Pasinformatik, Volume 5, Issue 2, July 2026
E-ISSN : 2986-5360

UU Perlindungan Data Pribadi vs Keamanan Siber : Analisis Kesenjangan dan Implikasinya terhadap Insiden Data di Indonesia

Doddy Ferdiansyah*, R. Sandhika Galih Amalga, M. Fadli Muttaqin*****

Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pasundan
Jln. Dr. Setiabudhi no. 193 Bandung, Jawa Barat
*doddy@unpas.ac.id *sandhikagalih@unpas.ac.id *miftahulfadli@unpas.ac.id

Abstrak: Maraknya insiden penyalahgunaan dan kebocoran data di Indonesia menunjukkan adanya kesenjangan antara kerangka hukum dan kesiapan teknis implementasinya. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah memberikan landasan hukum komprehensif, namun insiden-insiden nyata terus terjadi setelah regulasi ini disahkan. Penelitian ini menganalisis kesenjangan antara ketentuan normatif UU PDP dengan praktik teknis keamanan siber di Indonesia serta mengidentifikasi implikasinya terhadap insiden penyalahgunaan data. Metode yang digunakan adalah kualitatif deskriptif-analitis melalui studi literatur yang dikombinasikan dengan analisis studi kasus sekunder. Sumber data mencakup laporan resmi BSSN 2023, Kominfo-CSIRT 2024, laporan ancaman digital AwanPintar.id 2025, artikel jurnal ilmiah, serta tiga kasus insiden nyata pada 2025–2026. Hasil penelitian menunjukkan bahwa UU PDP masih bersifat prinsipil dan belum menetapkan standar teknis minimum yang eksplisit, sehingga menimbulkan compliance gap antara kewajiban normatif dan kesiapan operasional pengendali data. Kesenjangan ini terbukti dari tiga dimensi insiden: pencurian identitas digital (*social engineering*), penyalahgunaan data identitas sebagai instrumen kejahatan finansial (insider abuse), dan kegagalan pengamanan teknis sistem pemerintah (*technical breach*). Penelitian merekomendasikan penerbitan regulasi turunan teknis, percepatan pembentukan Badan Pelindungan Data Pribadi yang independen, serta adopsi standar ISO/IEC 27001 dan NIST sebagai acuan wajib bagi pengendali data.

Kata Kunci: UU Perlindungan Data Pribadi; Keamanan Siber; Kebocoran Data; Kesenjangan Regulasi; Implementasi Teknis; Pengendali Data

I. PENDAHULUAN

Transformasi digital yang berlangsung masif di Indonesia telah menggeser data pribadi dari sekadar informasi administratif menjadi aset digital yang bernilai tinggi sekaligus target kejahatan siber yang semakin canggih. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa total trafik anomali di Indonesia selama tahun 2023 mencapai 403.990.813 anomali, dengan jenis tertinggi berupa Generic Trojan RAT yang mengindikasikan aktivitas backdoor communication menuju server kendali milik aktor ancaman [2]. Lebih jauh, terdapat 347 dugaan insiden siber sepanjang 2023 dengan jenis insiden tertinggi adalah data breach, disertai 1.674.185 temuan data exposure di darknet yang berdampak pada 429 stakeholder. Sektor administrasi pemerintahan menjadi area paling terdampak dengan persentase 39,78% dari seluruh data exposure yang teridentifikasi [2].

Merespons eskalasi ancaman ini, pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai landasan hukum komprehensif yang mengatur hak subjek data, kewajiban pengendali data, dan mekanisme penegakan sanksi [1]. Kehadiran UU PDP dinilai sebagai tonggak legislasi penting yang mengakhiri fragmentasi pengaturan data yang sebelumnya tersebar di lebih dari 30 regulasi sektoral [17]. Namun demikian, efektivitas implementasi UU PDP masih menjadi pertanyaan mendasar, terutama dari perspektif teknis keamanan siber.

Realitas di lapangan membuktikan bahwa insiden penyalahgunaan data terus terjadi bahkan setelah UU PDP disahkan. Pada Juli 2026, seorang ibu rumah tangga di Jakarta Selatan kehilangan Rp250 juta akibat penipuan asmara daring yang memanfaatkan identitas digital polisi aktif yang dicatut tanpa sepengetahuannya [22]. Pada periode yang sama, Kejaksaan Tinggi Jawa Timur menetapkan tersangka dalam kasus penyalahgunaan data KTP dan Kartu Keluarga sekitar 900 petani untuk pengajuan kredit fiktif, dengan kerugian negara sebesar Rp41,48 miliar yang dikonfirmasi BPKP [23]. Sementara itu, pada April 2025, seorang teknisi ponsel berhasil membobol situs Dinas Sosial Provinsi Jawa Tengah dan mencuri 1.239.573 data NIK dan KK warga dengan mengeksploitasi kerentanan sistem yang belum diperbarui [24]. Ketiga insiden ini mengindikasikan adanya kesenjangan struktural yang belum tertangani antara regulasi dan realitas teknis.

Berdasarkan latar belakang tersebut, penelitian ini merumuskan tiga pertanyaan: (1) Sejauh mana ketentuan UU PDP mengatur standar teknis pengamanan data? (2) Di mana letak kesenjangan antara ketentuan normatif UU PDP dengan praktik teknis keamanan siber? (3) Apa implikasi kesenjangan tersebut terhadap insiden penyalahgunaan data yang terjadi? Penelitian ini berkontribusi dengan mengisi celah kajian yang ada dimana sebagian besar penelitian terdahulu berfokus pada analisis normatif-yuridis semata, sementara perspektif teknis keamanan siber masih kurang dieksplorasi secara sistematis [5],[8],[9].

II. TINJAUAN PUSTAKA

A. Kerangka Regulasi UU PDP No. 27 Tahun 2022

UU PDP merupakan instrumen hukum yang secara filosofis mengubah data pribadi dari komoditas administratif menjadi hak konstitusional yang melekat pada martabat manusia, sesuai amanat Pasal 28G ayat (1) UUD 1945 [18]. Secara normatif, UU PDP telah menetapkan sejumlah kewajiban teknis bagi pengendali data. Pasal 1 mendefinisikan Data Pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi. Pasal 20 mewajibkan pemrosesan berdasarkan persetujuan eksplisit (*consent*) dan tujuan yang sah. Pasal 35 mengharuskan pengendali data menerapkan langkah-langkah teknis dan organisasi yang memadai untuk melindungi data dari gangguan, kebocoran, dan kerusakan. Pasal 46 mewajibkan notifikasi kegagalan perlindungan data kepada subjek data dan lembaga paling lambat 3×24 jam. Pasal 47 menegaskan prinsip akuntabilitas pengendali data atas seluruh proses pemrosesan [1]. Namun demikian, UU PDP menghadapi tantangan implementasi yang signifikan. Putra dan Noriansyah (2026) menyatakan bahwa meskipun UU PDP telah memberikan landasan hukum yang kuat, implementasinya masih menghadapi tantangan seperti rendahnya kesiapan institusi, minimnya literasi perlindungan data, dan belum optimalnya mekanisme pengawasan [5]. Hal ini diperparah oleh belum terbentuknya Badan Pelindungan Data Pribadi (BPDP) yang diamanatkan undang-undang, sehingga pengawasan dan penegakan sanksi belum dapat berjalan efektif [8],[9].

B. Prinsip Teknis Keamanan Informasi dan Standar Internasional

Dari perspektif teknis keamanan informasi, perlindungan data pribadi bertumpu pada CIA Triad yaitu Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan), sebagai fondasi konseptual yang diakui secara internasional. Prinsip *Privacy by Design*, yang diperkenalkan oleh Ann Cavoukian dan diadopsi GDPR Pasal 25, mengharuskan perlindungan privasi diintegrasikan ke dalam desain sistem sejak tahap awal, bukan ditambahkan setelah sistem dibangun [6]. Standar ISO/IEC 27001 memberikan kerangka Sistem Manajemen Keamanan Informasi (ISMS), sementara ISO/IEC 27701 merupakan ekstensinya yang secara khusus mengatur Sistem Manajemen Informasi Privasi (PIMS) [18]. NIST SP 800-34 mengatur *contingency planning*, termasuk kewajiban *backup*, *recovery time objective* (RTO), dan *recovery point objective* (RPO) [6]. Penting untuk dicatat bahwa standar-standar internasional ini tidak diatur secara eksplisit sebagai kewajiban dalam UU PDP. Lie dan Fitriyantica (2026) menemukan bahwa meskipun kewajiban pengendali data dalam Pasal 35 dan 39 UU PDP sejalan dengan prinsip ketahanan data, undang-undang ini belum dilengkapi pedoman teknis minimum terkait mekanisme pencadangan, frekuensi *backup*, dan pengujian pemulihan, sehingga menimbulkan kesenjangan antara kepatuhan normatif dan kesiapan operasional [6].

C. Komparasi Regulasi Global: GDPR, PDPA Singapura, dan UU PDP

Perbandingan dengan regulasi internasional menunjukkan bahwa UU PDP masih tertinggal dalam hal preskriptivitas teknis. *General Data Protection Regulation* (GDPR) Uni Eropa Pasal 32 secara eksplisit mewajibkan pseudonymisasi, enkripsi, kemampuan pemulihan data, dan pengujian keamanan berkala. GDPR juga menetapkan *Data Protection Impact Assessment* (DPIA) sebagai kewajiban untuk sistem berisiko tinggi dan mengharuskan pembentukan *Data Protection Officer* (DPO) [8]. *Personal Data Protection Act* (PDPA) Singapura dilengkapi *Technical Guidelines* dari *Personal Data Protection Commission* (PDPC) yang memberikan panduan teknis operasional bagi pengendali data [6]. Sementara itu, UU PDP Indonesia belum memiliki regulasi turunan teknis yang setara, tidak mewajibkan DPIA secara eksplisit, dan belum mengatur standar minimum keamanan teknis yang terukur [14],[17]. Sanksi yang diatur pun relatif lebih rendah, maksimal 2% dari pendapatan tahunan korporasi (Pasal 57), dibanding GDPR yang dapat mencapai €20 juta atau 4% dari omzet global tahunan [8].

Tabel 1. Komparasi Regulasi Perlindungan Data Indonesia, Uni Eropa, dan Singapura

Aspek	**UU PDP Indonesia**	**GDPR Uni Eropa**	**PDPA Singapura**
Lembaga Pengawas	BPDP (belum terbentuk)	EDPB (independen, aktif)	PDPC (independen, aktif)
Standar Teknis	Prinsipil, tidak preskriptif	Wajib enkripsi, pseudonymisasi, backup	Technical Guidelines PDPC
DPIA	Tidak diatur eksplisit	Wajib untuk sistem berisiko tinggi	Dianjurkan, tidak wajib
Sanksi Maksimal	2% pendapatan tahunan	€20 juta / 4% omzet global	SGD 1 juta / 10% omzet
Kewajiban DPO	Tidak diatur eksplisit	Wajib untuk kategori tertentu	Tidak wajib, dianjurkan

D. Lanskap Ancaman Siber di Indonesia

Laporan AwanPintar.id Semester 1 Tahun 2025 mencatat 133.439.209 total serangan siber yang terdeteksi, dengan penurunan 94,66% dibanding semester 1 tahun 2024. Namun penurunan ini bukan karena sistem keamanan membaik, melainkan karena anomali lonjakan di tahun 2024 dipicu oleh konteks Pemilu [3]. Yang perlu diwaspadai adalah lonjakan *malware* sebesar 38,93% pada Januari 2025, kemunculan botnet Mirai berbasis Linux, serta peningkatan eksploitasi CVE (*Common Vulnerabilities and Exposures*) oleh pelaku kejahatan siber yang semakin mahir mengeksploitasi kerentanan yang belum ditambal [3]. Laporan Kominfo-CSIRT 2024 mencatat total trafik anomali 2.117 GBps dengan 27 insiden siber dalam lingkungan Kementerian Komunikasi dan Digital sendiri, didominasi *injected malicious file* sebanyak 17 kali [4]. Dari perspektif jenis ancaman yang relevan dengan kebocoran data pribadi, BSSN mengidentifikasi *data breach* sebagai jenis insiden dengan jumlah dugaan tertinggi di antara 347 dugaan insiden siber sepanjang 2023. Jenis kerentanan kritis tertinggi yang ditemukan melalui ITSA adalah *Insecure Direct Object Reference* (IDOR), yang memungkinkan aktor ancaman mengakses atau memodifikasi data tanpa otorisasi yang memadai [2]. Rambe dan Kurniawan (2026) menegaskan bahwa perbedaan mendasar antara sektor publik dan swasta dalam kebijakan keamanan siber, di mana sektor publik lebih lambat mengadopsi standar teknis modern, memperparah kondisi kerentanan ini [16].

E. Penelitian Terdahulu dan Posisi Artikel Ini

Kajian terdahulu terkait UU PDP dan keamanan siber dapat dipetakan ke dalam beberapa kelompok. Pertama, kelompok kajian normatif-yuridis yang menganalisis substansi pasal-pasal UU PDP, perbandingan dengan GDPR, dan kerangka sanksi [14],[17],[19]. Kedua, kelompok kajian implementasi yang membahas kesiapan institusi dan tantangan kepatuhan [5][9][12]. Ketiga, kelompok kajian studi kasus yang menganalisis insiden kebocoran data spesifik di sektor *e-commerce* atau pemilu [7][15]. Keempat, kajian teknis yang membahas standar keamanan dan ketahanan data [6],[16]. Qofifah et al. (2026) menambahkan dimensi etika komunikasi organisasi dalam pengelolaan data pribadi sesuai UU PDP [20]. Meskipun beragam, kajian-kajian tersebut umumnya masih memisahkan dimensi hukum dan teknis, atau hanya berfokus pada satu dimensi tanpa mengintegrasikan keduanya secara sistematis. Belum ada studi yang secara komprehensif memetakan gap teknis UU PDP menggunakan kasus-kasus insiden nyata terbaru (2025–2026) yang mencakup tiga dimensi berbeda *(social engineering, insider abuse, technical breach)* secara bersamaan. Artikel ini mengisi celah tersebut dengan pendekatan analisis kesenjangan regulatif-teknis yang didukung bukti kasus insiden empiris.

III. METODE PENELITIAN

A. Jenis dan Pendekatan Penelitian

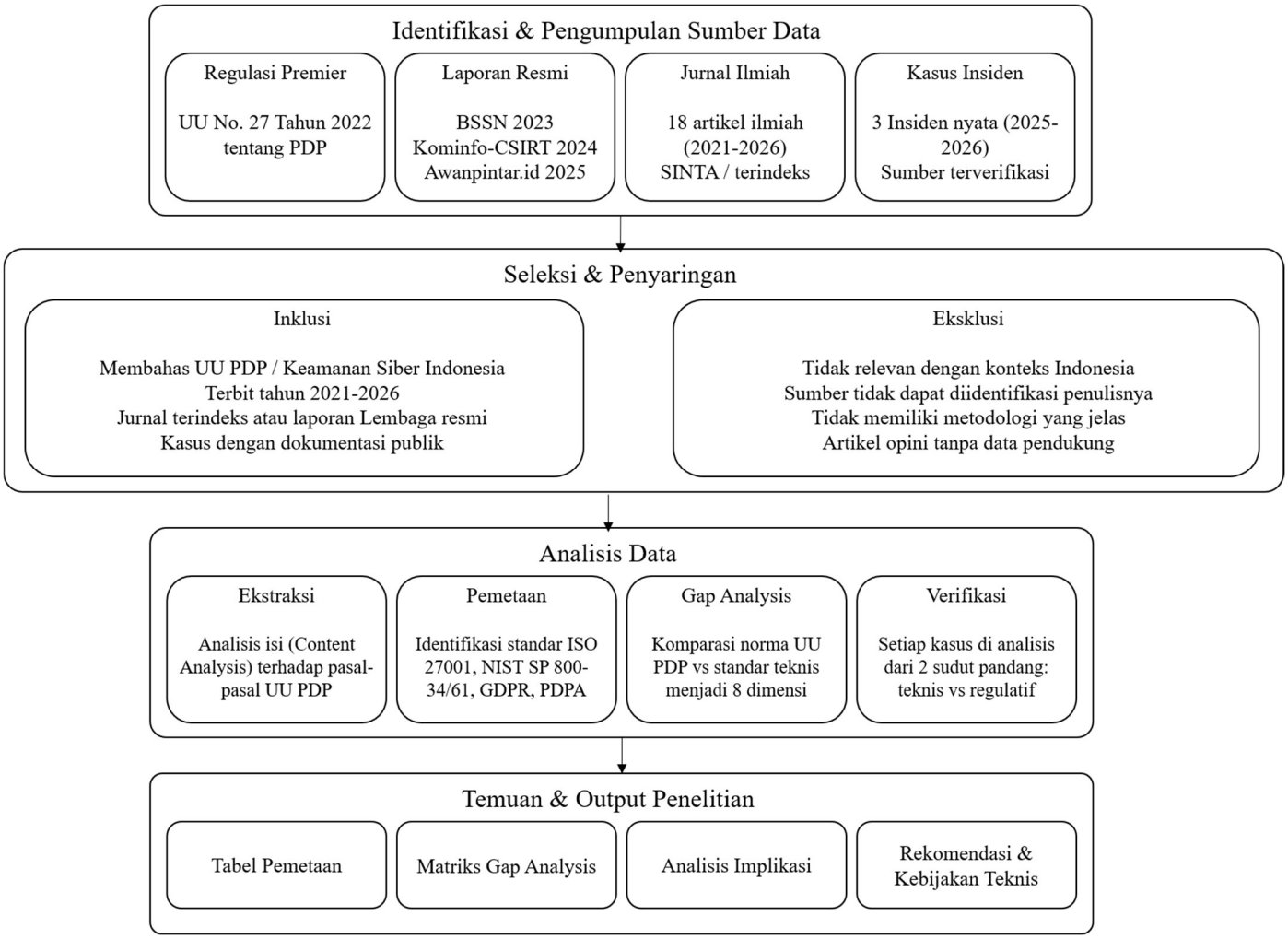
Penelitian ini menggunakan pendekatan kualitatif deskriptif-analitis, yaitu pendekatan yang bertujuan menggambarkan dan menganalisis fenomena secara mendalam berdasarkan data yang dikumpulkan dari sumber-sumber sekunder yang relevan [18]. Pendekatan ini dipilih karena tujuan penelitian bukan untuk menguji hipotesis statistik, melainkan untuk memahami dan memetakan kesenjangan antara norma regulatif dan praktik teknis secara sistematis. Desain penelitian yang digunakan adalah narrative literature review yang dikombinasikan dengan analisis studi kasus sekunder. Kombinasi ini memungkinkan peneliti untuk membangun pemahaman teoritis melalui kajian literatur sekaligus memverifikasi temuan tersebut melalui bukti empiris dari insiden nyata yang terdokumentasi. Kerangka alur metode penelitian disajikan pada Gambar 1.

B. Sumber dan Pengumpulan Data

Data dalam penelitian ini bersumber dari dua kategori utama, yaitu sumber literatur dan sumber kasus insiden. Sumber literatur meliputi: (1) regulasi primer berupa UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi [1]; (2) laporan resmi lembaga pemerintah, yaitu Laporan Lanskap Keamanan Siber Indonesia 2023 dari BSSN [2], Laporan Tahunan Kamsiber Kominfo-CSIRT 2024 [4], dan Laporan Ancaman Digital Semester 1 Tahun 2025 dari AwanPintar.id [3]; serta (3) artikel jurnal ilmiah yang relevan terbit pada rentang 2021-2026 [5]-[21]. Sumber kasus insiden mencakup tiga insiden penyalahgunaan data yang terjadi pada periode 2025-2026 dan bersumber dari laporan resmi pemerintah serta media berita yang terverifikasi [22]-[24]. Penelusuran literatur dilakukan menggunakan kata kunci utama antara lain "UU PDP", "perlindungan data pribadi", "keamanan siber Indonesia", "data breach", "personal data protection law", dan "cybersecurity regulation" pada basis data Google Scholar, Garuda, SINTA, dan jurnal terindeks nasional. Seluruh sumber yang ditemukan kemudian disaring berdasarkan kriteria inklusi yang telah ditetapkan.

C. Kriteria Seleksi Sumber

Untuk menjaga validitas dan relevansi data, diterapkan kriteria inklusi dan eksklusi. Kriteria inklusi meliputi: (1) membahas secara langsung topik UU PDP, perlindungan data pribadi, atau keamanan siber dalam konteks Indonesia; (2) diterbitkan antara tahun 2021 hingga 2026; (3) berasal dari jurnal ilmiah terindeks, laporan lembaga resmi pemerintah atau badan internasional yang terpercaya, atau media berita kredibel untuk sumber kasus insiden. Kriteria eksklusi meliputi: (1) artikel yang hanya membahas perlindungan data di luar konteks Indonesia tanpa relevansi komparatif; (2) sumber yang tidak dapat diidentifikasi asal lembaga atau penulisnya; (3) artikel tanpa metodologi yang jelas atau berasal dari sumber yang tidak dapat diverifikasi.



Gambar 1. Kerangka Alur Metode Penelitian

D. Teknik Analisis Data

Analisis data dilakukan menggunakan dua teknik utama yang diterapkan secara bertahap. Pertama, analisis isi (content analysis) digunakan untuk mengidentifikasi dan mengekstrak ketentuan-ketentuan UU PDP yang memiliki implikasi teknis, serta mengidentifikasi standar keamanan internasional yang relevan sebagai pembanding. Kedua, analisis kesenjangan (gap analysis) digunakan untuk memetakan perbedaan antara kewajiban normatif UU PDP dengan standar teknis yang seharusnya ada, lalu memverifikasi kesenjangan tersebut melalui tiga studi kasus insiden nyata.

Secara operasional, analisis dilaksanakan dalam empat tahap berurutan. Tahap pertama adalah identifikasi dan ekstraksi pasal-pasal UU PDP yang mengandung dimensi teknis keamanan data. Tahap kedua adalah pemetaan standar teknis internasional yang relevan (ISO/IEC 27001, ISO/IEC 27701, NIST SP 800-34, NIST SP 800-61) dan komparasi dengan GDPR serta PDPA Singapura. Tahap ketiga adalah sintesis kesenjangan antara ketentuan normatif dan standar teknis, yang dituangkan dalam matriks analisis kesenjangan. Tahap keempat adalah verifikasi empiris kesenjangan melalui analisis tiga kasus insiden nyata (2025-2026), di mana setiap kasus dianalisis dari dua sudut secara bersamaan: teknis (kegagalan kontrol keamanan) dan regulatif (celah UU PDP).

E. Keterbatasan Penelitian

Penelitian ini memiliki keterbatasan yang perlu diakui secara transparan. Karena seluruh data bersumber dari dokumen sekunder, temuan yang dihasilkan tidak merepresentasikan pengukuran langsung atas tingkat kepatuhan teknis pengendali data di lapangan. Tidak dilakukan wawancara dengan praktisi keamanan siber atau pengendali data, sehingga perspektif implementatif dari pelaku industri belum tercakup. Selain itu, tiga kasus insiden yang digunakan sebagai studi kasus dipilih berdasarkan ketersediaan dokumentasi publik yang memadai, sehingga tidak bersifat representatif secara statistik terhadap seluruh insiden kebocoran data yang terjadi di Indonesia. Penelitian lanjutan dengan metode survei atau wawancara mendalam disarankan untuk melengkapi temuan ini secara empiris.

IV. HASIL DAN PEMBAHASAN

A. Pemetaan Ketentuan Teknis UU PDP

Analisis terhadap UU PDP No. 27 Tahun 2022 menunjukkan bahwa undang-undang ini sudah menetapkan prinsip-prinsip perlindungan data yang sejalan dengan praktik internasional, namun masih bersifat prinsipil dan belum preskriptif secara teknis. Pasal 35 mewajibkan "langkah teknis yang layak" tanpa mendefinisikan tolok ukur teknis yang terukur. Pasal 46 mewajibkan notifikasi dalam 3×24 jam namun tidak mengatur prosedur teknis incident response. Pasal 47 menegaskan akuntabilitas namun tanpa mewajibkan audit keamanan independen secara berkala [1]. Kondisi ini berbeda dengan GDPR Pasal 32 yang secara eksplisit menyebut enkripsi, pseudonymisasi, dan mekanisme pemulihan data sebagai langkah teknis yang harus dipertimbangkan [8].

Tabel 2**.** Pemetaan Pasal UU PDP terhadap Dimensi Teknis dan Standar Internasional

Pasal	**Ketentuan Normatif**	**Implikasi Teknis**	**Standar Relevan**	**Status**
Ps. 20	Dasar pemrosesan: consent & tujuan sah	Consent management system, purpose limitation	ISO 27701	Prinsipil, tidak preskriptif
Ps. 35	Langkah teknis pengamanan data	Enkripsi, access control, patch mgmt, backup	ISO 27001, NIST SP 800-34	Prinsipil, tidak preskriptif
Ps. 39	Keamanan dari gangguan & kerusakan	RTO/RPO, DRP, data resilience	ISO 27040, NIST SP 800-34	Prinsipil, tidak preskriptif
Ps. 46	Notifikasi pelanggaran ≤3×24 jam	Incident response plan, SIEM, forensik digital	ISO 27035, NIST SP 800-61	Prinsipil, tidak preskriptif
Ps. 47	Akuntabilitas pengendali data	Audit log, dokumentasi pemrosesan, DPO	ISO 27001 Annex A	Prinsipil, tidak preskriptif

B. Analisis Studi Kasus: Tiga Dimensi Kesenjangan

Kasus 1 adalah Love Scam Jakarta Selatan: *Social Engineering* dan Pencurian Identitas Digital. Pada Januari 2026, seorang ibu rumah tangga berusia 54 tahun di Jakarta Selatan menjadi korban penipuan asmara daring. Penipu mencatut foto dan identitas seorang Aiptu aktif Polda Metro Jaya untuk membangun persona palsu di media sosial, lalu membangun kepercayaan korban selama berbulan-bulan sebelum berhasil menguras Rp250 juta melalui berbagai kedok biaya. Penipuan terbongkar saat korban secara tidak sengaja bertemu pemilik foto asli. Kasus dilaporkan ke Unit Siber Polda Metro Jaya dan diverifikasi oleh Cyberity Network. Bareskrim Polri mencatat bahwa romance scam meningkat 32% pada semester I 2026, dengan 60% korban adalah perempuan usia paruh baya hingga lansia [22].

Dari perspektif teknis, kasus ini mengekspos celah berupa ketiadaan mekanisme verifikasi identitas digital yang kuat di platform media sosial. Identitas seseorang seperti nama, foto, afiliasi institusi, dapat dengan mudah direplikasi tanpa kontrol teknis pencegahan. UU PDP tidak mengatur kewajiban platform untuk menerapkan reverse image search terintegrasi, verifikasi akun berbasis dokumen, atau deteksi akun duplikasi berbasis AI. Harahap dan Sazali (2026) menegaskan bahwa platform digital di Indonesia belum sepenuhnya menerapkan langkah-langkah teknis preventif yang sesuai prinsip UU PDP [12]. Gap ini juga bersinggungan dengan ketiadaan regulasi yang mengatur tanggung jawab platform atas penyalahgunaan identitas pihak ketiga, berbeda dengan GDPR yang mengatur *data controller obligations* secara lebih luas [8].

Kasus 2 adalah KUR Fiktif BNI Jember: *Insider Abuse* dan Penyalahgunaan Data Identitas. Selama 2021–2023, mantan Pemimpin Cabang BNI Jember (MFH) dan dua *collection agent* (AM, IIS) menyalahgunakan data KTP dan Kartu Keluarga sekitar 900 petani tanpa sepengetahuan mereka untuk mengajukan kredit fiktif. Proses verifikasi diloloskan secara tidak sah. Dana KUR yang seharusnya diterima petani justru dikuasai para tersangka. Kerugian negara dikonfirmasi BPKP Jawa Timur sebesar Rp41.487.138.481. Ratusan petani terancam masuk *blacklist* SLIK meski tidak pernah meminjam [23].

Kasus ini menunjukkan tiga kegagalan teknis simultan: (1) tidak adanya *role-based access control* (RBAC) yang ketat yang mencegah satu orang meloloskan seluruh proses verifikasi; (2) tidak adanya sistem deteksi anomali untuk mendeteksi pengajuan kredit massal dengan pola data serupa; (3) lemahnya *audit trail* internal yang seharusnya dapat mendeteksi pola penyimpangan sejak dini. UU PDP mewajibkan *purpose limitation* dan *consent* (Pasal 20), namun tidak menetapkan standar teknis minimum untuk kontrol akses dan verifikasi data di institusi keuangan. Sihombing et al. (2026) menegaskan bahwa mekanisme penegakan hukum perlindungan data masih

lemah dan konsumen sulit mengakses keadilan ketika haknya dilanggar [14]. Hal ini relevan langsung dengan kondisi 900 petani yang data pribadinya disalahgunakan tanpa adanya mekanisme perlindungan yang efektif.

Kasus 3 adalah Bobol Dinsos Jateng: *Technical Breach* Akibat *Unpatched Vulnerability*. Sejak April 2025, seorang teknisi ponsel berinisial RN berhasil membobol situs Dinas Sosial Provinsi Jawa Tengah dan mencuri 1.239.573 data NIK dan KK warga dengan mengeksploitasi *unpatched vulnerability*. Fakta bahwa pelaku bukan peretas profesional menjadi indikator kuat betapa rendahnya baseline keamanan teknis yang diterapkan pada sistem pemerintah yang menyimpan jutaan data kependudukan [24].

BSSN mengonfirmasi melalui ITSA terhadap 586 sistem elektronik bahwa ditemukan 2.860 celah keamanan, dengan jenis risiko Critical tertinggi adalah IDOR [2]. Ini menunjukkan bahwa kerentanan sistem bukan kasus individual melainkan fenomena sistemik. UU PDP Pasal 35 mewajibkan "pengamanan yang layak", namun tanpa definisi teknis terukur, tidak ada kewajiban *patch management* berkala, dan tidak ada standar minimum keamanan untuk sistem pemerintah yang menyimpan data kependudukan. Mongan (2026) menegaskan bahwa kesenjangan kapasitas pengawasan merupakan salah satu hambatan utama dalam implementasi UU PDP [17]. Rinjani dan Firmansyah (2025) menambahkan bahwa ketiadaan lembaga pengawas independen menyebabkan penegakan hukum tidak efektif dan akuntabilitas makin lemah [8].

C. Pola Sistemik di Balik Tiga Kasus

Meskipun ketiga kasus memiliki modus yang berbeda, terdapat pola sistemik yang menyatukan ketiganya. Pertama, semua kasus menunjukkan kegagalan pada lapisan pencegahan teknis (*preventive technical controls*), bukan hanya pada lapisan hukum. Kedua, data identitas kependudukan (NIK, KTP, KK) menjadi objek yang berulang kali menjadi sasaran, baik untuk penipuan identitas, kredit fiktif, maupun pencurian massal. Ketiga, lemahnya mekanisme deteksi (*detective controls*) menyebabkan semua kasus baru terungkap setelah kerugian terjadi, bukan dicegah sebelumnya. Keempat, dalam semua kasus, pelaku adalah non-profesional atau *insider*, bukan aktor negara atau peretas canggih, yang membuktikan bahwa ancaman nyata bukan hanya dari serangan teknis tingkat tinggi, melainkan juga dari kelemahan dasar (*basic security hygiene*) yang tidak ditangani. Pola ini konsisten dengan temuan Ghozi (2026) bahwa rendahnya kesadaran, kepatuhan pelaku usaha, dan kapasitas penegak hukum menjadi tiga hambatan utama efektivitas UU PDP [9].

D. Gap Analysis Matrix

Tabel 3. Matriks Analisis Kesenjangan UU PDP vs Praktik Teknis Keamanan Siber

No	Dimensi Gap	Ketentuan Ada	Standar/Regulasi yang Dibutuhkan	Kasus Pembuktian	Urgensi
1	Standar teknis minimum pengamanan	Ps. 35: "langkah layak"	ISO 27001, patch wajib, VAPT berkala	Kasus 3	Tinggi
2	Verifikasi identitas digital di platform	Tidak diatur	KYC digital, deteksi duplikasi akun	Kasus 1	Tinggi
3	Kontrol akses & audit insider threat	Ps. 20: consent, purpose	RBAC, audit trail, anomaly detection	Kasus 2	Tinggi
4	Kewajiban patch management berkala	Tidak diatur	Manajemen CVE, update SOP berkala	Kasus 3	Tinggi
5	Lembaga pengawas independen aktif	Ps. 47: amanat BPDP	BPDP dgn kapasitas audit teknis	Semua kasus	Sangat Tinggi
6	Standar teknis notifikasi insiden	Ps. 46: notifikasi 3×24 jam	IRP, SIEM, forensik digital wajib	Kasus 2, 3	Sedang
7	Kewajiban DPIA untuk sistem berisiko	Tidak diatur	DPIA wajib seperti GDPR Ps. 35	Kasus 3	Sedang
8	Regulasi tanggung jawab platform	Ps. 35 umum	Kewajiban teknis spesifik per sektor	Kasus 1, 2	Tinggi

E. Implikasi Multidimensi Kesenjangan

Kesenjangan yang teridentifikasi menimbulkan implikasi berlapis. Bagi subjek data, ketiadaan standar teknis minimum berarti hak privasi yang dijamin UU PDP belum terlindungi secara efektif. Data kependudukan jutaan warga dapat bocor akibat kerentanan yang seharusnya dapat dicegah, dan identitas dapat disalahgunakan sebagai instrumen kejahatan finansial tanpa mekanisme perlindungan yang memadai [7],[13]. Lestari (2026) menemukan bahwa kebijakan *platform* digital umumnya masih disusun secara umum dan belum sepenuhnya mencerminkan prinsip perlindungan data sebagaimana UU PDP amanatkan [13].

Bagi pengendali data, ketidakjelasan standar teknis menciptakan ketidakpastian kepatuhan. Tanpa patokan yang terukur, organisasi cenderung melakukan *formal compliance*, memenuhi persyaratan administratif tanpa memastikan ketahanan operasional yang nyata. Putra dan Noriansyah (2026) menemukan bahwa banyak organisasi di sektor publik belum memahami prinsip *data protection* secara substantif [5]. Kondisi ini diperparah oleh belum tersedianya panduan teknis operasional yang mudah diterapkan khususnya oleh UMKM [9]. Jika dibandingkan dengan JOLENS (2025) yang mencatat kasus Equifax 2017, di mana lemahnya kepatuhan teknis terhadap patch yang tersedia menyebabkan kebocoran 147 juta data, kesamaan pola dengan kasus Dinsos Jateng sangat mencolok [21].

Bagi penegakan hukum, ketiadaan standar teknis eksplisit mempersulit pembuktian apakah pengendali data telah memenuhi kewajiban "pengamanan yang layak". Tanpa referensi teknis yang jelas, sulit membuktikan negligence secara hukum. Hal ini diperparah oleh belum aktifnya BPDP, sehingga korban kebocoran data tidak memiliki saluran pengaduan yang jelas [8]. Dalam konteks pemilu, hal serupa juga dibuktikan dari kasus pencatutan NIK/KTP di SIPOL KPU, di mana sistem digital penyelenggara pemilu belum menerapkan standar perlindungan data yang memadai meski UU PDP sudah ada [15]. Ramli (2026) mengingatkan bahwa ancaman berbasis AI yang semakin canggih, termasuk *deepfake* dan *automated social engineering*, akan memperparah kesenjangan ini jika regulasi teknis tidak segera diperkuat [11].

Secara makro, kesenjangan regulatif-teknis ini mengancam kepercayaan publik terhadap ekosistem digital nasional. Qofifah et al. (2026) menegaskan bahwa dalam era digital, etika komunikasi organisasi mengharuskan perlindungan data tidak hanya menjadi kewajiban legal-administratif, tetapi juga norma operasional yang diwujudkan dalam praktik nyata [20]. Sementara itu, Febriansyah et al. (2026) menekankan bahwa transformasi hukum digital harus disertai penguatan kapasitas institusional, harmonisasi regulasi, dan kerja sama internasional untuk mewujudkan ketahanan keamanan siber nasional yang berkelanjutan [10].

V. KESIMPULAN DAN REKOMENDASI

Penelitian ini menyimpulkan bahwa UU Perlindungan Data Pribadi No. 27 Tahun 2022 telah memberikan kerangka hukum yang penting secara prinsipil, namun terdapat kesenjangan signifikan antara ketentuan normatifnya dengan standar teknis keamanan siber yang diperlukan. Menjawab pertanyaan penelitian pertama, UU PDP memang memuat sejumlah pasal yang berimplikasi teknis (Pasal 20, 35, 39, 46, 47), namun seluruhnya bersifat prinsipil dan tidak mendefinisikan standar teknis minimum yang terukur, berbeda dari GDPR dan PDPA yang lebih preskriptif. Menjawab pertanyaan kedua, kesenjangan teridentifikasi pada delapan dimensi utama: standar teknis minimum, verifikasi identitas digital, kontrol akses internal, *patch management*, lembaga pengawas aktif, prosedur notifikasi teknis, DPIA, dan tanggung jawab *platform*. Menjawab pertanyaan ketiga, kesenjangan ini terbukti dari tiga insiden nyata yang mencakup *social engineering, insider abuse,* dan *technical breach,* yang semuanya berhasil dilakukan bukan oleh aktor canggih, melainkan karena lemahnya *baseline* keamanan.

Berdasarkan temuan tersebut, direkomendasikan: Pertama, pemerintah segera menerbitkan regulasi turunan teknis UU PDP yang menetapkan standar minimum pengamanan dengan mengacu pada ISO/IEC 27001 dan NIST SP 800-34. Kedua, mewajibkan seluruh penyelenggara sistem elektronik yang memproses data pribadi melakukan *vulnerability assessment* dan *penetration testing* berkala serta menerapkan patch management terjadwal. Ketiga, mempercepat pembentukan BPDP yang independen dengan kapasitas audit teknis yang memadai. Keempat, mengatur kewajiban *platform* media sosial untuk menerapkan mekanisme verifikasi identitas digital guna mencegah pencatutan identitas. Kelima, mengadopsi DPIA sebagai kewajiban bagi sistem yang memproses data pribadi dalam jumlah besar atau kategori sensitif, mengikuti model GDPR. Keenam, mengalokasikan program peningkatan literasi keamanan data bagi organisasi pengelola data publik, khususnya di tingkat pemerintah daerah. Penelitian lanjutan disarankan menggunakan metode empiris dengan survei atau wawancara praktisi keamanan siber untuk mengukur secara kuantitatif tingkat kepatuhan teknis pengendali data di Indonesia.

Referensi

[1] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara RI Tahun 2022 Nomor 196, 2022.
[2] Badan Siber dan Sandi Negara (BSSN), "Lanskap Keamanan Siber Indonesia 2023," Direktorat Operasi Keamanan Siber, BSSN, Jakarta, 2023.
[3] AwanPintar.id, "Laporan Ancaman Digital di Indonesia Semester 1 Tahun 2025," AwanPintar.id, 2025.

[4] Kominfo-CSIRT, "Laporan Tahunan Keamanan Siber Kementerian Komunikasi dan Digital 2024," Kementerian Komunikasi dan Digital RI, Jakarta, 2024.
[5] J. M. Putra dan A. G. P. Noriansyah, "Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia: Antara Kepastian Hukum dan Realitas Praktik," J-DIKUMSI: Jurnal Pendidikan, Hukum, Komunikasi, vol. 2, no. 1, hal. 63–69, Mar. 2026.
[6] L. B. Lie dan A. Fitriyantica, "Mewujudkan Ketahanan dan Kepatuhan Data di Era Digital: Harmonisasi Strategi Backup 3-2-1 dengan Regulasi Keamanan Siber dan Pelindungan Data Pribadi di Indonesia," IBLAM Law Review, vol. 6, no. 1, Jan. 2026, doi: 10.52249/ilr.v6i1.657.
[7] M. I. A. Maulana, N. P. R. Yuliartini, dan D. G. S. Mangku, "Evaluasi Implementasi Undang-Undang Perlindungan Data Pribadi pada Kasus Kebocoran Data Pengguna E-Commerce di Indonesia," Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora, vol. 3, no. 2, hal. 41–51, Apr. 2026, doi: 10.62383/humif.v3i2.2980.
[8] M. A. Rinjani dan R. Firmansyah, "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia," Jurnal Analisis Hukum, vol. 8, no. 1, hal. 70–83, 2025, doi: 10.38043/jah.v8i1.6793.
[9] Ghozi, "Efektivitas Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam Mencegah Kebocoran Data di Era Digital," JUSTICES: Journal of Law, vol. 5, no. 1, 2026.
[10] F. I. Febriansyah, A. Ikhwan, U. S. Firdausi, dan A. D. Anggoro, "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity," International Journal Law and Society, vol. 5, no. 1, 2026.
[11] A. M. Ramli, "The Urgency of Regulating Artificial Intelligence in Relation to Cybersecurity and Cyber Resilience," Cogent Social Sciences, vol. 12, no. 1, 2026, doi: 10.1080/23311886.2026.2632977.
[12] A. Harahap dan H. Sazali, "Kebijakan Proteksi Data Pribadi dalam Platform Digital: Studi Kasus Implementasi Peraturan Perlindungan Data di Indonesia," FIKRUNA: Jurnal Ilmiah Kependidikan dan Kemasyarakatan, vol. 8, no. 1, hal. 1–17, Jan.–Mar. 2026.
[13] C. R. Lestari, "Analisis Kepatuhan Pengelolaan Data Pribadi Pengguna terhadap Undang-Undang Perlindungan Data Pribadi pada Platform Digital," Adagium: Jurnal Ilmiah Hukum, vol. 4, no. 1, hal. 152–167, 2026.
[14] P. Sihombing, W. S. Widiarty, dan B. Nadapdap, "Perlindungan Hukum Terhadap Data Pribadi Konsumen dalam Transaksi E-Commerce di Indonesia," Jurnal Sosial dan Teknologi (SOSTECH), vol. 6, no. 1, hal. 373–382, Jan. 2026, doi: 10.59188/jurnalsostech.v6i1.32627.
[15] G. F. Simanjuntak, N. A. Tobing, N. C. Tamba, dan J. R. Saragih, "Politik Hukum Pengawasan Data Pribadi dalam Pemilu: Analisis Kasus Pencatatan NIK/KTP di SIPOL dan Tantangan Implementasi UU PDP untuk Integritas Demokrasi," JIPM: Jurnal Ilmu Pemerintahan, vol. 4, no. 1, hal. 709–717, Feb. 2026.
[16] R. Rambe dan M. T. Kurniawan, "Cybersecurity Policies Differences in Indonesia: A Systematic Literature Review of Public and Private Sector," Elkawnie: Journal of Islamic Science and Technology, vol. 12, no. 1, Jun. 2026, doi: 10.22373/ekw.v12i1.31730.
[17] D. C. Mongan, "Efektivitas Undang-Undang Perlindungan Data Pribadi dalam Mengatur Praktik Pengumpulan Data oleh Platform Digital," Lex Technologia: Jurnal Hukum dan Masyarakat Digital, vol. 1, no. 1, hal. 1–10, Apr. 2026.
[18] S. A. Puspita, K. Septia, Sirojul Haq, dan D. P. Dwipayana, "Efektivitas Regulasi Perlindungan Data Pribadi dalam Sistem Teknologi Informasi di Indonesia," Jurnal Kajian Hukum dan Kebijakan Publik, vol. 4, no. 1, hal. 51–58, Jul.–Des. 2026.
[19] W. D. Cahyani dan A. Marianata, "Analisis Kebijakan Perlindungan Data Pribadi di Indonesia," Jurnal Kajian Hukum dan Kebijakan Publik, vol. 2, no. 1, hal. 623–626, Jul.–Des. 2024.
[20] W. I. Qofifah et al., "Organizational Communication Ethics and Personal Data Protection: The Legal Framework of Law Number 27 of 2022," vol. 2, no. 1, hal. 47–63, Jan. 2026.
[21] T. G. Laksana, "An Illustrative Analysis that Underscores the Significance of Legislation about the Safeguarding of Personal Data in Combating Cybercrime," Journal of Law, Economics, and Engineering (JOLENS), vol. 1, no. 2, hal. 48–59, 2025.
[22] T. L. Tirani dan P. Suwarno, "Ibu Ini Jual Mobil untuk Transfer Rp250 Juta Pria Dalam Love Scam," Swarajombang.com, 13 Jul. 2026. [Online]. Tersedia: https://swarajombang.com/ibu-ini-jual-mobil-untuk-transfer-rp250-juta-pria-dalam-love-scam/
[23] Kejaksaan Tinggi Jawa Timur, "Kejati Jatim Tetapkan Tiga Tersangka Korupsi Penyaluran KUR Mikro BNI Cabang Jember, Kerugian Negara Capai Rp41,48 Miliar," kejati-jatim.go.id, 9 Jul. 2026. [Online]. Tersedia: https://kejati-jatim.go.id/kejati-jatim-tetapkan-tiga-tersangka-korupsi-penyaluran-kur-mikro-bni-cabang-jember-kerugian-negara-capai-rp4148-miliar/
[24] R. Ridho dan I. Rastika, "Teknisi HP Bobol Situs Dinsos Jateng, Curi 1,2 Juta Data NIK dan KK," Kompas.com, 2 Jul. 2026. [Online]. Tersedia: https://regional.kompas.com/read/2026/07/02/170145078/teknisi-hp-bobol-situs-dinsos-jateng-curi-12-juta-data-nik-dan-kk-untuk?page=all