Vol 1 No. 2, November 2025
E-ISSN: 3110-3898; P-ISSN: 3110-4657; Page 123-131

Paradigma Baru Perlindungan Data Pribadi di Indonesia: Analisis Normatif-Komparatif UU No. 27 Tahun 2022 dan Tantangan Pembentukan Otoritas Pengawas Independen

Rhema Rosa Purnama Esther Manurung[1*]

[1*]Universitas Pembangunan Nasional Veteran, Jakarta, Indonesia
2210611464@mahasiswa.upnvj.ac.id

ABSTRAK

Perubahan lanskap digital di Indonesia menuntut hadirnya kerangka hukum yang mampu memberikan perlindungan memadai terhadap data pribadi sebagai bagian dari hak fundamental warga negara. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan tonggak penting karena untuk pertama kalinya Indonesia memiliki regulasi khusus yang mengatur pengumpulan, pemrosesan, dan distribusi data pribadi secara menyeluruh. Penelitian ini menganalisis paradigma baru perlindungan data melalui pendekatan normatif-komparatif dengan meninjau kesesuaian ketentuan UU PDP dengan prinsip-prinsip GDPR serta mengkaji kesiapan Indonesia dalam membentuk otoritas pengawas independen. Hasil analisis menunjukkan bahwa meskipun UU PDP telah mengadopsi berbagai prinsip penting seperti lawfulness, transparency, purpose limitation, dan accountability, Indonesia masih menghadapi tantangan serius pada aspek kelembagaan, termasuk potensi tumpang tindih kewenangan, keterbatasan sumber daya, serta belum adanya model lembaga independen yang sepenuhnya bebas dari pengaruh eksekutif. Studi ini menegaskan bahwa keberhasilan implementasi UU PDP sangat ditentukan oleh kejelasan desain institusi pengawas, harmonisasi regulasi sektoral, serta penguatan mekanisme penegakan hukum dan literasi digital masyarakat.

***Kata Kunci**: Perlindungan Data Pribadi; UU PDP; GDPR; Otoritas Pengawas Independen; Regulasi Digital.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang sangat cepat saat ini telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan peranan teknologi informasi menjadi suatu hal yang penting untuk digunakan dalam berbagai sektor kehidupan.

Submitted: 19-09-2025
Revised: 17-10-2025
Acepted: 20-11-2025

Fenomena digitalisasi yang masif telah menciptakan berbagai aktivitas digital, mulai dari *electronic government* (*e-government*) hingga *cloud computing*. Namun, kemajuan teknologi juga diibaratkan sebagai "pedang bermata dua" karena pada satu sisi menawarkan efisiensi, tetapi pada sisi lain juga membawa permasalahan hukum yang krusial, terutama masalah kerahasiaan dokumen atau privasi.

Penggunaan teknologi yang masif ini telah melahirkan berbagai aktivitas seperti *electronic government* (*e-government*), *electronic commerce* (*e-commerce*), dan *cloud computing*. Dalam konteks ini, data pribadi telah bertransformasi menjadi komoditas yang sangat berharga dan menjadi target komersialisasi, manipulasi informasi, dan kejahatan siber. Era transformasi digital telah mengubah data menjadi suatu aset yang berharga bagi seluruh sektor. Pengelolaan data yang baik menjadi kunci untuk pengambilan keputusan. Pasalnya, data tidak hanya sebatas kumpulan informasi melainkan perlu diidentifikasi sesuai konteks dan maknanya (Tasya, 2024). Mengingat setiap individu secara pribadi menghasilkan data-data ini, hal tersebut menimbulkan pertanyaan tentang bagaimana seseorang dapat memperoleh manfaat ekonomi dari data mereka sendiri, dan yang lebih penting, hak untuk menentukan bagaimana data tersebut digunakan dan dibagikan dengan pihak ketiga.

Dalam beberapa tahun terakhir, Indonesia telah mengalami serangkaian kasus kebocoran data pribadi yang melibatkan berbagai institusi dan platform digital, mengakibatkan terekspos nya informasi sensitif milik jutaan warga. Rentetan insiden ini menunjukkan masih banyaknya loopholes atau celah hukum dalam perlindungan data pribadi yang diakibatkan oleh kekosongan dan ketidakpastian hukum perlindungan data pribadi di Indonesia (Imanullah, 2025). Selama bertahun-tahun, perlindungan data pribadi di Indonesia terfragmentasi dalam sejumlah peraturan sektoral, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Kondisi fragmentasi ini berujung pada inkonsistensi dalam penerapan hukum, ketidakjelasan mengenai kewenangan, dan lemahnya mekanisme penegakan hukum terhadap pelanggaran data pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) muncul sebagai langkah signifikan dalam sistem hukum Indonesia, bertujuan untuk menyediakan kerangka hukum yang lebih menyeluruh dan terpusat. Kehadiran UU PDP memberikan penegasan bahwa data pribadi dilindungi oleh hukum sebagai bagian dari hak asasi manusia, sejalan dengan Pasal 28G ayat (1) UUD 1945, yang menegaskan bahwa setiap individu berhak mendapatkan perlindungan terkait diri pribadi, keluarga, kehormatan, martabat, serta harta benda yang berada di bawah penguasaan mereka. Secara luas, undang-undang ini mencakup aspek yang berlaku baik di dalam maupun di luar wilayah Indonesia, dengan dampak hukum yang tetap berlaku di tanah air.

METODE

Metode penelitian yang digunakan dalam penulisan ini adalah yuridis-normatif. Penelitian yuridis-normatif dilakukan dengan cara meneliti bahan pustaka atau bahan sekunder. Hal ini sejalan dengan pengertian bahwa penelitian hukum normatif adalah penelitian hukum yang dilaksanakan melalui studi pustaka. Penelitian ini bersifat deskriptif-analitis. Pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*), yang dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani. Selain itu, penelitian ini

juga menggunakan pendekatan komparatif (*comparative approach*) atau disebut juga dengan pendekatan perbandingan, melalui studi perbandingan hukum deskriptif. Sumber data yang dimanfaatkan meliputi bahan hukum primer, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK), Kitab Undang-Undang Hukum Perdata (KUHPerdata), dan General Data Protection Regulation (GDPR). Sementara itu, bahan hukum sekunder terdiri dari buku, jurnal, dan karya tulis ilmiah lainnya yang berkaitan dengan isu perlindungan data pribadi. Analisis data dilakukan secara kualitatif untuk mengkaji norma hukum dan kesesuaiannya dengan praktik implementasi, khususnya dalam mengukur efektivitas keberlakuan norma hukum yang telah ditetapkan.

HASIL DAN PEMBAHASAN

Paradigma Regulasi Perlindungan Data Pribadi dalam UU No. 27 Tahun 2022

UU No. 27 Tahun 2022 menunjukkan perubahan signifikan terhadap struktur perlindungan data pribadi di Indonesia dengan menempatkan hak privasi sebagai bagian dari hak konstitusional warga negara sebagaimana diatur dalam UUD 1945 (Undang-Undang Dasar 1945). Penguatan ini memberikan landasan normatif bagi pengaturan teknis perlindungan data yang sebelumnya tersebar dalam berbagai regulasi sektoral seperti UU ITE dan PP 71/2019 (Undang-Undang 11/2008). Kebutuhan akan regulasi khusus muncul akibat meningkatnya arus digitalisasi di berbagai sektor, mulai dari pelayanan kesehatan hingga transaksi keuangan (Nusantara, 2024). Transformasi digital tersebut memperbesar risiko kebocoran data pribadi sehingga mendorong negara untuk membentuk regulasi yang lebih terstruktur.

UU No. 27 Tahun 2022 menghadirkan struktur kewajiban yang lebih tegas bagi pengendali data dan prosesor data, suatu model pengaturan yang sebelumnya banyak didorong oleh literatur hukum dan GDPR Uni Eropa (Kusumadewi, 2023). Kewajiban tersebut meliputi dasar pemrosesan, transparansi, keamanan teknis, dan respons terhadap insiden kebocoran data. Ketentuan ini memperkuat hak subjek data seperti hak akses, hak perbaikan, hak penghapusan, dan hak keberatan, yang sebelumnya tidak diakomodasi secara eksplisit. Perluasan hak subjek data ini memperlihatkan arah harmonisasi Indonesia terhadap standar internasional.

Kebutuhan harmonisasi ini terlihat dari meningkatnya insiden kebocoran data yang tercatat oleh berbagai lembaga pemantau keamanan digital di kawasan Asia Tenggara. Indonesia menjadi salah satu negara dengan jumlah insiden tertinggi dalam kurun waktu 2020–2023, sebagaimana ditunjukkan dalam data Cybersecurity Malaysia dan laporan Kaspersky tahun 2023. Peningkatan insiden tersebut memperkuat urgensi penyusunan UU Perlindungan Data Pribadi sebagai kerangka hukum yang komprehensif (Wulansari, 2020). Berikut adalah tabel insiden kebocoran data yang menjadi landasan perlunya regulasi baru:

Tabel 1. Jumlah Insiden Kebocoran Data di Asia Tenggara (2020–2023)

Negara	2020	2021	2022	2023
Indonesia	102	159	196	232
Malaysia	41	58	63	71
Singapura	29	34	41	46
Thailand	38	56	62	70

Sumber: Kaspersky Cybersecurity Report 2023

Peningkatan angka insiden pada tabel menunjukkan bahwa Indonesia berada dalam posisi rawan kegagalan pengendalian data, terutama menyangkut lembaga publik yang kerap menjadi sasaran serangan siber. Ketiadaan otoritas pengawas independen pada periode sebelum UU PDP mengakibatkan koordinasi penanganan insiden berjalan tidak sistematis (Halbert, 2023). UU No. 27/2022 mencoba mengisi kekosongan tersebut melalui pengaturan mengenai kewajiban pelaporan insiden kepada subjek data dan pemerintah. Namun efektivitas norma tersebut masih bergantung pada institusi mana yang nantinya akan ditetapkan sebagai otoritas pengawas.

Penentuan otoritas pengawas merupakan salah satu perdebatan utama dalam diskursus implementasi UU PDP karena menyangkut masalah independensi, kewenangan investigatif, dan kapasitas institusional (Khansa, 2021). Otoritas yang ideal seharusnya memiliki karakter quasi-independent seperti KPPU, sebagaimana direkomendasikan beberapa pakar hukum administrasi (Matheus, 2024). Model pengawasan independen diperlukan untuk menjamin akuntabilitas penyelenggara sistem elektronik, khususnya sektor privat yang kerap mengumpulkan data dalam jumlah besar. Ketidakjelasan lembaga pengawas akan menimbulkan kekosongan penegakan hukum pada fase implementasi awal.

Perbandingan regulasi dengan Malaysia dan Uni Eropa memperlihatkan bahwa keberadaan data protection authority (DPA) menjadi elemen utama keberhasilan pelindungan data pribadi (Rizal, 2019). Di Uni Eropa misalnya, kehadiran European Data Protection Board mampu memastikan konsistensi kebijakan antarnegara anggota GDPR. Model pengaturan ini memberikan pembelajaran penting bagi Indonesia mengenai perlunya lembaga yang mampu mengkoordinasikan kebijakan antar-sektor, terutama perbankan, kesehatan, dan pendidikan. UU PDP telah menempatkan gagasan tersebut, tetapi belum memberikan bentuk kelembagaan final.

Penelitian hukum normatif menunjukkan bahwa kepastian hukum hanya dapat dicapai ketika norma pengaturan diikuti oleh kelembagaan yang memadai (Soekanto, 2003). Tanpa itu, hak subjek data yang dijamin oleh UU PDP berpotensi tidak dapat dieksekusi secara efektif. Hal ini juga ditegaskan oleh literatur hukum yang menyoroti potensi tumpang tindih kewenangan antara Kementerian Kominfo, OJK, dan lembaga sektor lainnya (Kholis, 2024). Kepastian kelembagaan menjadi prasyarat utama transisi menuju rezim perlindungan data modern.

Secara umum, UU PDP telah meletakkan fondasi normatif yang kuat bagi pembaruan tata kelola data di Indonesia, namun instrumen pendukungnya masih memerlukan optimalisasi. Pengaturan mengenai hak subjek data menunjukkan kemajuan berarti dalam perlindungan privasi warga negara. Penguatan dasar pemrosesan dan kewajiban pengendali data memperlihatkan arah Indonesia menuju standar internasional seperti GDPR. Tantangan berikutnya terletak pada pembentukan otoritas pengawas independen yang mampu menjalankan mandat pengawasan secara profesional dan berkelanjutan (Ayiliani, 2024).

Kebutuhan Reformasi Regulasi dan Kesenjangan Normatif UU PDP

Kerangka hukum perlindungan data pribadi yang diatur dalam UU No. 27 Tahun 2022 menunjukkan kemajuan signifikan, tetapi norma yang tersedia masih belum sepenuhnya menjawab kebutuhan masyarakat digital yang semakin kompleks. Ketentuan mengenai persetujuan, pemrosesan, dan hak subjek data masih membutuhkan penafsiran lebih matang agar implementasinya tidak menimbulkan ketidakpastian bagi

penyelenggara sistem elektronik. Situasi ini terlihat dari meningkatnya laporan kebocoran data yang melibatkan berbagai sektor, mulai dari kesehatan, keuangan, hingga pendidikan. Fenomena tersebut memperlihatkan bahwa perkembangan teknologi bergerak lebih cepat dibandingkan penguatan norma yang dirancang oleh pembuat kebijakan (Wulansari, 2020).

Kesenjangan normatif UU PDP juga tampak pada aspek pengawasan, sebab undang-undang tersebut belum memberikan desain kelembagaan yang final terkait otoritas independen yang bertugas mengawasi pemrosesan data. Ketidakjelasan ini memunculkan ketidakseimbangan antara kewenangan pemerintah dan hak warga negara atas privasi sebagaimana dijamin dalam UUD 1945 dan UU HAM. Dalam berbagai studi hukum tata negara, ketidakpastian kelembagaan sering kali memengaruhi efektivitas penegakan hukum di bidang yang sangat teknis, termasuk siber dan perlindungan data (Halbert, 2023). Situasi ini menunjukkan perlunya reformulasi norma secara segera agar pelaksanaan perlindungan data memiliki landasan kelembagaan yang kuat.

Untuk menggambarkan urgensi reformasi regulasi, data mengenai insiden kebocoran data global dapat dijadikan ilustrasi mengenai skala risiko yang dihadapi Indonesia. Laporan IBM Cost of Data Breach 2023 menunjukkan bahwa rata-rata kerugian akibat kebocoran data mencapai miliaran rupiah per insiden dan meningkat setiap tahun. Tren ini berpengaruh langsung terhadap kebutuhan harmonisasi hukum nasional dengan standar global yang lebih matang, seperti GDPR Uni Eropa (Kusumadewi & Cahyono, 2023). Data berikut memperlihatkan dinamika perubahan angka kerugian dalam tiga tahun terakhir:

Tabel 2. Rata-Rata Kerugian Kebocoran Data Global (IBM, 2021–2023)

Tahun	Rata-Rata Kerugian (USD)
2021	4,24 juta USD
2022	4,35 juta USD
2023	4,45 juta USD

Sumber: IBM Security – Cost of Data Breach Report 2023

Angka dalam tabel tersebut memberikan gambaran bahwa risiko kebocoran data memiliki dimensi ekonomi yang tidak dapat diabaikan oleh regulator. Indonesia sebagai negara dengan populasi digital terbesar keempat di dunia berada pada posisi yang rawan, sehingga diperlukan formulasi kebijakan yang lebih tegas terkait mitigasi risiko kebocoran data. UU PDP sebenarnya menyediakan kerangka dasar berupa kewajiban keamanan data, tetapi norma ini belum disertai standar teknis yang dapat dijadikan pedoman operasional bagi pelaku usaha maupun instansi publik (Pranoto, 2024). Kondisi ini menyebabkan kepatuhan berjalan secara bervariasi dan tidak seragam di setiap sektor.

Kelemahan desain regulasi juga terlihat dari belum adanya mekanisme sanksi administratif yang benar-benar operasional, sebab tanpa otoritas pengawas independen, kewenangan menjatuhkan sanksi masih tersebar di berbagai instansi. Fragmentasi kewenangan tersebut berpotensi menyulitkan pengawasan, terutama untuk kasus lintas sektor seperti kebocoran data keuangan yang merembet pada layanan e-commerce atau kesehatan. Model pengawasan terpusat seperti pada GDPR memberikan preseden bahwa satu lembaga independen jauh lebih efektif dalam menjamin perlindungan hak subjek data (Khansa, 2021). Indonesia memerlukan pola serupa agar penegakan hukum berjalan lebih terstruktur dan sistematis.

UU PDP juga belum sepenuhnya mengatur mekanisme remediasi bagi korban

kebocoran data, terutama terkait kompensasi dan bentuk pemulihan non-materiil. KUHPerdata memang memberikan landasan ganti rugi, tetapi kerangka perlindungan data membutuhkan norma yang lebih spesifik karena sifat kerugian digital tidak selalu dapat dihitung secara material (Soekanto & Mahmudji, 2003). Ketidakjelasan ini menjadikan posisi subjek data tidak begitu kuat ketika berhadapan dengan penyelenggara sistem elektronik berskala besar. Reformasi norma perlu diarahkan pada penguatan hak subjek data secara substantif agar mereka tidak hanya menjadi objek pemrosesan data, tetapi juga pemilik kendali atas informasi pribadi mereka.

Isu lain yang masih mengemuka adalah ketidaksiapan infrastruktur keamanan data pada berbagai layanan publik. Penelitian mengenai BPJS Kesehatan menunjukkan bahwa sistem informasi publik sering kali menghadapi serangan siber karena belum menerapkan standar keamanan yang memadai (Nusantara, 2024). Jika situasi tersebut tidak diatasi, maka penguatan norma hukum tidak akan memberikan hasil yang optimal. Regulasi teknis seperti PP 71/2019 perlu diperbaharui agar sejalan dengan UU PDP dan memberikan standar keamanan yang lebih ketat bagi semua pengendali data.

Keseluruhan tantangan normatif ini memperlihatkan kebutuhan mendesak untuk merapikan struktur regulasi perlindungan data pribadi. Kelemahan norma bukan hanya berpengaruh pada aspek kepastian hukum, tetapi juga berdampak pada kepercayaan publik terhadap layanan digital. Dalam kondisi masyarakat yang semakin bergantung pada transaksi elektronik, kepercayaan menjadi faktor yang sangat menentukan keberlanjutan pembangunan ekonomi digital (Rizal, 2019). Kesenjangan norma dalam UU PDP menunjukkan bahwa reformulasi wajib dilakukan agar ekosistem digital Indonesia dapat berkembang dengan aman dan berkelanjutan.

Tantangan Implementasi UU PDP dalam Praktik

Penerapan UU Nomor 27 Tahun 2022 masih menghadapi hambatan serius pada tahap operasional karena sebagian besar pengendali data belum sepenuhnya memahami standar kewajiban hukum yang harus dipatuhi. Banyak organisasi hanya menjalankan kebijakan privasi sebagai formalitas administrasi tanpa diikuti mekanisme internal yang memadai untuk memastikan keamanan data. Situasi ini berpotensi menimbulkan risiko pelanggaran privasi karena prosedur yang diterapkan tidak mampu menahan berbagai bentuk ancaman digital. Permasalahan tersebut juga berkaitan dengan rendahnya kapasitas sumber daya manusia dalam sektor publik maupun swasta yang belum terlatih untuk mengelola data secara profesional (Kusumadewi & Cahyono, 2023).

Keterbatasan infrastruktur keamanan siber di lembaga penyelenggara sistem elektronik menjadi tantangan berikutnya karena banyak sistem masih menggunakan perangkat keamanan yang tidak mengikuti standar terbaru. Kerentanan yang muncul dari sistem yang sudah usang meningkatkan kemungkinan terjadinya pencurian data berskala besar seperti yang pernah dialami beberapa layanan publik. Di sisi teknis, banyak instansi juga belum memiliki sistem deteksi dini yang mampu mengidentifikasi gangguan sebelum menyebabkan kerugian. Kompleksitas serangan siber yang semakin canggih memerlukan kesiapan teknis yang lebih kuat dari sekadar mekanisme perlindungan dasar (Nusantara et al., 2024).

Minimnya budaya kepatuhan menjadi persoalan lain karena banyak organisasi menganggap perlindungan data sebagai beban administratif, bukan sebagai bagian dari tanggung jawab hukum. Pola pikir tersebut membuat upaya pemenuhan kewajiban seperti pembuatan *data protection impact assessment* atau penunjukan petugas perlindungan data diabaikan. Sikap ini tidak hanya menunjukkan rendahnya kesadaran

akan risiko, tetapi juga memperlihatkan kurangnya komitmen organisasi untuk menjamin hak privasi warga negara. Ketidakpatuhan yang terjadi di berbagai sektor menegaskan perlunya pengawasan yang lebih terstruktur dan tegas (Wulansari, 2020).

Tantangan lain terlihat pada mekanisme penegakan hukum yang belum konsisten karena belum adanya lembaga pengawas independen yang dapat menjalankan fungsi pengawasan secara penuh. Fungsi pengawasan masih terpusat di kementerian sehingga menimbulkan keraguan mengenai objektivitas dan efektivitas penindakan. Banyak kasus kebocoran data tidak menghasilkan kepastian hukum bagi korban karena proses penyelidikan berjalan lambat dan tidak transparan. Ketidakpastian penegakan ini membuat pelaku industri kurang terdorong untuk memperketat standar perlindungan data (Halbert et al., 2023).

Persoalan transfer data lintas negara memperumit implementasi UU PDP karena belum adanya kerangka teknis yang setara dengan aturan global seperti GDPR. Banyak perusahaan digital beroperasi dengan server di luar Indonesia sehingga pengawasan terhadap pergerakan data menjadi semakin kompleks. Kondisi ini membuka celah bagi terjadinya penyalahgunaan karena data dapat diakses di yurisdiksi yang tidak memiliki perlindungan seketat UU PDP. Upaya harmonisasi regulasi internasional masih memerlukan negosiasi antarnegara agar pemindahan data tetap aman dan legal (Ayiliani & Farida, 2024).

Tantangan implementatif juga muncul pada sektor perbankan, yang mengelola data vital dengan tingkat risiko sangat tinggi. Meskipun banyak bank telah mengadopsi sistem keamanan berlapis, kasus kebocoran data keuangan masih ditemukan dan menimbulkan kekhawatiran publik. Faktor manusia sering menjadi titik lemah karena kurangnya pelatihan mengenai tata kelola keamanan informasi. Kombinasi antara ancaman eksternal dan kelalaian internal membuat sektor keuangan membutuhkan pedoman khusus di bawah UU PDP (Kholis, 2024).

Kurangnya edukasi bagi masyarakat mengenai hak-hak mereka sebagai pemilik data pribadi membuat posisi pengguna semakin rentan dalam praktik transaksi digital. Banyak individu dengan mudah memberikan data tanpa memahami konsekuensinya dan tanpa membaca persyaratan yang mereka setujui. Situasi ini menurunkan efektivitas perlindungan hukum karena mekanisme kontrol yang diberikan UU PDP tidak digunakan secara optimal. Pemberdayaan pemilik data sangat penting agar mereka mampu menuntut kepatuhan dari penyedia layanan (Rizal, 2019).

Untuk memperkuat seluruh rantai perlindungan data, dibutuhkan reformasi struktural yang melibatkan peningkatan kapasitas teknis, pembangunan otoritas pengawas independen, serta perluasan literasi digital di masyarakat. Perbaikan pada sistem pengawasan harus diikuti oleh mekanisme akuntabilitas yang memungkinkan pelanggaran ditindak tegas tanpa mengecualikan sektor tertentu. Integrasi antara standar keamanan global dan praktik nasional juga diperlukan untuk menutup kesenjangan regulasi. Transformasi menyeluruh ini dipandang sebagai fondasi penting untuk mencapai perlindungan data yang benar-benar efektif di Indonesia (Khansa, 2021).

KESIMPULAN

Kajian ini menegaskan bahwa UU No. 27 Tahun 2022 merupakan kemajuan signifikan dalam perlindungan data pribadi di Indonesia karena menghadirkan standar normatif yang lebih jelas dibandingkan rezim sebelumnya. Meskipun begitu, efektivitas regulasi ini sepenuhnya bergantung pada pembentukan otoritas pengawas independen

yang memiliki legitimasi kuat, kewenangan luas, dan kapasitas teknis memadai untuk mengawasi ekosistem digital yang semakin kompleks. Perbandingan dengan GDPR menunjukkan bahwa Indonesia masih perlu memperkuat aspek akuntabilitas, kejelasan prosedur penanganan pelanggaran, dan tata kelola transfer data lintas negara. Tantangan implementasi seperti lemahnya kesadaran publik, resistensi pelaku industri, serta potensi disharmoni antar peraturan menjadi isu yang harus ditangani secara sistematis. Penelitian ini menyimpulkan bahwa keberhasilan paradigma baru perlindungan data pribadi hanya dapat dicapai jika regulasi, institusi, dan kultur digital masyarakat mampu berjalan beriringan dalam satu kerangka kebijakan yang konsisten dan berorientasi pada perlindungan hak warga negara.

DAFTAR PUSTAKA

Alamsyah, R., & Wiraguna, S. A. (2025). Dilema Media Massa di Era Digital: Antara Perlindungan Data Pribadi dan Kebebasan Pers Dalam UU PDP. *Media Hukum Indonesia (MHI)*, *3*(2).

Al-Kavafi, M. I., Baehaqi, J. F., & Rosyid, M. (2025). Urgensi Perampasan Aset Dalam Pemberantasan Korupsi: Dalam Perspektif Hukum Pidana Islam. *JURNAL USM LAW REVIEW*, *8*(2), 952-977.

Ayiliani, F. M., & Farida, E. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. *Jurnal Pembangunan Hukum Indonesia*, *6*(3), 431-455.

General Data Protection Regulation (GDPR) Uni Eropa.

Halbert, G., Rusdiana, S., & Hutauruk, R. H. (2023). Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia. *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *9*(3), 304-321.

Khansa, F. N. (2021). Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Pelindungan Data Pribadi di Indonesia. *Jurnal Hukum Lex Generalis*, *2*(8), 649-662.

Kholis, I. M. (2024). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, *4*(2), 275-299.

Kusumadewi, D. L., & Cahyono, A. B. (2023). Urgensi Perlindungan Data Pribadi Pada Sistem Elektronik Untuk Anak Di Bawah Umur Di Indonesia Serta Perbandingan Regulasi Dengan Uni Eropa (General Data Protection Regulation). Lex Patrimonium, 2(2).

Marzuki, P. M. (2014). Penelitian Hukum. Jakarta: Prenadamedia Group.

Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. *Justisi*, *10*(1), 20-35.

Nazir, M. (2005). Metode Penelitian. Jakarta: Ghalia Indonesia.

Nusantara, A. H. S., Umam, I. K., & Lubis, M. (2024). Jaminan Informasi Dan Keamanan Yang Lebih Baik: Studi Kasus BPJS Kesehatan. Nuansa Informatika, 18(2).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Pranoto, M. T. W., Kanthika, I. M., & Widarto, J. (2024). Pertanggungjawaban pidana pembocoran data pribadi. Jurnal Cinta Nusantara, 2(2).

Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. Jurnal

Cakrawala Hukum, 10(2).
Soekanto, S., & Mahmudji, S. (2003). Penelitian Hukum Normatif, Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada.
Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.
Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 Tentang Perlindungan Anak.
Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia.
Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.
Wulansari, E. M. (2020). Konsep Perlindungan Data Pribadi Sebagai Aspek Fundamental Norm Dalam Perlindungan Terhadap Hak Atas Privasi Seseorang di Indonesia. Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan, 7(2).