Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025)
Tema/Edisi : Hukum dan Hak Asasi Manusia (Bulan Kedua belas)
https://jhlg.rewangrencang.com/

IMPLEMENTASI REGULASI PERLINDUNGAN DATA PRIBADI DALAM LAYANAN DIGITAL DI INDONESIA: *A SYSTEMATIC REVIEW*

IMPLEMENTATION OF PERSONAL DATA PROTECTION REGULATIONS IN DIGITAL SERVICES IN INDONESIA: A SYSTEMATIC REVIEW

Mardiman Sane, Hotman Sinambela, Rony Eli Hutahaean, Lamhot Hutahaean dan Lasbok Marbun

Fakultas Hukum Universitas Mpu Tantular

Korespondensi Penulis : mardimanshane@gmail.com, hotmanbertaok@gmail.com, hariararamos@gmail.com, lamhhutahaean@gmail.com, marbunlasbok@gmail.com

Citation Structure Recommendation :

Sane, Mardiman, Hotman Sinambela, Rony Eli Hutahaean, Lamhot Hutahaean dan Lasbok Marbun. *Implementasi Regulasi Perlindungan Data Pribadi dalam Layanan Digital di Indonesia: A Systematic Review*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2026).

ABSTRAK

Perkembangan layanan digital di Indonesia menimbulkan implikasi signifikan terhadap perlindungan data pribadi sebagai bagian dari hak atas privasi dan martabat manusia. Hak privasi menjadi prasyarat otonomi individu dalam negara hukum. Peningkatan pemanfaatan data mendorong lahirnya UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menggantikan rezim parsial UU ITE. Penelitian ini menggunakan Systematic Literature Review (SLR) dengan protokol PRISMA pada 30 jurnal nasional dan internasional (2018-2025) untuk mengkaji implementasi UU PDP, kasus kebocoran data, serta kesenjangan normatif dan praktik. Hasil menunjukkan UU PDP lebih komprehensif, namun implementasinya menghadapi kendala: literasi data rendah, kapasitas data controller terbatas, otoritas pengawas independen belum terbentuk, dan mekanisme penegakan lemah. Efektivitas perlindungan data memerlukan penguatan regulasi, lembaga pengawas independen, dan peningkatan kapasitas pemangku kepentingan.

Kata Kunci: Layanan Digital, Normative Gap, Perlindungan Data Pribadi, Regulatory Framework, UU PDP

ABSTRACT

The advancement of digital services in Indonesia has significant implications for personal data protection as an integral part of the right to privacy and human dignity. The right to privacy serves as a prerequisite for individual autonomy within a constitutional state (Rechtsstaat). The increasing utilization of data prompted the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which replaces the partial regime of the Electronic Information and Transactions (ITE) Law. This research employs a Systematic

Literature Review (SLR) using the PRISMA protocol on 30 national and international journals (2018–2025) to examine the implementation of the PDP Law, data breach cases, as well as normative and practical gaps. The results indicate that while the PDP Law is more comprehensive, its implementation faces several obstacles: low data literacy, limited capacity of data controllers, the absence of an independent supervisory authority, and weak enforcement mechanisms. Effective data protection requires regulatory strengthening, the establishment of an independent supervisory body, and capacity building for all stakeholders.
Keywords: Digital Services, Normative Gap, Personal Data Protection, Regulatory Framework, UU PDP

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah secara fundamental cara manusia berinteraksi, bertransaksi dan mengakses layanan publik. Di tengah arus transformasi digital yang masif, data pribadi individu menjadi sumber daya strategis yang diperebutkan oleh berbagai entitas—mulai dari korporasi multinasional hingga lembaga pemerintah. Fenomena ini memunculkan pertanyaan filosofis yang mendasar: sejauh mana negara bertanggung jawab untuk melindungi hak privasi warganya dalam ruang digital?

Secara filosofis, hak atas privasi bukan sekadar kepentingan individual yang bersifat residual, melainkan merupakan prasyarat fundamental bagi terwujudnya martabat manusia (*human dignity*) dan otonomi individu. Alan Westin mendefinisikan privasi sebagai hak individu, kelompok, atau institusi untuk menentukan sendiri kapan, bagaimana dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain.[1] Dalam perspektif ini, perlindungan data pribadi bukan hanya soal teknis-regulatoris, tetapi menyentuh inti dari gagasan tentang kebebasan manusia dalam negara modern. Shoshana Zuboff bahkan mengidentifikasi bahaya sistemik dari 'kapitalisme pengawasan' (*surveillance capitalism*) di mana data pribadi dieksploitasi sebagai komoditas oleh perusahaan-perusahaan teknologi tanpa persetujuan yang bermakna dari pemiliknya.[2]

Di Indonesia, Mahkamah Konstitusi telah mengakui hak atas privasi sebagai hak konstitusional yang dilindungi oleh Pasal 28G ayat (1) UUD 1945.[3]

[1] Alan Westin, *Privacy and Freedom*, Atheneum, New York, 1967, p.7.
[2] Shoshana Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, New York, 2019, p.63-67.
[3] Putusan Mahkamah Konstitusi Republik Indonesia No. 5/PUU-VIII/2010 tentang Hak atas Informasi dan Privasi sebagai Hak Konstitusional.

Pengakuan konstitusional ini meletakkan tanggung jawab positif kepada negara untuk mengambil langkah-langkah konkret dalam melindungi privasi warganya—termasuk di ruang digital. Dalam konteks teori negara hukum (*rechtsstaat*), negara tidak hanya wajib menghormati hak privasi secara pasif (*negative obligation*), tetapi juga berkewajiban aktif untuk menciptakan infrastruktur hukum yang mampu melindungi warganya dari pelanggaran privasi oleh pihak ketiga.[4]

Teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon membedakan antara perlindungan hukum preventif dan represif.[5] Perlindungan hukum preventif bertujuan mencegah terjadinya pelanggaran melalui pengaturan yang komprehensif, sementara perlindungan hukum represif bertujuan menyelesaikan pelanggaran yang telah terjadi melalui mekanisme penegakan hukum. Dalam konteks perlindungan data pribadi, kedua dimensi ini sama-sama krusial: regulasi yang kuat diperlukan untuk mencegah kebocoran data, sementara mekanisme sanksi yang efektif diperlukan untuk memulihkan hak-hak subjek data yang telah dilanggar. Satjipto Rahardjo lebih lanjut mengingatkan bahwa hukum yang baik tidak cukup sekadar ada dalam teks, tetapi harus hidup dalam praktik sosial (*law in action*).[6]

Di Indonesia, transformasi digital berkembang dengan pesat. Layanan digital yang mencakup perdagangan elektronik (e-commerce), layanan keuangan berbasis teknologi (fintech), layanan kesehatan digital, hingga sistem pemerintahan berbasis elektronik (e-government) telah menjadi bagian tak terpisahkan dari kehidupan masyarakat. Pemanfaatan layanan digital ini tidak dapat dilepaskan dari proses pengumpulan dan pemrosesan data pribadi dalam skala masif. Data pribadi—mulai dari nama, alamat, nomor identitas, data biometrik, hingga data kesehatan dan keuangan—menjadi komponen operasional yang fundamental dalam ekosistem digital.

Sebelum lahirnya UU PDP sendiri, rezim perlindungan data pribadi di Indonesia bergantung pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah beberapa kali diubah,

[4] Franz Magnis-Suseno, *Etika Politik: Prinsip-Prinsip Moral Dasar Kenegaraan Modern*, PT Gramedia, Jakarta, 1987, p.298-300.
[5] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat Indonesia*, Bina Ilmu, Surabaya, 1987, p.30.
[6] Satjipto Rahardjo, *Ilmu Hukum*, Citra Aditya Bakti, Bandung, 2014, p.53.

yang hanya mengatur aspek perlindungan data secara parsial dan tidak sistematis melalui Pasal 26.[7] Ketidaklengkapan rezim hukum inilah yang kemudian berkontribusi pada serangkaian kasus kebocoran data yang menimpa berbagai platform digital dan lembaga pemerintah di Indonesia. Data Badan Siber dan Sandi Negara (BSSN) mencatat lonjakan signifikan insiden siber yang berkaitan dengan kebocoran data pribadi dalam beberapa tahun terakhir, dengan Indonesia menjadi salah satu negara dengan tingkat insiden kebocoran data tertinggi di kawasan Asia Tenggara.[8]

Lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak bersejarah dalam sistem hukum nasional.[9] Untuk pertama kalinya, Indonesia memiliki regulasi *lex specialis* yang mengatur perlindungan data pribadi secara komprehensif, mencakup definisi data pribadi, hak-hak subjek data, kewajiban pengendali data (*data controller*) dan mekanisme penegakan hukum beserta sanksinya. Secara normatif, UU PDP dipandang sejalan dengan standar internasional seperti General Data Protection Regulation (GDPR) Uni Eropa, meskipun terdapat beberapa kesenjangan dalam aspek enforcement.[10]

Namun, keberadaan regulasi yang komprehensif secara normatif belum serta merta menjamin efektivitas perlindungan data pribadi dalam praktik. Berbagai penelitian menunjukkan adanya normative gap yang signifikan antara ketentuan UU PDP dan realitas implementasi di lapangan. Penyedia layanan digital—khususnya usaha kecil dan menengah—masih menghadapi kesulitan dalam menyesuaikan sistem dan kebijakan internal mereka dengan ketentuan UU PDP.

---

[7] Indonesia, *Undang-Undang tentang Informasi dan Transaksi Elektronik*, Pasal 26 UU No.11 Tahun 2008, LN Tahun 2008 No.58, TLN No.4843 sebagaimana diubah dengan UU No.19 Tahun 2016, LN Tahun 2016 No.251, TLN No.5952 dan UU No.1 Tahun 2024, LN Tahun 2024 No.1, TLN No.6905.

[8] Kementerian Komunikasi dan Digital Republik Indonesia, *Laporan Tahunan Kementerian Komunikasi dan Informatika 2021*, Kementerian Komunikasi dan Digital Republik Indonesia, Jakarta, 2022, p.45.

[9] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, Pasal 1 Angka 1 UU No.27 Tahun 2022, LN Tahun 2022 No.196, TLN No.6820.

[10] Risky Budiman, *The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022*, Jurnal Smart Hukum (JSH), Vol.2, No.1 (2023), p.24.

Di sisi lain, belum terbentuknya otoritas pengawas perlindungan data pribadi yang independen sebagaimana diamanatkan UU PDP menjadi hambatan struktural yang serius dalam penegakan regulatory framework yang ada.

Berdasarkan uraian di atas, terdapat kesenjangan penelitian (research gap) yang signifikan: pertama, minimnya kajian yang secara komprehensif menelaah evolusi regulasi perlindungan data dari rezim UU ITE menuju UU PDP beserta implikasinya; kedua, kurangnya analisis normatif terhadap kasus-kasus kebocoran data nyata dalam kaitannya dengan kewajiban pengendali data menurut UU PDP; dan ketiga, terbatasnya sintesis literatur sistematis yang mengkaji tren penelitian perlindungan data di Indonesia dalam rentang 2018–2025. Penelitian ini hadir untuk mengisi kesenjangan tersebut melalui pendekatan Systematic Literature Review (SLR) yang komprehensif.

Dengan demikian, penelitian ini bertujuan untuk: (1) menganalisis evolusi regulasi perlindungan data pribadi di Indonesia dari rezim UU ITE menuju UU PDP; (2) mengkaji kasus-kasus kebocoran data pada platform pemerintah dan implikasinya secara normatif berdasarkan kewajiban pengendali data menurut UU PDP; (3) mengidentifikasi normative gap antara ketentuan UU PDP dan praktik implementasi dalam layanan digital; serta (4) merumuskan rekomendasi normatif dan kebijakan untuk penguatan perlindungan data pribadi di Indonesia.

B. PEMBAHASAN

1. Metodologi: Systematic Literature Review dengan Protokol PRISMA

Penelitian ini menggunakan metode Systematic Literature Review (SLR) dengan protokol PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) sebagai panduan dalam identifikasi, seleksi dan sintesis literatur.[11] SLR dipilih karena kemampuannya untuk mengidentifikasi, mengevaluasi dan mensintesis semua bukti yang relevan dengan pertanyaan penelitian secara sistematis, transparan dan dapat direproduksi—sebuah pendekatan yang sangat relevan dalam kajian hukum yang bertujuan untuk memetakan lanskap regulasi dan penelitian secara komprehensif.

[11] Muhammad Gustryan dan Zainal Arifin Hoesein, *Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital*, Jurnal Minfo Polgan, Vol.14, No.2 (2025), p.301.

Pencarian literatur dilakukan pada basis data bereputasi internasional dan nasional, meliputi: Scopus, Web of Science, Google Scholar dan portal jurnal nasional terakreditasi Sinta. Kata kunci yang digunakan meliputi kombinasi dari: 'perlindungan data pribadi', 'personal data protection', 'UU PDP', 'UU ITE', 'data breach Indonesia', 'privacy regulation Indonesia', 'digital services data protection' dan 'cybersecurity Indonesia'. Rentang waktu pencarian dibatasi pada 2018–2025 untuk mencakup periode pra-UU PDP (di bawah rezim UU ITE) hingga pasca-enactment UU PDP, sehingga memungkinkan analisis evolusi regulasi secara longitudinal.

Kriteria inklusi meliputi: (1) artikel yang membahas perlindungan data pribadi atau privasi digital di Indonesia; (2) diterbitkan dalam jurnal ilmiah nasional terakreditasi (minimal Sinta 2) atau jurnal internasional terindeks Scopus/Web of Science; (3) diterbitkan dalam rentang 2018–2025; dan (4) tersedia dalam bahasa Indonesia atau Inggris. Kriteria eksklusi meliputi: (1) artikel yang tidak membahas konteks Indonesia secara spesifik; (2) artikel tanpa peer-review; dan (3) artikel yang teridentifikasi sebagai duplikasi. Berdasarkan proses seleksi bertahap tersebut, diperoleh 30 artikel ilmiah yang memenuhi kriteria dan dianalisis secara mendalam.

Tabel 1. Penelitian Terdahulu: Pemetaan Literatur Perlindungan Data Pribadi di Indonesia (2018–2025)

No.	Penulis dan Tahun	Fokus Penelitian	Metode	Temuan Utama	Relevansi
1	Suryanto dan Nugroho (2021)	Keamanan data pribadi dalam layanan digital berbasis UU ITE	Kualitatif-Normatif	UU ITE Pasal 26 tidak komprehensif; tidak ada sanksi efektif bagi pelanggaran data di platform digital	Normative gap pra-UU PDP
2	Khansa (2021)	Urgensi otoritas pengawas independen dalam pelindungan data pribadi	Normatif	Indonesia belum memiliki lembaga pengawas independen; pengawasan tersebar di berbagai kementerian	Penguatan institutional framework
3	Disemadi (2021)	Regulasi AI dan perlindungan data pribadi	Yuridis-Normatif	Belum ada regulasi AI khusus; kekosongan hukum menimbulkan risiko penyalahgunaan data oleh sistem AI	Identifikasi regulatory gap berbasis teknologi
4	Nugroho, Pratiwi dan Zahro (2021)	Kebocoran data dan solusi teknologi	Yuridis-Empiris	Kebocoran data BPJS Kesehatan menunjukkan lemahnya	Analisis kasus kebocoran data pemerintah

No.	Penulis dan Tahun	Fokus Penelitian	Metode	Temuan Utama	Relevansi
		blockchain		sistem keamanan; blockchain menawarkan solusi pengamanan berbasis desentralisasi	
5	Kusnadi (2021)	Data pribadi sebagai hak privasi	Filosofis-Normatif	Perlindungan data merupakan bagian dari hak privasi yang dijamin konstitusi; diperlukan regulasi komprehensif bersifat lex specialis	Dasar filosofis dan konstitusional artikel ini
6	Nurmalasari (2021)	Urgensi pengesahan RUU PDP	Normatif	Ketiadaan UU PDP menimbulkan ketidakpastian hukum; Indonesia tertinggal dibanding negara ASEAN dalam regulasi perlindungan data	Historical gap sebelum UU PDP
7	Rahmawati (2022)	Kesadaran privasi pengguna digital	Survei-Kuantitatif	Literasi perlindungan data pengguna digital masih sangat rendah (di bawah 30%); mayoritas pengguna tidak mengetahui hak-hak mereka sebagai subjek data	Justifikasi empiris kebutuhan edukasi publik
8	Badar, Fauzi dan Jazuli (2023)	Kebijakan UU PDP perspektif hukum positif dan Islam	Normatif-Komparatif	UU PDP sejalan dengan prinsip perlindungan martabat dalam hukum Islam; implementasinya masih butuh penguatan sanksi	Analisis multi-perspektif regulasi PDP
9	Ardika (2023/2025)	Perlindungan data dalam e-commerce: kasus kebocoran data	Studi Kasus	Kebocoran data e-commerce akibat lemahnya enkripsi dan tidak adanya audit keamanan berkala; korban tidak memiliki mekanisme ganti rugi memadai	Basis analisis kasus empiris e-commerce
10	Budiman (2023)	Perkembangan hukum PDP Indonesia pasca UU No. 27/2022	Normatif-Komparatif	UU PDP sejalan dengan GDPR namun lemah dalam aspek enforcement; diperlukan penguatan kelembagaan pengawas	Komparasi UU PDP dengan standar internasional
11	Matheus dan Gunadi (2023)	Pembentukan lembaga pengawas PDP	Normatif-Komparatif	Efektivitas lembaga pengawas bergantung pada independensi struktural dan kapasitas investigasi yang memadai	Desain kelembagaan pengawasan PDP
12	Heriyanto (2023)	Komparasi regulasi privasi data pasien: Indonesia,	Komparatif-Normatif	Indonesia masih tertinggal dibanding Singapura dalam enforcement dan	Benchmark komparatif regional

No.	Penulis dan Tahun	Fokus Penelitian	Metode	Temuan Utama	Relevansi
		Singapura, Laos		kelengkapan regulasi; Laos belum memiliki regulasi khusus	
13	Admiral dan Pauck (2023)	Fintech dan pelanggaran perlindungan data pengguna	Studi Kasus-Kualitatif	Pinjaman online ilegal menjadi modus pelanggaran data masif; tidak ada sanksi deterren efektif di bawah rezim UU ITE	Pemetaan sektor risiko pelanggaran tinggi
14	Mipon dan Putra (2023)	Perlindungan data oleh notaris berdasarkan UU PDP	Normatif	Notaris sebagai pengendali data wajib menerapkan prinsip kerahasiaan dan keamanan data sebagaimana UU PDP	Aplikasi UU PDP pada profesi hukum
15	Hidayat dan Putri (2023)	Regulasi data pribadi pasca UU PDP	Normatif	UU PDP sudah komprehensif secara normatif namun perlu peraturan pelaksana lebih detail dan pembentukan otoritas pengawas	Evaluasi kesiapan normatif UU PDP
16	Natamiharja dan Setiawan (2024)	Komparasi strategi perlindungan data Indonesia dan Prancis	Komparatif-Yuridis	Prancis melalui CNIL memiliki mekanisme enforcement jauh lebih kuat; Indonesia perlu belajar dari model lembaga pengawas independen	Model kelembagaan berbasis perbandingan
17	Afifah (2024)	Tanggung jawab hukum e-commerce dalam keamanan data	Normatif	UU PDP 2022 memperkuat tanggung jawab data controller; platform e-commerce wajib memenuhi prinsip keamanan data dan bertanggung jawab atas pelanggaran	Analisis tanggung jawab pengendali data
18	Kurdi dan Cahyono (2024)	Perlindungan data pribadi berdasarkan UU No. 27/2022	Yuridis-Normatif	UU PDP memberikan kerangka hukum lebih komprehensif namun perlu harmonisasi dengan peraturan sektoral yang ada	Analisis komprehensif UU PDP
19	Kurniawan, dkk. (2024)	Sanksi pidana dan perlindungan data pribadi	Normatif-Empiris	Sanksi pidana UU PDP bersifat deterren namun belum optimal karena keterbatasan kapasitas aparat penegak hukum	Evaluasi efektivitas sanksi UU PDP
20	Prasanti dan Gunadi (2025)	Prinsip necessity dan proportionality dalam berbagi data nasabah	Normatif	Berbagi data nasabah bank dengan vendor harus memenuhi prinsip kebutuhan dan proporsionalitas; pelanggaran merupakan normative gap serius	Aplikasi prinsip-prinsip UU PDP dalam praktik

No.	Penulis dan Tahun	Fokus Penelitian	Metode	Temuan Utama	Relevansi
21	Abdullah, Durand dan Moonti (2025)	Transformasi digital dan hak privasi di era Big Data	Kritis-Normatif	Era big data mengintensifkan risiko pelanggaran privasi; UU PDP belum cukup mengakomodasi tantangan big data analytics dan profiling	Relevansi UU PDP dalam konteks big data
22	Ahmad, Puspaningtyas dan Pankratev (2025)	Perlindungan hukum privasi data di era digital	Normatif-Komparatif	Terdapat kesenjangan antara norma hukum dan praktik perlindungan data; diperlukan penguatan mekanisme audit dan sertifikasi keamanan data	Pemetaan normative gap dalam implementasi
23	Ardana, Akbar dan Martadireja (2025)	Systematic Literature Review metode PRISMA	SLR-PRISMA	Metode SLR dengan PRISMA terbukti efektif untuk mengidentifikasi tren penelitian dan research gap secara sistematis	Justifikasi metodologis penelitian ini
24	Gustryan dan Hoesein (2025)	Peran UU ITE dan UU PDP dalam perlindungan data	Komparatif-Normatif	UU PDP menggantikan fungsi perlindungan data parsial dalam UU ITE; terdapat pergeseran paradigma dari pendekatan sektoral ke komprehensif	Analisis evolusi regulasi PDP di Indonesia
25	Nurmansyah, Natamiharja dan Setiawan (2025)	Perlindungan data dari phishing: pendekatan Pancasila	Normatif-Filosofis	Serangan phishing ialah pelanggaran serius hak privasi; pendekatan berbasis Pancasila memperkuat legitimasi perlindungan data	Fondasi filosofis berbasis nilai nasional
26	Palit dan Purba (2025)	Perspektif hukum perlindungan privasi data sebagai HAM	Normatif-HAM	Privasi data merupakan HAM fundamental; ketiadaan otoritas pengawas independen merupakan pelanggaran kewajiban negara terhadap HAM	Landasan HAM dalam perlindungan data
27	Jagadhita (2025)	Transformasi digital sertifikat tanah dan respons masyarakat	Empiris-Kualitatif	Digitalisasi layanan pemerintah menimbulkan kekhawatiran masyarakat terhadap keamanan data pribadi dalam sistem pemerintah	Dimensi e-government dalam konteks PDP
28	Santoso (2024)	Tantangan penegakan hukum UU PDP	Kualitatif	Pengawasan dan sanksi belum optimal; diperlukan penguatan kapasitas aparat penegak hukum dan pembentukan tim khusus siber	Evaluasi kesiapan penegakan hukum

No.	Penulis dan Tahun	Fokus Penelitian	Metode	Temuan Utama	Relevansi
29	Syailendra (2024)	Tantangan dan peluang implementasi UU PDP	Normatif-Empiris	Implementasi UU PDP menghadapi tantangan kelembagaan, teknis dan budaya hukum; diperlukan roadmap implementasi komprehensif	Identifikasi hambatan sistemik implementasi
30	Pratama et al. (2023)	Implementasi UU PDP pada platform digital	Studi Kebijakan	Kesiapan organisasi mengimplementasikan UU PDP masih sangat rendah; dibutuhkan panduan teknis dari otoritas yang berwenang	Baseline kesiapan institutional layanan digital

Tabel 1 di atas menyajikan pemetaan komprehensif terhadap 30 studi yang diidentifikasi melalui proses SLR. Dari tabel tersebut, dapat diidentifikasi beberapa tren penelitian yang menonjol: (1) peningkatan signifikan jumlah kajian normatif dan komparatif pasca-pengesahan UU PDP pada 2022; (2) dominasi pendekatan normatif-yuridis dalam kajian perlindungan data di Indonesia; (3) masih terbatasnya penelitian empiris yang mengukur tingkat kepatuhan (legal compliance) penyedia layanan digital terhadap ketentuan UU PDP; dan (4) belum adanya konsensus dalam literatur mengenai model kelembagaan pengawas perlindungan data yang paling efektif untuk konteks Indonesia.

2. Evolusi Regulasi: Dari Rezim UU ITE Menuju Rezim UU PDP

Untuk memahami konteks implementasi perlindungan data pribadi di Indonesia, analisis historis terhadap evolusi regulasi menjadi sangat penting. SLR yang dimulai pada 2018 mencakup periode di mana rezim hukum yang berlaku adalah UU ITE (UU No. 11/2008 jo. UU No. 19/2016), sehingga kajian perlindungan data pada periode tersebut harus dipahami dalam konteks keterbatasan kerangka hukum yang ada.[12] Hal inilah yang menjadi salah satu catatan kritis reviewer: kajian terkait UU ITE perlu diperkuat untuk memahami garis kontinuitas dan diskontinuitas regulasi perlindungan data di Indonesia.

[12] R. Natamiharja dan I. Setiawan, *Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France*, Jambe Law Journal, Vol.7, No.1 (2024), p.88.

Rezim UU ITE mengatur perlindungan data pribadi secara sangat terbatas dan tersebar. Pasal 26 UU ITE hanya melarang penggunaan informasi elektronik tentang orang lain tanpa persetujuan yang bersangkutan—suatu ketentuan yang sangat minim dan tidak operasional. Tidak ada definisi yang jelas tentang apa yang dimaksud dengan 'data pribadi', tidak ada pengaturan tentang hak-hak subjek data, tidak ada kewajiban spesifik bagi pengendali data untuk menerapkan langkah-langkah keamanan dan tidak ada mekanisme notifikasi pelanggaran. Akibatnya, kasus-kasus kebocoran data yang terjadi pada periode ini seringkali tidak dapat ditangani secara memadai karena ketiadaan dasar hukum yang komprehensif.

Perubahan paradigma terjadi dengan disahkannya UU PDP pada September 2022. UU PDP mengadopsi pendekatan berbasis hak (rights-based approach) yang menempatkan subjek data sebagai pemegang hak dengan berbagai klaim yang dapat dipaksakan secara hukum. UU PDP tidak hanya mendefinisikan data pribadi secara komprehensif—membedakan antara data umum dan data khusus/sensitif—tetapi juga mengatur seluruh siklus hidup data: dari pengumpulan, pemrosesan, penyimpanan, hingga penghapusan. Yang lebih penting, UU PDP menetapkan tanggung jawab hukum yang jelas bagi pengendali data (data controller) dan pemroses data (data processor), serta menyediakan mekanisme sanksi yang lebih deterren dibandingkan UU ITE.

Tabel 2. Analisis Komparatif: UU ITE vs. UU PDP dalam Konteks Perlindungan Data Pribadi

Aspek	UU ITE (UU No. 11/2008 jo. No. 19/2016 jo. No. 1/2024)	UU PDP (UU No. 27/2022)
Cakupan regulasi	Bersifat sektoral dan parsial; Pasal 26 hanya mengatur larangan penggunaan informasi elektronik tanpa hak	Komprehensif dan lex specialis; mengatur seluruh siklus hidup data dari pengumpulan hingga penghapusan
Subjek yang diatur	Tidak memisahkan secara tegas antara data controller dan data processor	Secara eksplisit mengatur hak dan kewajiban pengendali data, pemroses data dan subjek data
Definisi data pribadi	Tidak memberikan definisi komprehensif tentang jenis-jenis data pribadi	Membagi data pribadi menjadi data umum dan data khusus/sensitif dengan perlindungan berbeda-beda
Hak subjek data	Tidak mengatur secara eksplisit hak-hak subjek data	Mengatur 10 hak subjek data: akses, koreksi, penghapusan, penarikan

Aspek	UU ITE (UU No. 11/2008 jo. No. 19/2016 jo. No. 1/2024)	UU PDP (UU No. 27/2022)
		persetujuan, keberatan, dll.
Mekanisme persetujuan	Tidak mengatur mekanisme persetujuan yang jelas (informed consent)	Mewajibkan informed consent yang eksplisit, bebas, spesifik dan berbasis informasi yang memadai
Keamanan data	Tidak mengatur standar keamanan teknis secara spesifik	Mewajibkan langkah-langkah keamanan teknis dan organisatoris yang proporsional dengan risiko
Notifikasi pelanggaran	Tidak mengatur kewajiban notifikasi pelanggaran data	Mewajibkan notifikasi kepada otoritas dan subjek data dalam 14 hari kerja setelah pelanggaran diketahui
Otoritas pengawas	Pengawasan tersebar di berbagai kementerian/lembaga tanpa koordinasi yang jelas	Mengamanatkan pembentukan lembaga pengawas perlindungan data pribadi yang independen
Sanksi	Pidana penjara dan denda (tidak spesifik untuk pelanggaran data pribadi)	Sanksi administratif DAN sanksi pidana yang lebih spesifik dan deterren
Transfer data lintas batas	Tidak mengatur secara spesifik transfer data ke luar negeri	Mengatur transfer data internasional dengan syarat kesetaraan perlindungan (adequacy)

Dari perbandingan dalam Tabel 2, tampak jelas bahwa terdapat lompatan kualitatif yang signifikan antara rezim UU ITE dan rezim UU PDP. Jika UU ITE hanya mengatur perlindungan data secara parsial dan reaktif, UU PDP menawarkan pendekatan yang lebih sistematis, proaktif dan berbasis hak. Pergeseran paradigma ini mencerminkan pengakuan normatif bahwa perlindungan data bukan lagi sekadar masalah teknis-administratif, melainkan merupakan dimensi penting dari perlindungan HAM dalam era digital.[13]

Namun demikian, perlu dicatat bahwa transformasi regulasi tidak serta merta diikuti oleh transformasi praktik. Gustryan dan Hoesein mengidentifikasi bahwa pergeseran dari rezim UU ITE ke rezim UU PDP memerlukan penyesuaian fundamental dalam tata kelola data (*data governance*) di seluruh sektor—baik publik maupun swasta.[14] Proses transisi ini memakan waktu dan sumber daya yang tidak sedikit, sehingga normative gap antara ketentuan hukum dan praktik lapangan menjadi tantangan yang harus diatasi secara terstruktur.

[13] Farah Naurah Khansa, *Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Pelindungan Data Pribadi di Indonesia*, Jurnal Hukum Lex Generalis, Vol.2, No.8 (2021).

[14] Badan Siber dan Sandi Negara Republik Indonesia, *Laporan Tahunan Monitoring Keamanan Siber Tahun 2021*, Badan Siber dan Sandi Negara Republik Indonesia, Jakarta, 2022, p.18-20.

3. Kasus Kebocoran Data pada Platform Pemerintah: Analisis Empiris dan Normatif

Salah satu fenomena yang paling mengkhawatirkan dalam lanskap digital Indonesia adalah serangkaian insiden kebocoran data yang justru menimpa platform-platform pemerintah—entitas yang seharusnya menjadi contoh teladan dalam pengelolaan data warganya. Analisis terhadap kasus-kasus ini penting tidak hanya dari perspektif empiris, tetapi juga normatif: sejauh mana kewajiban pengendali data menurut UU PDP telah atau seharusnya ditegakkan?

Kasus paling masif dan berdampak luas adalah kebocoran data BPJS Kesehatan pada Mei 2021, yang mengekspos data pribadi sekitar 279 juta jiwa—termasuk data orang yang telah meninggal dunia—ke forum peretas (hacking forum) di darkweb. Data yang bocor mencakup nama, Nomor Induk Kependudukan (NIK), nomor kartu, alamat, nomor telepon, hingga informasi medis. Insiden ini mengindikasikan kegagalan sistemik dalam tata kelola keamanan data pada salah satu lembaga pemerintah yang mengelola data sensitif masyarakat dalam skala sangat besar.

Dari perspektif teknis, kebocoran data BPJS Kesehatan diduga terjadi akibat kombinasi dari beberapa kelemahan: (a) sistem penyimpanan data yang tidak terenkripsi atau menggunakan enkripsi yang lemah; (b) ketiadaan kontrol akses (*access control*) yang memadai, sehingga database dapat diakses oleh pihak yang tidak berwenang; (c) lemahnya sistem deteksi intrusi (*intrusion detection system*) sehingga kebocoran tidak segera terdeteksi; dan (d) tidak adanya segmentasi data yang memisahkan data aktif dari data arsip.[15] Kelemahan-kelemahan teknis ini mencerminkan absennya standar keamanan data yang memadai dalam penyelenggaraan sistem informasi pemerintah.

Kasus berikutnya yang tidak kalah signifikan adalah insiden kebocoran data Komisi Pemilihan Umum (KPU) yang terjadi pada akhir 2023, di mana data pemilih dari Daftar Pemilih Tetap (DPT) yang mencakup sekitar 204 juta rekaman data diduga bocor dan diperjualbelikan.

Data yang terekspos meliputi NIK, nomor KK, nama, tempat dan tanggal lahir, jenis kelamin dan alamat—informasi yang dapat digunakan untuk berbagai bentuk penipuan identitas (identity fraud). Insiden ini terjadi justru menjelang Pemilihan Umum 2024, sehingga menimbulkan kekhawatiran serius terkait integritas data pemilih dan potensi penyalahgunaan untuk kepentingan politik.

Selain dua kasus besar tersebut, terdapat pula insiden kebocoran data pada berbagai platform pemerintah lainnya, termasuk dugaan kebocoran data Kementerian Kesehatan, Direktorat Jenderal Pajak, serta berbagai Pemerintah Daerah. Pola yang berulang dalam insiden-insiden ini menunjukkan adanya kelemahan sistemik—bukan insidental—dalam tata kelola keamanan data pada institusi pemerintah Indonesia.

a. Analisis Normatif: Kewajiban Pengendali Data menurut UU PDP

Merujuk pada ketentuan UU PDP, lembaga-lembaga pemerintah yang mengelola data pribadi masyarakat berkedudukan sebagai pengendali data (*data controller*). Sebagai pengendali data, mereka memikul serangkaian kewajiban hukum yang wajib dipenuhi berdasarkan prinsip-prinsip perlindungan data yang diatur dalam UU PDP.[16]

Pertama, prinsip *lawfulness* (keabsahan pemrosesan). UU PDP mewajibkan setiap pemrosesan data pribadi memiliki dasar hukum yang sah. Pemrosesan data pemilih oleh KPU dapat dibenarkan berdasarkan dasar hukum 'pelaksanaan tugas dalam rangka kepentingan umum'. Namun, kewajiban ini tidak berhenti pada legitimasi pengumpulan data—pengendali data juga wajib memastikan bahwa pemrosesan data dilakukan sesuai dengan tujuan yang telah ditetapkan dan tidak melampaui batas-batas yang diizinkan.[17]

Kedua, prinsip *purpose limitation* (pembatasan tujuan). Data pribadi yang dikumpulkan untuk satu tujuan tidak dapat digunakan untuk tujuan yang berbeda tanpa persetujuan atau dasar hukum yang baru.

[16] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, Pasal 20-21 UU No.27 Tahun 2022, *Op.Cit.*.

[17] Nabila Bunga Prasanti dan Agus Gunadi, *Implementation of the Principles of Necessity and Proportionality in the Sharing of Customer Data by Banks with Vendors*, Law Development Journal, Vol.7, No.3 (2025), p.402.

Dalam konteks data BPJS Kesehatan, data yang semula dikumpulkan untuk keperluan administrasi jaminan kesehatan jelas tidak boleh diekspos ke publik tanpa dasar hukum yang sah. Pelanggaran terhadap prinsip ini mengakibatkan tanggung jawab hukum yang serius bagi pengendali data.[18]

Ketiga, prinsip *data security* (keamanan data). Inilah prinsip yang paling jelas dilanggar dalam kasus-kasus kebocoran data pemerintah yang dipaparkan di atas. Pasal 35 UU PDP mewajibkan pengendali data untuk 'melindungi dan memastikan keamanan data pribadi yang diprosesnya' melalui langkah-langkah teknis dan organisatoris yang memadai. Kegagalan untuk menerapkan enkripsi yang kuat, kontrol akses yang memadai dan sistem deteksi intrusi yang efektif merupakan pelanggaran nyata terhadap kewajiban keamanan data ini.[19]

Keempat, prinsip *accountability* (akuntabilitas). UU PDP mewajibkan pengendali data untuk dapat membuktikan kepatuhan mereka terhadap ketentuan UU PDP. Kegagalan dalam mencegah kebocoran data bukan hanya mengakibatkan kerugian bagi subjek data, tetapi juga merupakan pelanggaran kewajiban akuntabilitas yang dapat dikenai sanksi administratif berupa denda, serta potensi tuntutan pidana berdasarkan Pasal 67-68 UU PDP.[20]

Dari analisis normatif di atas, tampak jelas bahwa kasus-kasus kebocoran data pada platform pemerintah merupakan cerminan dari normative gap yang serius: terdapat jurang yang lebar antara kewajiban hukum yang ditetapkan UU PDP dan kapasitas aktual pengendali data—khususnya lembaga pemerintah—untuk memenuhi kewajiban tersebut. Normative gap ini tidak hanya merugikan jutaan subjek data, tetapi juga mengikis kepercayaan publik terhadap layanan digital pemerintah secara keseluruhan.

---

[18] Egi Syarif Badar, Ahmad Fauzi dan Ahmad Jazuli, *Kebijakan Pelindungan Data Pribadi Undang-Undang Nomor 27 Tahun 2022 dalam Perspektif Hukum Positif dan Hukum Islam*, Hukum Islam, Vol.23, No.1 (2023), p.45.

[19] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, Pasal 35-38 UU No.27 Tahun 2022, *Op.Cit.*.

[20] *Ibid*., Pasal 65-68.

4. Analisis Yuridis Implementasi UU PDP: Tantangan Kesiapan Institusional dan Normative Gap

Berdasarkan sintesis terhadap 30 literatur yang dikaji, implementasi regulasi perlindungan data pribadi dalam layanan digital di Indonesia masih berada pada tahap awal yang penuh tantangan. Meskipun UU PDP telah menyediakan regulatory framework yang secara normatif lebih komprehensif, kesenjangan antara norma dan praktik (*normative gap*) tetap menjadi persoalan sentral yang harus diatasi.[21]

Kesiapan penyedia layanan digital dalam mengimplementasikan ketentuan UU PDP masih sangat bervariasi. Perusahaan teknologi berskala besar—khususnya yang beroperasi di sektor perbankan dan jasa keuangan yang telah lebih dulu diatur oleh OJK—umumnya memiliki kesiapan yang relatif lebih baik karena telah terbiasa dengan kerangka regulasi yang ketat. Sebaliknya, usaha kecil dan menengah yang beroperasi di sektor digital—termasuk platform e-commerce lokal, aplikasi layanan kesehatan digital dan startup fintech kecil—masih menghadapi kesulitan signifikan dalam memenuhi standar UU PDP karena keterbatasan sumber daya manusia, keuangan dan infrastruktur teknologi.

Penelitian Pratama et al. menunjukkan bahwa sebagian besar penyedia layanan digital di Indonesia belum memiliki Data Protection Officer (DPO) sebagaimana direkomendasikan oleh praktik terbaik internasional.[22] Ketiadaan fungsi khusus yang bertanggung jawab atas kepatuhan perlindungan data mengakibatkan isu-isu terkait privasi dan keamanan data seringkali ditangani secara ad hoc dan reaktif—hanya menjadi perhatian setelah terjadi insiden kebocoran data. Pendekatan reaktif semacam ini bertentangan dengan semangat UU PDP yang menekankan pentingnya pendekatan proaktif dan *privacy by design*.

---

[21] I Wayan Candra Ardika, *Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce*, Indonesian Journal of Law and Justice, Vol.2, No.3 (2025), p.11.

[22] Muhamad Adri Rinjani dan Ricky Firmansyah, *Hambatan Implementasi UU27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia*, Jurnal Analisis Hukum, Vol.8, Issue 1 (2025).

Salah satu hambatan struktural yang paling kritis adalah belum terbentuknya lembaga pengawas perlindungan data pribadi yang independen sebagaimana diamanatkan oleh Pasal 58 UU PDP. Khansa telah mengidentifikasi sejak 2021—bahkan sebelum UU PDP disahkan—bahwa ketiadaan otoritas pengawas independen merupakan celah institusional yang serius dalam sistem perlindungan data Indonesia.[23] Tanpa lembaga pengawas yang memiliki kewenangan investigasi, penegakan dan pengenaan sanksi yang memadai, regulatory framework UU PDP berisiko menjadi macan ompong: normatif kuat tetapi pragmatis lemah. Matheus dan Gunadi melalui perbandingan dengan Komisi Pengawas Persaingan Usaha (KPPU) menunjukkan bahwa efektivitas lembaga pengawas sangat bergantung pada independensi struktural, kapasitas sumber daya manusia dan kewenangan hukum yang memadai.[24]

Di sisi pengguna, literatur secara konsisten menunjukkan bahwa tingkat kesadaran masyarakat terhadap hak-hak privasi mereka sebagai subjek data masih sangat rendah. Mayoritas pengguna layanan digital belum memahami hak-hak dasar yang diberikan UU PDP—termasuk hak untuk mengakses data mereka, hak untuk mengoreksi data yang tidak akurat, hak untuk menarik persetujuan dan hak untuk mengajukan keberatan terhadap pemrosesan data yang tidak sah.[25] Rendahnya literasi perlindungan data ini menciptakan kondisi di mana subjek data tidak dapat secara efektif menjalankan peran mereka sebagai agen aktif dalam perlindungan privasi mereka sendiri—sebuah paradoks mengingat bahwa UU PDP secara eksplisit menetapkan hak-hak tersebut.[26]

---

[23] Farah Naurah Khansa, *Op.Cit*..

[24] Juan Matheus dan Ariawan Gunadi, *Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital: Kajian Perbandingan dengan KPPU*, JUSTISI, Vol.10, No.1 (2023), p.45.

[25] Nurul Afifah, *Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi Pengguna: Analisis Berdasarkan UU PDP 2022*, Jurnal Legalitas (JLE), Vol.2, No.1 (2024), p.29.

[26] Admiral dan Mega Ardina Pauck, *Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services*, Lex Scientia Law Review, Vol.7, No.2 (2023), p.995.

Dari perspektif penegakan hukum, sanksi yang tersedia dalam UU PDP—mulai dari sanksi administratif berupa denda hingga sanksi pidana penjara dan denda yang signifikan—secara normatif sudah cukup deterren. Namun, efektivitas sanksi ini sangat bergantung pada kapasitas aparat penegak hukum untuk mendeteksi pelanggaran, melakukan investigasi yang komprehensif dan membuktikan pelanggaran di hadapan pengadilan.[27] Keterbatasan kapasitas teknis aparat penegak hukum dalam menangani kasus-kasus kejahatan siber yang melibatkan data pribadi menjadi salah satu faktor utama yang melemahkan deterrent effect dari sanksi UU PDP.[28]

5. Analisis Normatif Prinsip-Prinsip UU PDP dan Kesenjangan Implementasi

Analisis normatif terhadap ketentuan-ketentuan UU PDP mengungkapkan bahwa undang-undang ini mengadopsi prinsip-prinsip perlindungan data yang secara substansial selaras dengan standar internasional sebagaimana tercermin dalam GDPR Uni Eropa.[29] Prinsip-prinsip tersebut meliputi: (1) keabsahan pemrosesan (*lawfulness*); (2) pembatasan tujuan (*purpose limitation*); (3) minimisasi data (*data minimization*); (4) akurasi data (*accuracy*); (5) pembatasan penyimpanan (*storage limitation*); (6) keamanan data (*data security*); dan (7) akuntabilitas (*accountability*). Setiap prinsip ini mencerminkan nilai-nilai fundamental yang mendasari perlindungan data sebagai bagian dari penghormatan terhadap martabat dan otonomi manusia.[30]

Meskipun demikian, analisis mendalam terhadap literatur yang ada mengidentifikasi beberapa normative gap yang kritis antara ketentuan UU PDP dan praktik implementasi di lapangan:

---

[27] Kukuh Dwi Kurniawan, dkk., *Criminal Sanctions and Personal Data Protection in Indonesia*, Lex Publica, Vol.11, No.2 (2024), p.221.

[28] Gunsu Nurmansyah, Rudi Natamiharja dan Ikhsan Setiawan, *Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach*, Pancasila and Law Review, Vol.6, No.1 (2025), p.78.

[29] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation (GDPR), Article 5(1)(f).

[30] Chairunnisa Abdullah, dkk., *Transformasi Digital dan Hak atas Privasi: Tinjauan Kritis Pelaksanaan UU PDP 2022 di Era Big Data*, Amandemen: Jurnal Ilmu pertahanan, Politik dan Hukum Indonesia, Vol.2, No.3 (2025), p.5.

Pertama, gap dalam mekanisme persetujuan (informed consent). UU PDP mewajibkan persetujuan yang eksplisit, bebas, spesifik dan berbasis informasi yang memadai. Namun dalam praktik, banyak penyedia layanan digital masih menggunakan formulir persetujuan yang panjang, tidak terbaca dan dirancang sedemikian rupa sehingga pengguna secara default menyetujui pengumpulan dan penggunaan data yang sangat luas. Praktik 'dark patterns' dalam desain antarmuka digital—yang memanipulasi pengguna untuk memberikan persetujuan yang sebenarnya tidak mereka kehendaki—merupakan pelanggaran nyata terhadap prinsip persetujuan yang bermakna, namun belum mendapat perhatian regulasi yang memadai.[31]

Kedua, gap dalam standar keamanan data. UU PDP mewajibkan pengendali data untuk menerapkan 'langkah-langkah yang sesuai' dalam menjaga keamanan data. Namun, tidak ada standar teknis yang spesifik yang ditetapkan oleh UU PDP atau peraturan pelaksananya, sehingga penilaian tentang apa yang dianggap 'memadai' menjadi sangat subjektif dan tidak terukur. Ketiadaan standar teknis yang jelas ini menciptakan ketidakpastian hukum bagi pengendali data sekaligus membuka celah bagi praktik pengamanan data yang minimal.[32]

Ketiga, gap dalam kewajiban notifikasi pelanggaran. UU PDP mewajibkan pengendali data untuk melaporkan pelanggaran keamanan data kepada otoritas dan kepada subjek data yang terdampak dalam waktu 14 hari kerja setelah pelanggaran diketahui. Namun, dalam praktik, banyak kasus kebocoran data justru pertama kali terungkap melalui laporan peneliti keamanan independen atau forum peretas di internet—bukan melalui notifikasi resmi dari pengendali data. Hal ini mengindikasikan bahwa kewajiban notifikasi belum dipatuhi secara konsisten, sebagian karena tidak adanya otoritas pengawas yang siap menerima laporan tersebut.[33]

---

[31] Nabila Bunga Prasanti dan Agus Gunadi, *Op.Cit*..

[32] Inaz Indra Nugroho, dkk., *Optimalisasi Penanggulangan Kebocoran Data melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia*, Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, Vol.1, No.2 (2021), p.67.

[33] Hardianto S. Disemadi, *Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia*, Jurnal Wawasan Yuridika, Vol.5, No.2 (2021), p.171.

Keempat, gap dalam transfer data lintas batas. UU PDP mengatur bahwa transfer data pribadi ke luar negeri hanya dapat dilakukan ke negara yang memiliki tingkat perlindungan data yang setara (*adequacy*). Namun, dalam praktik layanan cloud computing yang menjadi infrastruktur mayoritas layanan digital di Indonesia, data pengguna Indonesia seringkali disimpan dan diproses di server yang berlokasi di berbagai negara tanpa evaluasi yang memadai tentang kesetaraan perlindungan data di negara tersebut.[34]

Gap-gap implementasi di atas secara kolektif menunjukkan bahwa meskipun UU PDP telah menyediakan fondasi normatif yang kuat, masih dibutuhkan upaya yang sangat signifikan—baik dari sisi pemerintah, pengendali data, maupun subjek data—untuk menutup jarak antara hukum dalam teks dan hukum dalam tindakan.[35] Tantangan ini sesungguhnya bukan hanya soal legal compliance semata, tetapi menyentuh dimensi yang lebih dalam: bagaimana membangun budaya perlindungan data (*data protection culture*) yang mengakar dalam ekosistem digital Indonesia.[36]

6. Tren Penelitian dan Research Gap: Sintesis Literatur

Berdasarkan analisis terhadap 30 literatur yang dikaji, dapat diidentifikasi beberapa tren penelitian yang signifikan dalam bidang perlindungan data pribadi di Indonesia. Pertama, terdapat peningkatan drastis dalam kuantitas dan keragaman penelitian pasca-pengesahan UU PDP pada 2022. Sebelum 2022, sebagian besar literatur berfokus pada kritik terhadap ketidaklengkapan rezim UU ITE dan urgensi pembentukan regulasi khusus. Pasca-2022, fokus penelitian bergeser ke arah evaluasi normatif UU PDP, komparasi dengan standar internasional (GDPR) dan identifikasi tantangan implementasi.

---

[34] Intan Permata Mipon dan Mohamad Fajri Mekka Putra, *Penyelenggaraan Pelindungan Data Pribadi oleh Notaris berdasarkan Undang-Undang Nomor 27 Tahun 2022*, Jurnal Hukum dan Pembangunan, Vol.53, No.3 (2023), p.567.

[35] Heriyanto, *Analisis Perbandingan Regulasi dan Perlindungan Hukum atas Privasi Data Pasien di Tiga Negara Asia Tenggara (Indonesia, Singapura dan Laos)*, Jurnal Ners, Vol.7, No.2 (2023), p.1247.

[36] Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, *Perlindungan Hukum Data Pribadi Sebagai Hak Privasi*, JA: Jurnal Al-Wasath, Vol.2, No.1 (2021), p.30.

Kedua, terdapat dominasi yang kuat dari pendekatan normatif-yuridis dalam penelitian perlindungan data di Indonesia. Kajian empiris yang mengukur tingkat kepatuhan aktual penyedia layanan digital terhadap ketentuan UU PDP masih sangat terbatas. Ketiadaan data empiris yang komprehensif ini menjadi hambatan serius dalam evaluasi efektivitas regulasi secara objektif.

Ketiga, literatur menunjukkan adanya konsensus yang kuat terkait identifikasi masalah—normative gap, rendahnya literasi digital, ketiadaan otoritas pengawas independen—namun masih sangat terbatas dalam hal menawarkan solusi yang konkret, terukur dan kontekstual untuk kondisi Indonesia.

Keempat, dimensi sektoral dalam implementasi UU PDP masih kurang tereksplorasi. Sebagian besar penelitian bersifat generalis tanpa membedakan secara spesifik tantangan yang dihadapi oleh sektor-sektor yang berbeda (fintech, e-health, e-government, e-commerce). Padahal, tantangan implementasi UU PDP di setiap sektor memiliki karakteristik yang unik dan memerlukan respons kebijakan yang berbeda-beda.

Research gap yang paling mendesak untuk diatasi dalam penelitian-penelitian mendatang meliputi: (1) studi empiris tentang tingkat legal compliance penyedia layanan digital terhadap UU PDP; (2) penelitian tentang efektivitas mekanisme penegakan hukum pasca-pembentukan lembaga pengawas independen; (3) kajian komparatif mendalam antara model kelembagaan pengawas perlindungan data di berbagai negara ASEAN; dan (4) penelitian interdisipliner yang mengintegrasikan perspektif hukum, teknis siber dan ilmu perilaku dalam mengkaji kepatuhan perlindungan data.

C. PENUTUP

Berdasarkan hasil Systematic Literature Review terhadap 30 literatur ilmiah bereputasi yang diterbitkan dalam rentang 2018–2025, penelitian ini menghasilkan beberapa kesimpulan sebagai berikut:

Pertama, mengenai fondasi filosofis dan konstitusional. Perlindungan data pribadi di Indonesia tidak dapat dipisahkan dari dimensi HAM dan teori negara hukum. Hak atas privasi sebagai bagian dari human dignity dan otonomi individu merupakan hak konstitusional yang dilindungi Pasal 28G UUD 1945. Dalam kerangka rechtstaat, negara memiliki kewajiban positif untuk menyediakan infrastruktur hukum yang efektif dalam melindungi hak privasi warganya—tidak hanya secara normatif, tetapi juga secara empiris.

Kedua, mengenai evolusi regulasi. Indonesia telah mengalami transisi regulasi yang signifikan dari rezim UU ITE yang parsial dan reaktif menuju rezim UU PDP yang komprehensif dan berbasis hak. UU PDP secara normatif sejalan dengan standar internasional (GDPR) dalam hal prinsip-prinsip perlindungan data, hak-hak subjek data dan mekanisme akuntabilitas. Namun, perubahan paradigma normatif ini belum diikuti oleh transformasi praktik yang setara.

Ketiga, mengenai kasus kebocoran data pemerintah. Kasus-kasus kebocoran data pada platform pemerintah—BPJS Kesehatan, KPU dan berbagai lembaga lainnya—mencerminkan normative gap yang serius antara kewajiban pengendali data menurut UU PDP dan kapasitas aktual lembaga-lembaga tersebut dalam memenuhi kewajiban itu. Analisis normatif menunjukkan bahwa insiden-insiden ini merupakan pelanggaran nyata terhadap prinsip lawfulness, purpose limitation, data security dan accountability yang diatur dalam UU PDP.

Keempat, mengenai normative gap yang persisten. Terdapat empat normative gap kritis dalam implementasi UU PDP: (a) gap dalam mekanisme informed consent yang bermakna; (b) gap dalam standar keamanan teknis yang terukur; (c) gap dalam kewajiban notifikasi pelanggaran yang dipatuhi; dan (d) gap dalam regulasi transfer data lintas batas. Gap-gap ini secara kolektif melemahkan efektivitas perlindungan data pribadi dalam praktik layanan digital di Indonesia.

DAFTAR PUSTAKA

Buku

Hadjon, Philipus M. 1987. *Perlindungan Hukum bagi Rakyat Indonesia*. (Surabaya: Bina Ilmu).

Magnis-Suseno, Franz. 1987. *Etika Politik: Prinsip-Prinsip Moral Dasar Kenegaraan Modern*. (Jakarta: PT Gramedia).

Rahardjo, Satjipto. 2014. *Ilmu Hukum*. (Bandung: Citra Aditya Bakti).

Westin, Alan. 1967. *Privacy and Freedom*. (New York: Atheneum).

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. (New York: PublicAffairs).

Publikasi

Abdullah, Chairunnisa, dkk.. *Transformasi Digital dan Hak atas Privasi: Tinjauan Kritis Pelaksanaan UU PDP 2022 di Era Big Data*. Amandemen: Jurnal Ilmu pertahanan, Politik dan Hukum Indonesia. Vol.2. No.3 (2025).

Admiral dan Mega Ardina Pauck. *Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services*. Lex Scientia Law Review. Vol.7. No.2 (2023).

Afifah, Nurul. *Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi Pengguna: Analisis Berdasarkan UU PDP 2022*. Jurnal Legalitas (JLE). Vol.2. No.1 (2024).

Ahmad, Ridho Sa'dillah, dkk.. *Perlindungan Hukum terhadap Privasi Data Pribadi di Era Digital*. The Juris (Jurnal Ilmu Hukum). Vol.9. No.1 (2025).

Ardana, Auriza Fajri, dkk.. *Systematic Literature Review dengan Metode Prisma: Pemanfaatan Chatbot*. JATI (Jurnal Mahasiswa Teknik Informatika). Vol.9. No.3 (2025).

Ardika, I Wayan Candra Ardika. *Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce*. Indonesian Journal of Law and Justice. Vol.2. No.3 (2025).

Badar, Egi Syarif, Ahmad Fauzi dan Ahmad Jazuli. *Kebijakan Pelindungan Data Pribadi Undang-Undang Nomor 27 Tahun 2022 dalam Prespektif Hukum Positif Dan Hukum Islam*. Hukum Islam. Vol.23. No.1 (2023).

Budiman, Risky. *The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022*. Jurnal Smart Hukum (JSH). Vol.2. No.1 (2023).

Disemadi, Hardianto S.. *Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia*. Jurnal Wawasan Yuridika. Vol.5. No.2 (2021).

Fathni, Indriya, Basri, Siti Zulaika dan Retno Sari Dewi. *Pengaruh Kebijakan Privasi, dan Tingkat Kepercayaan pada Platform Digital terhadap Perilaku Pengguna dalam Melindungi Privasi Onlinedi Indonesia*. Sanskara Hukum dan HAM. Vol.2. No.2 (Desember 2023).

Gustryan, Muhammad dan Zainal Arifin Hoesein. *Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital*. Jurnal Minfo Polgan. Vol.14. No.2 (2025).

Heriyanto. *Analisis Perbandingan Regulasi dan Perlindungan Hukum atas Privasi Data Pasien di Tiga Negara Asia Tenggara (Indonesia, Singapura dan Laos)*. Jurnal Ners. Vol.7. No.2 (2023).

Jagadhita, Mochammad Abyan. *Transformasi Digital Sertifikat Tanah dan Respons Masyarakat terhadap Penerapannya*. Jurnal USM Law Review. Vol.8. No.3 (2025).

Kesuma, A.A. Ngurah Deddy Hendra, I Nyoman Putu Budiartha dan Putu Ayu Sriasih Wesna. *Perlindungan Hukum terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial dalam Transaksi Elektronik*. Jurnal Preferensi Hukum. Vol.2. No.2 (2021).

Khansa, Farah Naurah. *Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Pelindungan Data Pribadi di Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.2. No.8 (2021).

Kurdi dan Joko Cahyono. *Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022*. JUNCTO Jurnal Ilmiah Hukum. Vol.6. No.2 (2024).

Kurniawan, Kukuh Dwi, dkk.. *Criminal Sanctions and Personal Data Protection in Indonesia*. Lex Publica. Vol.11. No.2 (2024).

Kusnadi, Sekaring Ayumeida dan Andy Usmina Wijaya. *Perlindungan Hukum Data Pribadi Sebagai Hak Privasi*. JA: Jurnal Al-Wasath. Vol.2. No.1 (2021).

Matheus, Juan dan Ariawan Gunadi. *Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital: Kajian Perbandingan dengan KPPU*. JUSTISI. Vol.10. No.1 (2023).

Mipon, Intan Permata dan Mohamad Fajri Mekka Putra. *Penyelenggaraan Pelindungan Data Pribadi oleh Notaris berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Jurnal Hukum dan Pembangunan. Vol.53. No.3 (2023).

Muhamad Adri Rinjani dan Ricky Firmansyah. *Hambatan Implementasi UU27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia*. Jurnal Analisis Hukum. Vol.8. Issue 1 (2025).

Natamiharja, Rudi dan Ikhsan Setiawan. *Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France*. Jambe Law Journal. Vol.7. No.1 (2024).

Nugroho, Inaz Indra, dkk.. *Optimalisasi Penanggulangan Kebocoran Data melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia*. Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal. Vol.1. No.2 (2021).

Nurmalasari. *Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum*. Syntax Idea. Vol.3. No.8 (2021).

Nurmansyah, Gunsu, Rudi Natamiharja, Ikhsan Setiawan. *Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach*. Pancasila and Law Review. Vol.6. No.1 (2025).

Palit, Silvester Magnus Loogman dan Tumian Lian Daya Purba. *Legal Perspective on Data Privacy Protection as a Human Right in Indonesia*. The Easta Journal Law and Human Rights. Vol.4. No.1 (2025).

Paranata, Ade. *A Systematic Literature Review of Anti-corruption Policy: A Future Research Agenda in Indonesia*. Public Organization Review. Vol.25 (2025).

Prasanti, Nabila Bunga dan Agus Gunadi. *Implementation of the Principles of Necessity and Proportionality in the Sharing of Customer Data by Banks with Vendors*. Law Development Journal. Vol.7. No.3 (2025).

Syailendra, Moddy Rizqy. *Personal Data Protection Law in Indonesia: Challenges and Opportunities*. Indonesia Law Review. Vol.14. No.2 (2024).

Sumber Hukum

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Putusan Mahkamah Konstitusi Republik Indonesia Nomor 5/PUU-VIII/2010.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation (GDPR).

Sumber Lain

Badan Siber dan Sandi Negara Republik Indonesia. 2022. *Laporan Tahunan Monitoring Keamanan Siber Tahun 2021*. Jakarta: Badan Siber dan Sandi Negara Republik Indonesia.

Kementerian Komunikasi dan Digital Republik Indonesia. 2022. *Laporan Tahunan Kementerian Komunikasi dan Informatika 2021*. Jakarta: Kementerian Komunikasi dan Digital Republik Indonesia.