tabel 4 menunjukkan pernyataan aktor kunci memperkuat temuan dokumenter bahwa respons institusi lebih administratif daripada substantif. Sebagian informan juga menyatakan bahwa koordinasi antar lembaga seringkali terhambat oleh tumpang tindih kewenangan dan orientasi politik sektoral.

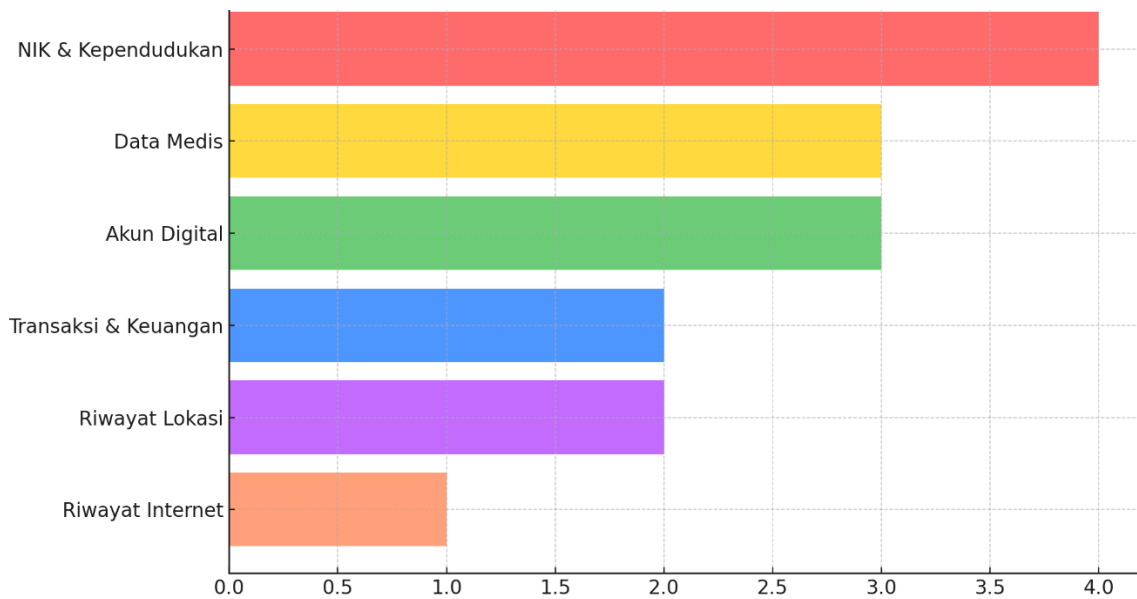
Tabel 4. Ringkasan Kutipan Wawancara Kunci tentang Disfungsi Perlindungan Data Pribadi

No	Nama Samaran	Latar Belakang	Kutipan Pernyataan Utama	Tanggal Wawancara
1	Ratna	Pegawai Kementerian	"Kami tahu bahwa ada insiden data breach, tapi tidak ada prosedur wajib memberi tahu publik atau korban."	Apr-24
2	Ratih	Pegawai Kementerian	"Akhirnya, masyarakat hanya tahu dari media, bukan dari kami."	Apr-24
3	Budi	ASN lembaga teknis perlindungan data	"Bahkan dalam lingkungan kami sendiri, siapa yang bertanggung jawab jika data bocor itu belum jelas."	Mei 2024
4	Budi	ASN lembaga teknis perlindungan data	"Semua merasa bukan tugasnya langsung."	Mei 2024
5	Lestari	Akademisi dan peneliti privasi digital	"Selama belum ada lembaga pengawas independen yang kuat, UU PDP ya hanya simbol saja."	Juni 2024
6	Lestari	Akademisi dan peneliti privasi digital	"Implementasinya bisa dibilang hampir nol."	Juni 2024
7	Fadli	Mantan staf teknis BSSN	"Sebagian besar serangan itu baru diketahui setelah ramai di media sosial. Bukan dari sistem deteksi kita."	Juni 2024
8	Wulan	Aktivis digital dan advokat privasi	"Kalau terjadi kebocoran, publik tidak punya mekanisme formal untuk menuntut kejelasan siapa pelakunya."	Mei 2024

9	Doni	Praktisi keamanan siber	"Sebagian lembaga masih pakai sistem lama tanpa enkripsi. Padahal itu wajib."	Apr-24
10	Sinta	Dosen kebijakan publik	"Lembaga kita terlalu fokus pada pelaporan, bukan pada pencegahan kebocoran."	Maret 2024
11	Rizky	Peneliti independen kebijakan digital	"Koordinasi antar-lembaga sangat lemah. Bahkan kadang antar kementerian saling menyalahkan."	Juni 2024
12	Angga	Konsultan transformasi digital	"UU PDP itu penting, tapi kalau tidak ada sanksi tegas, lembaga akan tetap cuek."	Mei 2024
13	Tania	Pegiat literasi digital masyarakat	"Orang biasa tidak tahu datanya bocor sampai viral. Harusnya ada kewajiban notifikasi langsung ke pengguna."	Apr-24

E. Dominasi Kebocoran pada Data Berisiko Tinggi

Salah satu dimensi penting dari krisis perlindungan data pribadi di Indonesia adalah tingginya frekuensi kebocoran pada jenis data yang sangat sensitif. Penelitian ini menemukan bahwa kategori seperti data kependudukan (NIK), data medis, dan akun digital menjadi target utama dari insiden kebocoran dalam lima tahun terakhir. Distribusi jenis data yang bocor divisualisasikan dalam Gambar 2. Data kependudukan seperti NIK seringkali digunakan untuk berbagai tindakan penipuan yang memanfaatkan informasi pribadi korban.



Gambar 2. Jenis Data yang Sering Bocor di Indonesia

Diskusi

Hasil penelitian ini menunjukkan bahwa kebocoran data pribadi di Indonesia bukan hanya akibat lemahnya regulasi, tetapi juga disfungsi kelembagaan yang bersifat struktural dan kultural. Meskipun UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi telah disahkan, pelaksanaannya belum didukung oleh lembaga pengawas independen, mekanisme tanggap darurat, dan budaya birokrasi yang akuntabel (Hukom et al., 2025). Temuan ini sejalan dengan teori institusional baru yang menekankan pentingnya norma, perilaku, dan logika kepatasan dalam efektivitas kebijakan publik (Integra, 2024) dan (Risi et al., 2023), menyoroti peran nilai dalam kapasitas kelembagaan, sedangkan (Alam & Miah,

2024) menegaskan pengaruh *logic of appropriateness* pada perilaku institusional. Norma dan nilai yang berkembang dalam institusi sering kali menentukan sejauh mana aturan formal diikuti atau diabaikan oleh pelaku di lapangan.

Penelitian ini memperdalam analisis sebelumnya. (Nurchayhan et al., 2023) menyoroti lemahnya koordinasi antarlembaga. Penelitian ini mengidentifikasi tumpang tindih kewenangan. Penelitian ini juga menemukan ketiadaan SOP wajib lapor. Laporan juga menyoroti lemahnya akuntabilitas. Variasi respons institusi antara pengakuan, penyangkalan, dan diam menunjukkan absennya standar etis (Khan, 2025). Kelemahan ini kontras dengan negara lain. Singapura memiliki PDPC yang independen (Idris et al., 2024). PDPC proaktif dalam edukasi dan penegakan hukum (Dwi et al., 2024). Filipina melalui NPC menetapkan SOP pelaporan insiden 72 jam (Datu et al., 2024). NPC juga melibatkan masyarakat sipil (Khan, 2025). Jerman menerapkan prinsip *privacy by design* (Custers et al., 2018). Jerman memberi wewenang badan pengawas untuk menjatuhkan sanksi (Alberton, 2021). Perbandingan ini menegaskan pentingnya otoritas independen, transparansi, dan respons cepat hal yang masih absen di Indonesia.

Secara teoritis, penelitian ini menegaskan pendekatan institusional sebagai kerangka untuk memahami efektivitas kebijakan perlindungan data. Secara praktis, diperlukan pembentukan lembaga pengawas independen. Diperlukan penyusunan SOP wajib lapor. Kapasitas teknis harus diperkuat. Keterlibatan publik perlu diperluas agar UU PDP tidak menjadi produk hukum simbolik. Penelitian ini terbatas karena hanya menggunakan data kualitatif. Fokus masih pada aktor kelembagaan. Pengalaman korban kebocoran belum terwakili. Tingkat literasi digital nasional belum terukur. Penelitian lanjutan dapat melibatkan survei publik, analisis big data, dan studi komparatif ASEAN.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa kebocoran data pribadi di Indonesia merupakan gejala dari persoalan kelembagaan yang lebih dalam. Ketidakjelasan peran antar instansi, lambatnya respons terhadap insiden, dan absennya standar prosedural menjadi indikator lemahnya tata kelola perlindungan data. Temuan ini diperkuat oleh data kasus, wawancara kunci, dan grafik tren yang menampilkan konsistensi kegagalan dalam aspek pencegahan maupun penanganan kebocoran. Selain itu, rendahnya pemahaman masyarakat atas hak-hak data pribadi turut memperburuk kerentanan terhadap pelanggaran. Secara teoritis, penelitian ini memperluas pemahaman tentang pentingnya dimensi norma dan budaya institusional dalam pelaksanaan regulasi digital. Sementara secara praktis, hasil studi ini menegaskan perlunya pembentukan lembaga pengawas yang independen, penyusunan SOP wajib lapor insiden, serta program literasi data bagi publik.

Adapun keterbatasan studi ini terletak pada cakupan informan yang terbatas pada aktor kelembagaan dan tidak mencakup suara korban secara langsung. Penelitian mendatang disarankan untuk mengeksplorasi pengalaman warga, serta melakukan studi komparatif antar negara guna memperkaya wawasan kelembagaan dalam konteks regional. Keseluruhan hasil penelitian ini menegaskan bahwa tanpa pembenahan institusi secara menyeluruh, perlindungan data pribadi di Indonesia akan terus berada

dalam posisi yang rapuh. Sebagai rekomendasi kebijakan, penelitian ini mengusulkan peta jalan penguatan perlindungan data pribadi. Dalam jangka pendek (1-2 tahun), pemerintah perlu membentuk lembaga pengawas independen, menetapkan SOP mitigasi kebocoran, dan mewajibkan mekanisme notifikasi korban. Dalam jangka menengah (3-5 tahun), kapasitas teknis kelembagaan harus diperkuat melalui pelatihan siber nasional, pembangunan infrastruktur deteksi dini, serta harmonisasi regulasi antarlembaga. Peta jalan ini memungkinkan perbaikan kelembagaan dilakukan secara bertahap, sehingga UU PDP dapat berfungsi secara substantif dan tidak hanya simbolis.

REFERENSI

- Alam, M. K., & Miah, M. S. (2024). Do Islamic Banks use Institutional Theory in the Light of Shariah Governance? Empirical Evidence from a Muslim Dominant Country. *Heliyon*, *10*(2), 24252. <https://doi.org/10.1016/j.heliyon.2024.e24252>
- Alberton, C. S. C. (2021). The Fundamental Right of Confidentiality and Integrity of IT systems in Germany: a call for “IT Privacy” right in Brazil? *International Cybersecurity Law Review*, *2*(2), 253–269. <https://doi.org/10.1365/s43439-021-00037-4>
- Arda, R., Christian, D., & Raga, W. J. (2025). Restorative Justice for Online Hate Speech: A Socio-Legal Framework. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(2), 1179–1193. <https://doi.org/10.51903/zywfje63>
- Aurellia, A. (2025). Cara Hindari Penipuan Pinjol yang Makin Marak, Simak soal Data Pribadi! *Detik.Com*. <https://www.detik.com/jatim/hukum-dan-kriminal/d-7908836/cara>
- Chan, H. Y., Toh, H. J., & Lysaght, T. (2024). Cross-jurisdictional Data Transfer in Health Research: Stakeholder Perceptions on the Role of Law. *Asian Bioethics Review*, *16*(4), 663–682. <https://doi.org/10.1007/s41649-024-00283-8>
- Coates, S. K., Trudgett, M., & Page, S. (2023). Indigenous Institutional Theory: a New Theoretical Framework and Methodological Tool. *Australian Educational Researcher*, *50*(3), 903–920. <https://doi.org/10.1007/s13384-022-00533-4>
- Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A Comparison of Data Protection Legislation and Policies across the EU. *Computer Law and Security Review*, *34*(2), 234–243. <https://doi.org/10.1016/j.clsr.2017.09.001>
- Datu, A. K. K., Mharcelyn, M. K., Jul-Asri, A. H., & Merhana, T. (2024). Data Governance and Privacy in Sulu, Philippines: Building Trust and Ensuring Accountability in Digital Public Service Delivery. *Open Access Indonesia Journal of Social Sciences*, *8*(1), 1952–1966. <https://doi.org/10.37275/oaijss.v8i1.283>
- Dewi, R. I. (2024). Pusat Data Nasional Kena Ransomware, Guru Besar IT Angkat Bicara. *Cnbcindonesia.Com*. <https://www.cnbcindonesia.com/tech/20240627081538-37-549695/pusat>
- Dwi, K. K., Hehanussa, D. J., Setiawan, R., Susilowati, I., & Helfisar, D. (2024). Criminal Sanctions and Personal Data Protection in Indonesia. *Lex Publica*, *11*(2), 221–247. <https://doi.org/10.58829/lp.11.2.2024.1-27>
- Hukom, S., Humi, N., & Lukman, I. (2025). The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(1), 974–

992. <https://doi.org/10.51903/hakim.v3i1.2291>
- Idris, M. F., Laksito, J., & Ariyani, W. (2024). Tanggung Jawab Hukum Perusahaan Teknologi Atas Penyalahgunaan Data Pengguna : Studi Kasus Di ASEAN. *Jaksa : Jurnal Kajian Ilmu Hukum Dan Politik*, 2(4), 45–56. <https://doi.org/10.51903/jaksa.v2i4.2268>
- Integra, P. (2024). Institutional Theory dalam Tata Kelola Perusahaan: Perspektif Legitimasi dan Keberlanjutan. *Pragmaintegra.Com*. <https://pragmaintegra.com/institutional>
- Kalsum, U. (2025). Data Nasional Bocor, Apa Dampaknya pada Data Pribadi Kita? *Rri.Co.Id*. <https://rri.co.id/lain-lain/801191/data>
- Kennedy, A. (2025). Tantangan Implementasi dan Perkembangan Hukum Telematika di Indonesia. *Ethics and Law Journal: Business and Notary*, 3(2), 1–9. <https://doi.org/10.61292/eljbn.262>
- Khan, M. N. I. (2025). Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices. *American Journal of Scholarly Research and Innovation*, 4(1), 138–174. <https://doi.org/10.63125/a4gbeb22>
- Kossay, M., Putra, R. K., & Idris, M. F. (2025). Keberlanjutan Ekonomi dalam Perspektif Hukum: Analisis Regulasi Environmental, Social, and Governance di Indonesia. *Perkara : Jurnal Ilmu Hukum Dan Politik*, 3(1), 675–693. <https://doi.org/10.51903/perkara.v3i1.2355>
- Lhotta, R. (2024). Dysfunctional Constitutionalism or Dysfunctional Politics: A Matter of Law, Politics, and Institutional Design. *Politische Vierteljahresschrift*, 65(2), 285–309. <https://doi.org/10.1007/s11615-023-00505-y>
- Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal Badjeber, M., & Rahmadia, M. H. (2023). Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas di Indonesia. *Jurnal Esensi Hukum*, 5(2), 115–131. <https://doi.org/10.35586/jsh.v5i2.240>
- Maharani, T., & Meiliana, D. (2021). Dugaan Kebocoran Data 279 Juta WNI, BPJS Kesehatan Tempuh Langkah Hukum. *Kompas.Com*. <https://nasional.kompas.com/read/2021/05/25/11140881/dugaan>
- MetroTv. (2023). Lagi, Data Pribadi WNI di Kemendagri Diduga Bocor dan Dijual di Dark Web. *Metronews.Com*. <https://www.metrotvnews.com/play/nxgc5lq0>
- 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. <https://doi.org/10.62379/wxf6a077>
- Perdana, P. A. (2022). Dugaan Kebocoran Data MyPertamina Menjadi Ujian UU Perlindungan Data Pribadi. *Kompas.Id*. <https://www.kompas.id/artikel/masih-diinvestigasi-bocornya-data-juga-menjadi-ujian-uu-pdp>
- Ramiro, A. (2025). Democratic Oversight of Government Hacking by Intelligence Agencies A Critical Analysis of Brazil and Germany. *Weizenbaum Journal of the Digital Society*, 02. <https://doi.org/10.34669/wi.wjds/5.2.3>
- Risi, D., Vigneau, L., Bohn, S., & Wickert, C. (2023). Institutional Theory-Based Research on Corporate Social Responsibility: Bringing Values Back in. *International Journal of Management Reviews*, 25(1), 3–23. <https://doi.org/10.1111/ijmr.12299>

- Sagita, S. N. (2025). Penjelasan Kemenkes soal PeduliLindungi Berubah Jadi Laman Judi Online. *Detik.Com*. <https://www.tempo.co/hukum/penjelasan-kemenkes-soal-dugaan-pedulilindungi-berubah-jadi-situs-judi-online-1493867>
- Wahyuni, W. (2023). Ancaman Data Pribadi Diperjualbelikan di Balik Judi Online. *Hukumonline.Com*. <https://www.hukumonline.com/berita/a/ancaman-data-pribadi-diperjualbelikan-di-balik-judi-online-lt651ad5dc97c13/>
- Yonatan, A. (2023). Indonesia Peringkat 4, Ini Dia 7 Negara Pengguna Internet Terbesar di Dunia. *Goodstats*. <https://data.goodstats.id/statistic/indonesia-peringkat-4-ini-dia-7-negara-pengguna-internet-terbesar-di-dunia-flw6v>