Author's name: Muhamad Adri Rinjani. "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia" *Jurnal Analisis Hukum 8* no. 1 (2025): 70-83.
DOI: https://doi.org/10.38043/jah.v8i1.6793

Jurnal Analisis Hukum
Volume 8 Issue 1, 2025
P-ISSN: 2620-4959, E-ISSN: 2620-3715

Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia

Muhamad Adri Rinjani[1*], Ricky Firmansyah[2],

[1] *Teknik Informatika, Universitas Adhirajasa Reswara Sanjaya, Indonesia. E-mail: rinjaniadri@gmail.com*
[2] *Teknik Informatika, Universitas Adhirajasa Reswara Sanjaya, Indonesia E-mail: ricky@ars.ac.id*

Abstract: *This research discusses the challenges of implementing Law No. 27 of 2022 on Personal Data Protection (PDP Law) in Indonesia through a literature study. Although this law is expected to be a shield for citizens' digital rights, in practice there are still many obstacles, such as weak law enforcement and overlapping tasks between institutions. The study looked at various reports, research, and data on data leakage cases that occurred, as well as how institutions responded to the problem. It found that the unpreparedness of the legal and institutional systems, coupled with a lack of accountability, are the main reasons why the law has not worked optimally. The study suggests that institutional capacity be strengthened and authority between agencies be clarified so that the right to personal data is truly protected.*

Keywords: *Personal Data Protection; PDP Law; Data Leakage; Law Enforcement*

Abstrak: Penelitian ini membahas tantangan dalam implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia melalui metode studi literatur. Meskipun UU ini diharapkan menjadi pelindung hak digital warga negara, dalam praktiknya masih terdapat berbagai kendala seperti lemahnya penegakan hukum dan tumpang tindih kewenangan antar lembaga. Penelitian ini menelaah berbagai laporan, kajian, dan data terkait kasus kebocoran data yang terjadi serta respons lembaga terhadap permasalahan tersebut. Hasil studi menunjukkan bahwa ketidaksiapan sistem hukum dan kelembagaan, ditambah dengan rendahnya akuntabilitas, menjadi penyebab utama belum optimalnya implementasi UU ini. Penelitian ini merekomendasikan penguatan kapasitas kelembagaan dan kejelasan otoritas antar lembaga agar hak atas data pribadi dapat terlindungi secara efektif.

Kata Kunci: Perlindungan Data Pribadi; UU PDP; Kebocoran Data; Penegakan Hukum

1. Pendahuluan

Perkembangan teknologi digital telah membawa dampak besar terhadap kehidupan sosial, ekonomi, dan hukum masyarakat Indonesia. Di tengah kemajuan tersebut, data pribadi menjadi aset yang sangat bernilai dan digunakan oleh berbagai pihak, mulai dari individu hingga institusi pemerintah dan swasta, untuk beragam kepentingan, seperti pelayanan publik dan strategi bisnis. Namun, percepatan transformasi digital ini tidak diiringi dengan kesiapan regulasi dan kelembagaan yang memadai, sehingga menimbulkan risiko tinggi terhadap privasi dan keamanan data pribadi.

Berbagai laporan internasional, seperti UNCTAD (2021), menunjukkan bahwa negara berkembang termasuk Indonesia masih memiliki kerangka hukum perlindungan data yang lemah, sehingga meningkatkan kerentanan terhadap penyalahgunaan data. Untuk menjawab tantangan ini, pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai regulasi utama yang diharapkan mampu memberikan perlindungan hukum yang kuat terhadap hak-hak privasi warga negara.

Sejumlah penelitian terdahulu telah membahas aspek hukum dan kelembagaan dari perlindungan data pribadi. Misalnya, Mahardika (2021) menekankan pentingnya pembentukan otoritas independen untuk mengawasi implementasi UU PDP, sementara Hertianto (2021) menyoroti lemahnya penegakan hukum dalam kasus kebocoran data. Namun, sebagian besar studi tersebut masih berfokus pada analisis normatif atau desain kelembagaan, tanpa menelaah secara menyeluruh hambatan konkret dalam implementasi UU PDP serta belum menyajikan sintesis strategi komprehensif yang dapat diadopsi oleh pembuat kebijakan.

Penelitian ini bertujuan untuk mengisi celah tersebut dengan melakukan studi literatur terhadap sumber-sumber akademik, laporan kebijakan, dan berita resmi dalam lima tahun terakhir. Fokus utama penelitian ini adalah mengidentifikasi hambatan aktual dalam pelaksanaan UU PDP di Indonesia serta merumuskan strategi penguatan perlindungan data pribadi secara praktis dan aplikatif. Dengan pendekatan ini, studi ini diharapkan dapat memberikan kontribusi ilmiah yang bersifat strategis dan memperkaya diskursus mengenai tata kelola data pribadi di Indonesia.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (library research). Pendekatan ini dipilih karena memungkinkan peneliti untuk menganalisis fenomena hukum dan kebijakan terkait perlindungan data pribadi melalui telaah mendalam terhadap dokumen-dokumen tertulis. Studi ini menekankan pemahaman yang mendalam terhadap tantangan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dengan merujuk pada berbagai sumber ilmiah, regulasi, laporan kebijakan, dan berita resmi.

Jenis data yang digunakan adalah data sekunder, yaitu data yang tidak dikumpulkan secara langsung oleh peneliti, tetapi diperoleh dari sumber yang telah ada. Data ini mencakup dokumen hukum, jurnal ilmiah, laporan institusi pemerintah (seperti Kominfo dan BSSN), serta artikel berita dari media daring kredibel. Sumber data diperoleh dari

beberapa platform seperti Google Scholar, Perpustakaan Nasional RI, situs resmi instansi pemerintah, serta publikasi internasional seperti UNCTAD dan European Commission.

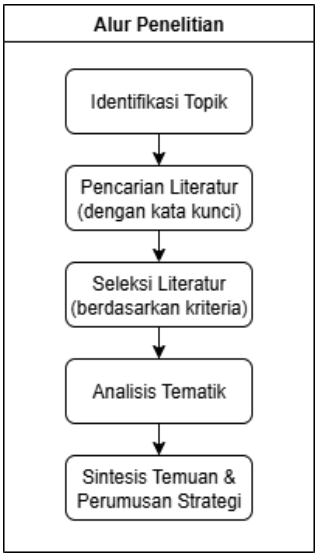
Penelitian ini tidak menggunakan informan atau responden karena sifatnya tidak melibatkan pengumpulan data primer. Instrumen penelitian yang digunakan berupa pedoman analisis dokumen, yaitu daftar kriteria untuk mengevaluasi relevansi, kredibilitas, dan aktualitas sumber yang dikaji. Kriteria seleksi literatur meliputi: (1) relevansi terhadap topik perlindungan data pribadi, (2) tahun terbit antara 2020–2025, dan (3) bersifat ilmiah atau berbasis bukti.

Teknik pengumpulan data dilakukan melalui pencarian terstruktur menggunakan kata kunci tertentu seperti “UU PDP”, “kebocoran data”, “perlindungan privasi”, dan “lembaga pengawas data”, dengan filter waktu dan sumber yang sesuai. Seluruh sumber yang memenuhi kriteria dianalisis secara deskriptif-kualitatif untuk mengidentifikasi tema-tema utama seperti lemahnya penegakan hukum, belum terbentuknya lembaga pengawas (OPDP), dan rendahnya literasi publik.

Kerangka teori yang digunakan dalam penelitian ini merujuk pada pendekatan hak asasi manusia terhadap privasi digital (UNCTAD, 2021), serta teori kelembagaan yang menekankan pentingnya pembentukan lembaga pengawas independen (Mahardika, 2021; Tambunan et al., 2024). Pendekatan ini membantu memetakan dimensi struktural, normatif, dan operasional dalam implementasi kebijakan perlindungan data.

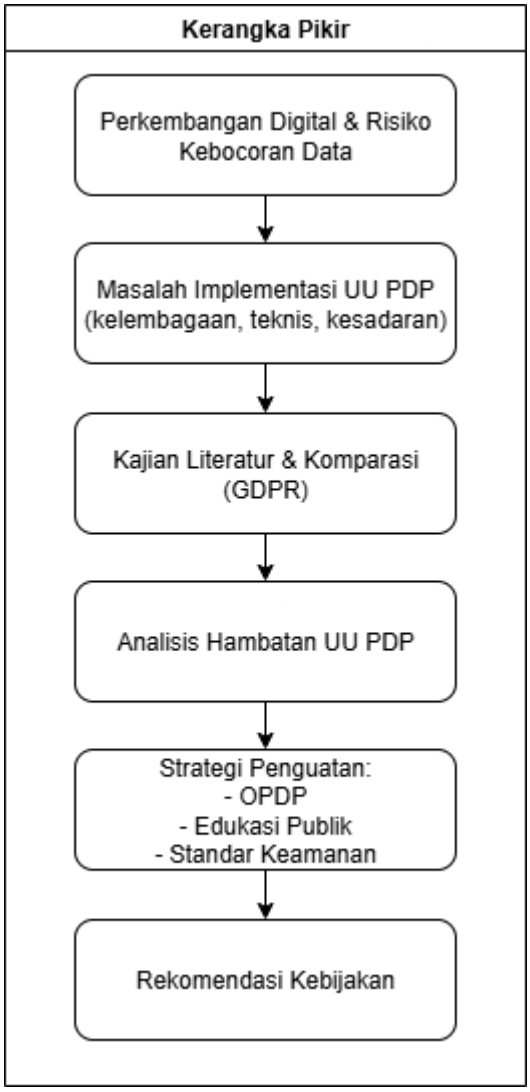
Teknik analisis data dilakukan secara kualitatif melalui proses reduksi data, kategorisasi tematik, dan penarikan simpulan berbasis sintesis literatur. Untuk menjaga kredibilitas data, digunakan teknik triangulasi sumber, yaitu dengan membandingkan informasi dari berbagai jenis publikasi (jurnal ilmiah, laporan resmi, dan media kredibel), serta memastikan bahwa seluruh dokumen yang digunakan memiliki kejelasan institusi penerbit dan tahun publikasi yang valid.

Adapun alur penelitian ini digambarkan dalam Gambar 1.



Gambar 1. Alur Penelitian.

Kerangka pikir penelitian ini menggambarkan bagaimana penulis memetakan hubungan antara konteks kebijakan, masalah implementasi UU PDP, perbandingan internasional, hingga formulasi strategi kebijakan. Visualisasi ini membantu memperjelas struktur argumentasi yang dikembangkan dalam analisis.



Gambar 2. Kerangka Pikir Penelitian.

Kerangka pikir ini menggambarkan proses pemikiran peneliti dalam mengidentifikasi permasalahan, melakukan kajian literatur, menganalisis hambatan UU PDP, hingga merumuskan strategi penguatan dan rekomendasi kebijakan.

Daftar sumber utama yang menjadi acuan dalam studi ini disajikan pada Tabel 1.

Tabel 1. Tinjauan Literatur.

No	Judul	Penulis/Instansi	Tahun	Penerbit
1	*Raising Standards for Data and AI in Southeast Asia: Indonesia*	Asia Society	2021	Asia Society
2	Laporan Tahunan Keamanan Siber Nasional 2023	Badan Siber dan Sandi Negara	2023	BSSN
3	*Measuring State's Commitment to Implementing PDP Law*	Center for Indonesian Policy Studies	2022	CIPS
4	Kebocoran Data KPU: 204 Juta Data Pemilih Diduga Bocor	CNN Indonesia	2023	CNN Indonesia
5	Lembaga Pengawas Belum Terbentuk, Pengaduan Kebocoran Data Pun Jadi Tak Jelas	Djafar, W.	2024	Kompas.id
6	*General Data Protection Regulation (GDPR) and European Data Protection Board*	European Commission	2023	European Commission
7	UU PDP: Apakah cukup untuk melindungi data pribadi di Indonesia?	Fourtrezz	2024	Fourtrezz Media
8	Data 91 Juta Akun Tokopedia Bocor, Ini Penjelasan Perusahaan	Kompas	2023	Kompas
9	4 Tantangan implementasi UU PDP di perusahaan dan solusi efektifnya	Putri, W. A.	2025	Cloud Helios
10	*Preparing for Indonesia's New Data Protection Law: What Your Business Needs to Know*	RSM Indonesia	2024	RSM Indonesia
11	*Data Protection and Privacy Legislation Worldwide*	UNCTAD	2021	United Nations (UNCTAD)
12	Menyorot Independensi Lembaga Pengawas Data Pribadi	Wijaya, T.	2023	Hukumonline
13	*Digital Ethics and Pancasila: Synergy for Student Transformation through digital technology innovation projects*	Firmansyah, R., dkk.	2025	Pancasila: Jurnal Keindonesiaan

3. Hasil dan Pembahasan

3.1. Pentingnya Perlindungan Data Pribadi di Zaman Digital

Kemajuan teknologi di era digital telah banyak mengubah cara orang berkomunikasi, bekerja, dan menggunakan layanan sehari-hari. Tapi di balik kemudahan tersebut, muncul tantangan baru, salah satunya adalah perlindungan data pribadi. Saat ini, data pribadi sudah dianggap sebagai aset yang sangat berharga, tapi juga rawan disalahgunakan, baik oleh pemerintah, perusahaan, maupun pihak yang tidak bertanggung jawab.

Pentingnya perlindungan data pribadi berakar pada hak atas privasi, yang merupakan

bagian dari hak asasi manusia. Laporan dari UNCTAD (2021) menyebutkan bahwa banyak negara berkembang belum punya aturan yang cukup kuat untuk melindungi data warganya. Hal ini membuat risiko pelanggaran privasi jadi semakin besar. Jika perlindungan datanya lemah, orang bisa jadi ragu untuk ikut aktif dalam dunia digital, dan ini bisa memperlambat inovasi maupun pertumbuhan ekonomi.

Selain itu, data yang bocor atau disalahgunakan bisa berdampak serius—mulai dari manipulasi opini publik, diskriminasi, hingga mengancam keamanan negara. Karena itu, perlindungan data tidak bisa dianggap sepele. Negara perlu punya aturan yang jelas dan menyeluruh, seperti prinsip data protection by design and by default, serta adanya lembaga pengawas independen yang punya kewenangan kuat.

Dengan demikian, di tengah cepatnya perkembangan teknologi, perlindungan data pribadi bukan hanya soal privasi, tapi juga bagian penting dari membangun ekosistem digital yang aman dan bisa dipercaya semua pihak.

3.2. Harapan dan Kenyataan dari UU PDP

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) adalah langkah besar bagi Indonesia dalam menghadapi tantangan perlindungan data di era digital. Sebelum ada UU ini, aturan soal data pribadi tersebar di berbagai sektor dan belum terkoordinasi dengan baik. Jadi, kehadiran UU PDP membawa harapan baru, masyarakat ingin ada perlindungan hukum yang lebih jelas dan kuat atas data pribadinya.

Banyak harapan yang melekat pada UU ini. Misalnya, masyarakat ingin mengetahui hak-hak mereka sebagai pemilik data, kewajiban pihak yang mengelola data, dan bagaimana hukuman bagi pelanggar dapat ditegakkan. Tak kalah penting, masyarakat juga menanti dibentuknya lembaga pengawas yang independen dan efektif dalam mengawasi praktik perlindungan data di lapangan. Seperti yang diungkapkan oleh Wijaya (2023), keberadaan lembaga pengawas independen akan mendorong kepercayaan publik terhadap pemerintah dan mitigasi risiko kejahatan siber.

Namun, realitasnya belum sesuai harapan. Salah satu masalah mendasar adalah belum terbentuknya otoritas pengawas data pribadi yang dijanjikan oleh UU PDP. Padahal, lembaga ini sangat penting untuk memastikan aturan dijalankan dengan benar. Selain itu, banyak pelaku usaha, terutama UMKM, masih belum sepenuhnya memahami apa yang harus mereka lakukan untuk mematuhi UU ini, sehingga ada risiko pelanggaran yang sebenarnya tidak disengaja (Universitas Medan Area, 2024).

Masalah lainnya, kebocoran data masih saja terjadi, meskipun UU sudah berlaku. Ini menunjukkan bahwa masih ada kekurangan dalam kemampuan teknis dan tata kelola data di berbagai instansi. Karena itu, dibutuhkan strategi nasional yang lebih menyeluruh, mulai dari edukasi ke publik, peningkatan kapasitas teknis, hingga penyesuaian aturan lain yang berkaitan.

Jadi, meskipun UU PDP adalah langkah maju yang penting, masih banyak pekerjaan

rumah yang harus diselesaikan agar perlindungan data pribadi benar-benar bisa dirasakan oleh masyarakat luas.

Untuk memahami lebih dalam keterbatasan implementasi UU PDP dan potensi penguatan kebijakan, penting juga melihat bagaimana negara lain merancang regulasi serupa. Salah satu rujukan global yang dapat dibandingkan adalah General Data Protection Regulation (GDPR) di Uni Eropa yang telah menjadi standar internasional dalam perlindungan data pribadi. Oleh karena itu, subbab selanjutnya membahas perbandingan antara UU PDP dan GDPR dari sisi kelembagaan dan norma pelaksanaannya.

3.3. Perbandingan UU PDP dengan GDPR: Evaluasi Kelembagaan dan Norma

Untuk memperkuat pemahaman terhadap kekuatan dan keterbatasan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, penting untuk membandingkannya dengan kerangka hukum internasional yang telah mapan, seperti General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa. GDPR tidak hanya menjadi acuan regional, tetapi juga rujukan global dalam perlindungan data pribadi.

Secara substansi, baik UU PDP maupun GDPR mengatur prinsip-prinsip penting seperti persetujuan eksplisit, transparansi, dan hak subjek data. Namun, terdapat perbedaan signifikan dari sisi kelembagaan dan implementasi. GDPR menetapkan pembentukan lembaga pengawas independen yang disebut European Data Protection Board (EDPB), yang memiliki kewenangan untuk menerima pengaduan, menjatuhkan sanksi, serta melakukan inspeksi. Sebaliknya, di Indonesia, hingga kini Otoritas Pelindungan Data Pribadi (OPDP) belum terbentuk, sehingga pengawasan belum dapat dilakukan secara efektif (Mahardika, 2021).

Dalam aspek penegakan hukum, GDPR menetapkan sanksi administratif yang tegas, yaitu denda hingga 20 juta Euro atau 4% dari pendapatan global tahunan perusahaan. Sementara itu, meskipun UU PDP juga mengatur sanksi administratif dan pidana, implementasinya masih lemah karena belum ada peraturan turunan dan belum pernah diterapkan secara nyata (Hertianto, 2021; European Commission, 2023).

Tabel 2 berikut menyajikan perbandingan singkat antara GDPR dan UU PDP.

Tabel 2. Perbandingan GDPR dan UU PDP.

Aspek	UU PDP (Indonesia)	GDPR (Uni Eropa)
Lembaga Pengawas	Belum terbentuk (OPDP)	EDPB (independen)
Dasar Hukum	UU No. 27 Tahun 2022	Regulasi EU 2016/679
Sanksi	Belum rinci, belum diterapkan	Tegas: hingga €20 juta atau 4% omzet
Hak Subjek Data	Tercantum, masih terbatas	Komprehensif: akses, koreksi, penghapusan, portabilitas

Aspek	UU PDP (Indonesia)	GDPR (Uni Eropa)
Kewajiban Pelaku	Belum spesifik	DPIA, DPO, notifikasi insiden

Perbandingan ini memperlihatkan bahwa Indonesia perlu mengakselerasi pembentukan OPDP, menetapkan standar teknis minimum, serta memperjelas mekanisme sanksi agar pelaksanaan UU PDP tidak hanya normatif, tetapi juga efektif di lapangan.

3.4. Kasus-Kasus Kebocoran Data Setelah UU PDP

Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sudah disahkan untuk memperkuat perlindungan informasi pribadi, kasus kebocoran data dalam skala besar masih terus terjadi. Hal ini menunjukkan bahwa keberadaan aturan saja belum cukup jika tidak diiringi dengan pelaksanaan teknis yang memadai dan pengawasan yang benar-benar efektif.

Salah satu contoh besar terjadi pada tahun 2023, yaitu dugaan kebocoran data pemilih dari Komisi Pemilihan Umum (KPU). Lebih dari 200 juta data warga Indonesia, termasuk Nomor Induk Kependudukan (NIK), alamat, dan informasi pribadi lainnya, diklaim dijual di forum dark web (CNN Indonesia, 2023). Meskipun pihak KPU membantah sepenuhnya, kasus ini tetap menimbulkan kekhawatiran besar, apalagi menjelang tahun politik. Pemerintah pun mengakui bahwa audit forensik dan peningkatan sistem keamanan sangat dibutuhkan.

Kasus lainnya datang dari dunia e-commerce. Tokopedia dilaporkan mengalami kebocoran data lebih dari 91 juta akun pengguna, termasuk email, nama pengguna, dan kata sandi yang sudah terenkripsi (Kompas, 2023). Meski kejadian ini terjadi sebelum UU PDP resmi berlaku, dampaknya masih terasa setelahnya, dan turut mendorong kesadaran publik serta pelaku usaha tentang pentingnya perlindungan data.

Kedua insiden ini memperlihatkan masih besarnya jarak antara regulasi yang sudah dibuat dan kesiapan infrastruktur teknis di lapangan. Banyak lembaga di Indonesia belum memiliki sistem perlindungan data yang memadai, baik dari sisi teknologi maupun dari tata kelola organisasi (Putri, 2025).

Karena itu, agar perlindungan data pribadi bisa berjalan lebih baik, diperlukan langkah-langkah serius seperti peningkatan kapasitas lembaga, audit keamanan yang dilakukan secara berkala, serta pembentukan otoritas perlindungan data yang benar-benar independen dan mampu menjalankan pengawasan secara efektif.

3.5. Tantangan dalam Penegakan Hukum

Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sudah menjadi dasar hukum penting untuk melindungi data pribadi, penegakannya masih menghadapi banyak tantangan. Salah satu masalah utamanya adalah sedikitnya kasus kebocoran data yang benar-benar diproses secara hukum, padahal insiden seperti itu terus terjadi. Salah satu penyebabnya adalah belum

terbentuknya lembaga pengawas independen yang seharusnya bertugas sebagai otoritas penegakan UU PDP (Fourtrezz, 2024).

Masalah lainnya adalah belum jelasnya cara menerapkan sanksi yang diatur dalam UU PDP. Meskipun undang-undang ini sudah memuat ancaman sanksi administratif dan pidana, mekanisme teknisnya, seperti cara menentukan tingkat pelanggaran dan jenis sanksinya, belum diatur secara rinci dalam aturan turunannya. Menurut Djafar (2024), ketiadaan lembaga pengawas menyebabkan masyarakat kebingungan harus mengadu ke mana ketika terjadi insiden kebocoran data pribadi, dan penegakan hukum menjadi tidak efektif.

Tantangan tambahan datang dari rendahnya kesadaran dan kemampuan teknis para pengelola sistem elektronik, baik di sektor publik maupun swasta. Banyak organisasi belum punya sistem perlindungan data yang baik, sehingga proses investigasi dan pembuktian pelanggaran jadi rumit dan memakan waktu. Sementara itu, korban kebocoran data juga sering tidak tahu harus melapor ke mana, atau bagaimana memperjuangkan haknya—yang membuat akuntabilitas makin lemah.

Karena itu, agar UU PDP bisa ditegakkan secara efektif, tidak cukup hanya dengan aturan hukum. Diperlukan juga lembaga pengawas yang bekerja optimal, SDM yang punya keahlian teknis, serta panduan operasional yang jelas dan bisa dijalankan dalam praktik.

Ketiadaan lembaga pengawas independen merupakan kelemahan mendasar dalam struktur pelaksanaan UU PDP. Dalam praktiknya, penegakan hukum menjadi tidak terkoordinasi dan kehilangan fokus institusional. Padahal, dalam sistem hukum modern, otoritas pengawasan merupakan elemen krusial dalam memastikan kepatuhan serta pemulihan hak korban.

Selain itu, ketidakjelasan teknis mengenai mekanisme pelaporan, investigasi insiden, dan pemberian sanksi menyebabkan keraguan pada efektivitas hukum. Meskipun undang-undang telah mengatur ancaman pidana dan administratif, tanpa peraturan pelaksana yang operasional dan dapat diterapkan, norma tersebut berisiko menjadi simbolik semata (symbolic legislation). Hal ini memperlihatkan adanya jurang antara desain normatif dan implementasi praktis dalam penegakan hukum perlindungan data pribadi.

3.6. Kesiapan Infrastruktur Keamanan Siber

Kesiapan infrastruktur keamanan siber adalah bagian penting dalam mendukung pelaksanaan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Tanpa sistem yang kuat, perlindungan data pribadi sulit dijalankan secara optimal dan berkelanjutan.

Dari sisi kemajuan, Indonesia sudah melakukan beberapa langkah positif. Salah satunya lewat pembentukan Badan Siber dan Sandi Negara (BSSN) yang menjadi koordinator utama keamanan siber nasional. BSSN (2023) mencatat bahwa sistem deteksi dini dan pusat operasi keamanan siber (Security Operations Center/SOC) sudah mulai

dikembangkan di berbagai sektor penting. Pemerintah juga terus mendorong peningkatan literasi keamanan siber lewat pelatihan dan kerja sama internasional.

Selain itu, banyak institusi bergantung pada sistem pihak ketiga tanpa pengawasan ketat, yang justru memperbesar risiko kebocoran data. RSM Indonesia (2024) juga menyoroti lemahnya standar minimum keamanan yang wajib dipenuhi oleh penyelenggara sistem elektronik, yang membuat tingkat perlindungan antar sektor jadi tidak seimbang.

Salah satu isu krusial dalam kesiapan infrastruktur adalah ketimpangan standar keamanan antar sektor. Banyak lembaga pemerintahan masih menggunakan sistem keamanan dasar, bahkan tanpa enkripsi yang memadai. Di sisi lain, perusahaan teknologi besar sudah memiliki SOC (Security Operations Center) yang jauh lebih mutakhir.

Ketimpangan ini memperbesar potensi kerentanan sistemik, karena pelanggaran di satu titik dapat berdampak lintas sektor. Selain itu, tidak adanya kewajiban audit independen berkala membuat celah keamanan sering tidak terdeteksi. Negara perlu menetapkan standar nasional minimal keamanan siber, sebagaimana diterapkan dalam GDPR melalui kewajiban Data Protection Impact Assessment (DPIA).

Kurangnya kesiapan ini membuat hak pemilik data belum sepenuhnya terlindungi, dan pelaksanaan aturan teknis seperti kewajiban notifikasi insiden kebocoran pun jadi terhambat. Karena itu, Indonesia perlu memperkuat infrastrukturnya secara menyeluruh, menetapkan standar keamanan nasional yang mengikat, serta mewajibkan audit keamanan siber bagi semua penyelenggara sistem elektronik.

3.7. Rendahnya Kesadaran dan Kepatuhan

Keberhasilan penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sangat bergantung pada tingkat kesadaran dan kepatuhan dari masyarakat serta organisasi. Sayangnya, banyak individu yang belum sepenuhnya memahami hak-haknya terkait data pribadi. Menurut survei yang dilakukan oleh Kementerian Komunikasi dan Informatika bersama Katadata Insight Center pada tahun 2021, lebih dari 60% responden tidak mengetahui adanya Rancangan Undang-Undang Perlindungan Data Pribadi, dan hanya 31,8% perusahaan yang menyadari keberadaan rancangan undang-undang tersebut.

Di sisi organisasi, baik sektor swasta maupun pemerintah daerah, banyak yang belum menerapkan prinsip dasar perlindungan data seperti transparansi, akuntabilitas, dan minimisasi data. Hal ini sebagian besar disebabkan oleh kurangnya tenaga ahli di bidang perlindungan data serta kurangnya investasi dalam sistem keamanan data yang memadai. Menurut Hertianto (2021), sistem penegakan hukum terhadap kegagalan perlindungan data pribadi di Indonesia masih belum berjalan efektif, disebabkan oleh belum adanya pengaturan yang jelas, pelaku penyerangan yang anonim, serta kualitas aparat penegak hukum yang masih terbatas.

Kurangnya kesadaran ini berdampak pada lambatnya proses kepatuhan terhadap UU PDP. Banyak organisasi yang belum menunjuk petugas perlindungan data (DPO) atau belum memiliki kebijakan privasi yang jelas. Bahkan, ketika terjadi kebocoran data, insiden tersebut sering tidak segera dilaporkan, meskipun UU PDP mewajibkan notifikasi dalam waktu tertentu.

Untuk itu, untuk meningkatkan pemahaman dan kepatuhan, pemerintah perlu mengadakan program edukasi publik secara lebih luas, melakukan audit dan sertifikasi perlindungan data, serta memberikan sanksi tegas bagi pelanggar. Tanpa dukungan dari masyarakat dan pelaku industri, perlindungan data pribadi di Indonesia akan sulit berjalan dengan baik.

Lemahnya kesadaran publik bukan hanya persoalan individu, tetapi merupakan indikasi kegagalan sistemik dalam pendidikan literasi digital. Negara belum menjalankan peran promotif secara optimal, seperti kampanye nasional yang masif dan berkelanjutan terkait hak privasi dan perlindungan data.

Di sisi pelaku usaha, belum ada insentif atau paksaan hukum yang cukup kuat untuk mendorong kepatuhan. Penunjukan petugas perlindungan data (DPO), penyusunan kebijakan privasi, dan transparansi pemrosesan data belum menjadi kewajiban tegas. Dalam konteks ini, pemerintah perlu meniru pendekatan compliance-driven seperti di GDPR, di mana pelanggaran dapat berdampak finansial besar dan reputasional serius.

3.8. Dampak Sosial dan Ekonomi dari Kebocoran Data

Kebocoran data dalam skala besar di Indonesia tidak hanya berdampak pada pelanggaran hak individu, tetapi juga menimbulkan konsekuensi serius terhadap aspek sosial dan ekonomi. Salah satu dampak yang paling nyata adalah kerugian finansial yang dialami oleh individu maupun organisasi. Data pribadi yang bocor dapat dimanfaatkan untuk penipuan identitas, pencurian dana, atau transaksi tidak sah yang merugikan korban. Hertianto (2021) mencatat bahwa insiden kebocoran data pada platform e-commerce atau lembaga pemerintah seringkali menjadi celah bagi pelaku kejahatan siber, dan penegakan hukum terhadap kegagalan perlindungan data pribadi masih belum berjalan efektif.

Di samping itu, reputasi organisasi yang mengalami kebocoran data juga akan terpengaruh secara negatif. Kegagalan dalam menjaga keamanan data dapat mengakibatkan penurunan kepercayaan publik dan berujung pada berkurangnya jumlah pengguna atau pelanggan. RSM Indonesia (2024) menunjukkan bahwa insiden kebocoran data cenderung berdampak pada kinerja bisnis, termasuk perlambatan pertumbuhan dan rusaknya hubungan jangka panjang dengan konsumen.

Kepercayaan masyarakat terhadap ekosistem digital pun berpotensi menurun. Ketika keamanan data pribadi diragukan, masyarakat menjadi enggan untuk memanfaatkan layanan digital, termasuk layanan keuangan dan administrasi publik. Hal ini dapat menghambat laju transformasi digital nasional, yang menjadi salah satu prioritas pemerintah dalam mewujudkan pertumbuhan ekonomi berbasis teknologi (RSM

Indonesia, 2024).

Secara keseluruhan, kebocoran data tidak hanya merugikan secara individu atau organisasi, tetapi juga dapat mengganggu stabilitas sosial dan memperlambat kemajuan ekonomi digital Indonesia.

3.9. Rekomendasi untuk Perbaikan

Untuk menjamin efektivitas penerapan UU No. 27 Tahun 2022 mengenai Perlindungan Data Pribadi, diperlukan sejumlah strategi penguatan yang bersifat menyeluruh. Langkah-langkah ini penting untuk memastikan pengawasan berjalan optimal dan tingkat kepatuhan terhadap aturan semakin meningkat.

Pertama, pembentukan Otoritas Perlindungan Data Pribadi (OPDP) yang independen perlu segera direalisasikan. Mahardika (2021) menyatakan bahwa pembentukan otoritas independen perlindungan data pribadi sangat penting sebagai upaya kehadiran negara untuk menjamin hak privasi setiap warga negara. Tanpa keberadaan lembaga pengawas yang kuat, pelaksanaan UU PDP akan sulit mencapai tujuannya.

Kedua, peningkatan kesadaran publik dan pelaku usaha mengenai pentingnya perlindungan data pribadi menjadi hal yang mendesak. Sari (2024) mengungkapkan bahwa pemahaman publik terhadap hak mereka sebagai pemilik data masih tergolong rendah. Oleh karena itu, diperlukan kampanye edukasi yang luas serta pelatihan bagi organisasi untuk mendorong kepatuhan terhadap prinsip perlindungan data.

Ketiga, keberadaan sanksi yang tegas dan mekanisme audit yang transparan harus diperkuat. Mengacu pada praktik di Uni Eropa melalui GDPR, sanksi administratif berupa denda yang besar dapat memberikan efek jera bagi pelanggar (European Commission, 2023). Model tersebut dapat dijadikan contoh dalam membentuk sistem penegakan hukum yang lebih solid dan lebih kuat di Indonesia.

Dengan menerapkan strategi-strategi tersebut secara konsisten, UU PDP diharapkan mampu memberikan perlindungan yang optimal terhadap data pribadi serta meningkatkan kepercayaan masyarakat terhadap ekosistem digital nasional.

4. Kesimpulan

Implementasi Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia masih menghadapi berbagai tantangan serius meskipun telah menjadi kerangka hukum tunggal untuk melindungi data pribadi. Masalah utama yang ditemukan meliputi belum terbentuknya Otoritas Perlindungan Data Pribadi (OPDP), rendahnya infrastruktur keamanan siber, serta kurangnya kesadaran masyarakat dan pelaku usaha akan pentingnya perlindungan data. Kasus kebocoran data besar seperti pada KPU menunjukkan bahwa meskipun regulasi sudah ada, penegakan hukum masih lemah dan tidak transparan.

Untuk meningkatkan efektivitas UU PDP, diperlukan pembentukan OPDP yang independen, peningkatan literasi digital, serta penguatan sistem keamanan siber secara

nasional. Selain itu, integrasi nilai-nilai etika digital dan Pancasila juga perlu dipertimbangkan untuk membentuk budaya digital yang bertanggung jawab. Bagi peneliti selanjutnya, disarankan untuk menggunakan metode penelitian yang lebih empiris seperti studi kasus, wawancara, atau survei guna memperoleh data yang lebih aktual dan mendalam mengenai implementasi UU PDP di lapangan.

Daftar Referensi

Asia Society. (2021). *Raising standards for data and AI in Southeast Asia: Indonesia*. https://asiasociety.org/policy-institute/raising-standards-data-ai-southeast-asia/data/indonesia

Badan Siber dan Sandi Negara. (2023). *Laporan tahunan keamanan siber nasional 2023*. https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

Center for Indonesian Policy Studies. (2022, September 20). *Measuring state's commitment to implementing PDP law*. https://www.cips-indonesia.org/post/measuring-state-s-commitment-to-implementing-pdp-law-1

CNN Indonesia. (2023, November 23). *Kebocoran data KPU: 204 juta data pemilih diduga bocor*. https://www.cnnindonesia.com/nasional/20231123164923-12-1028711/kebocoran-data-kpu-204-juta-data-pemilih-diduga-bocor

Djafar, W. (2024, Desember 20). *Lembaga pengawas belum terbentuk, pengaduan kebocoran data pun jadi tak jelas*. Kompas.id. https://www.kompas.id/artikel/lembaga-pengawas-belum-terbentuk-pengaduan-kebocoran-data-tak-jelas

European Commission. (2023). *General Data Protection Regulation (GDPR) and European Data Protection Board (EDPB)*. https://gdpr-info.eu/

Firmansyah, R., Hamzah, S., & Almuntarizi. (2025). Digital ethics and Pancasila: Synergy for student transformation through digital technology innovation projects. *Pancasila: Jurnal Keindonesiaan, 5*(1), 89–100. https://doi.org/10.52738/pjk.v5i1.673

Fourtrezz. (2024, Februari 20). *UU PDP: Apakah cukup untuk melindungi data pribadi di Indonesia?* https://fourtrezz.co.id/uu-pdp-apakah-cukup-untuk-melindungi-data-pribadi-di-indonesia/

Hertianto, M. R. (2021). Sistem penegakan hukum terhadap kegagalan dalam perlindungan data pribadi di Indonesia. *Kertha Patrika, 43*(1), 85–100. https://doi.org/10.24843/KP.2021.v43.i01.p07

Kompas. (2023, Januari 17). *Data 91 juta akun Tokopedia bocor, ini penjelasan perusahaan*. https://www.kompas.com/global/read/2020/05/03/133257970/data-91-juta-pengguna-tokopedia-diduga-bocor-media-asing-ikut-soroti

Mahardika, A. M. (2021). Desain ideal pembentukan otoritas independen perlindungan data pribadi dalam sistem ketatanegaraan Indonesia. *Jurnal Hukum, 37*(2), 213–230. http://dx.doi.org/10.26532/jh.v37i2.16994

Putri, W. A. (2025, Januari 11). *4 tantangan implementasi UU PDP di perusahaan dan solusi efektifnya*. Cloud Helios. https://cloud.helios.id/id/blog/4-tantangan-implementasi-uu-pdp-di-perusahaan-dan-solusi-efektifnya/

RSM Indonesia. (2024, Oktober 5). *Preparing for Indonesia's new data protection law: What your business needs to know*. https://www.rsm.global/indonesia/en/insights/preparing-indonesias-new-data-protection-law-what-your-business-needs-know

Sari, N. (2024). An analysis of the gap between data protection regulations and implementation in Indonesia. *Easta Journal of Law and Human Rights, 3*(2), 87–104. https://esj.eastasouth-institute.com/index.php/eslhr/article/download/351/293/2740

Tambunan, S. L. A., Musa, A., & Nachrawy, N. (2024). Urgensi pembentukan lembaga pelindungan data pribadi yang independen berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Lex Crimen, 12*(4), 45–60. https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/58892

UNCTAD. (2021). *Data protection and privacy legislation worldwide*. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Universitas Medan Area. (2024, September 14). *Analisis hukum terhadap perlindungan data pribadi di Indonesia*. Fakultas Hukum UMA. https://hukum.uma.ac.id/2024/09/14/analisis-hukum-terhadap-perlindungan-data-pribadi-di-indonesia/

Wijaya, T. (2023, Mei 15). *Menyorot independensi lembaga pengawas data pribadi*. Hukumonline. https://www.hukumonline.com/berita/a/menyorot-independensi-lembaga-pengawas-data-pribadi-lt6461f9e088aeb