Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora
Volume 5, Nomor 2, April 2026
E-ISSN .: 2828-7622; P-ISSN .: 2828-7630, Hal. 793-805
DOI: https://doi.org/10.55606/jurrish.v5i2.8513
Tersedia: https://prin.or.id/index.php/JURRISH

Kebuntuan Pembentukan Lembaga Pelindungan Data Pribadi dan Implikasinya terhadap Efektivitas UU PDP di Indonesia

Gusti Ramadhani[1*], Cecep Suhardiman[2]
[1-2] Magister Ilmu Hukum, Universitas 17 Agustus 1945 Jakarta, Indonesia
Penulis Korespondensi: gustirmd93@gmail.com [1]

Abstract. *This article examines Indonesia's public policy on personal data protection in light of Law No. 27/2022, which mandates the establishment of an independent Personal Data Protection Authority (PDP Authority). Despite this legal requirement (Article 58 UU PDP), no such institution has been formed. As a result, there is currently no supervisory authority with the mandate to audit compliance, impose administrative sanctions, or resolve data protection disputes. Enforcement of the law has thus remained reactive rather than preventive, with violations prosecuted only after harm occurs. Experts warn that without a strong implementing agency, deterrence is weak: administrative sanctions cannot be effectively applied and punished violations continue unchecked. Cybersecurity analysts even describe this gap as a national digital protection crisis, as personal data leaks (e.g. millions of citizens' records exposed in recent breaches) continue unabated. Using a normative legal research approach and literature review, this study analyzes how the lack of the mandated PDP Authority undermines the effectiveness of data protection in Indonesia. The article reviews relevant legal theory on regulatory independence and deterrence, and compares with international best practices (e.g. EU/GDPR). We find that the absence of the agency creates serious implementation gaps, and we urge the government to immediately form the PDP Authority and clarify its powers.*

Keywords: *Administrative Sanctions; Indonesia; Personal Data Protection; Public Policy; Supervisory Authority.*

Abstrak. Artikel ini mengkaji kebijakan publik mengenai perlindungan data pribadi di Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) mengamanatkan pembentukan Lembaga Pelindungan Data Pribadi (LPDP) sebagai otoritas pengawas independen (Pasal 58). Lembaga ini dirancang memiliki kewenangan strategis: mengaudit kepatuhan pengendali data, menjatuhkan sanksi administratif, dan menyelesaikan sengketa perlindungan data. Hingga tiga tahun pasca pengesahan, lembaga tersebut belum juga direalisasikan. Ketiadaan otoritas pengawas ini menciptakan kekosongan kelembagaan yang berdampak sistemik terhadap efektivitas perlindungan data di Indonesia. Tanpa pengawas yang berwenang, tidak ada mekanisme audit kepatuhan yang sistematis, tidak ada prosedur pengaduan yang terlembaga bagi korban kebocoran data, dan yang terpenting, sanksi administratif sebagaimana diatur Pasal 57 UU PDP, termasuk denda hingga dua persen dari pendapatan tahunan pelaku usaha, tidak dapat ditegakkan. Akibatnya, penegakan hukum bersifat reaktif dan hanya menyasar pelaku teknis, bukan institusi yang lalai menjaga data. Lemahnya efek jera ini berimplikasi pada terus berulangnya kasus kebocoran data berskala besar, yang oleh pakar keamanan siber disebut sebagai krisis perlindungan data nasional. Menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan perbandingan dengan praktik internasional (GDPR Uni Eropa dan PDPA Singapura), penelitian ini menemukan tiga kesenjangan kritis: kesenjangan pengawasan (*supervisory gap*), kesenjangan penegakan sanksi (*sanction enforcement gap),* dan kesenjangan pemulihan hak (*remedy gap*). Penelitian ini merekomendasikan pemerintah untuk segera membentuk Lembaga PDP dengan independensi dan kewenangan yang memadai, karena tanpa lembaga tersebut, UU PDP hanya akan menjadi norma tanpa daya, dan tujuan luhurnya, memberikan perlindungan nyata bagi warga negara, tidak akan pernah tercapai.

Kata kunci: Indonesia; Kebijakan Publik; Otoritas Pengawas; Perlindungan Data Pribadi; Sanksi Administratif.

1. LATAR BELAKANG

Proteksi data pribadi menjadi isu global seiring digitalisasi luas. Indonesia merespons dengan mengesahkan UU No. 27/2022 tentang Pelindungan Data Pribadi pada 17 Oktober 2022. Undang-undang ini menjamin hak konstitusional atas privasi (Pasal 28G UUD 1945) di era informasi. Salah satu fitur penting UU ini adalah mandat Pembentukan Lembaga Perlindungan Data Pribadi yang bersifat independen (Nafisah & Diniyanto, 2024). Lembaga

Naskah Masuk: 31 Desember 2025; Revisi: 28 Januari 2026; Diterima:16 Februari 2026; Tersedia: 19 Februari 2026

ini diamanatkan untuk membuat kebijakan nasional, mengawasi pemenuhan aturan, menjatuhkan sanksi administratif, dan menyelesaikan sengketa terkait data pribadi (lihat Pasal 59-60 UU PDP). Dengan hadirnya lembaga tersebut, diharapkan penegakan hukum PDP bersifat preventif serta memberikan efek jera.

Hingga pertengahan 2025, Lembaga Pelindungan Data Pribadi (LPDP) yang diamanatkan Pasal 58 UU PDP belum juga terbentuk. Kemacetan institusional ini disebabkan oleh ketiadaan Peraturan Pemerintah (PP) sebagai payung hukum pelaksanaan yang mengatur struktur organisasi, mekanisme kerja, pendanaan, serta tata hubungan lembaga tersebut dengan kementerian/lembaga lain. Tanpa PP dimaksud, pemerintah tidak memiliki dasar hukum untuk mengalokasikan anggaran dalam APBN, merekrut sumber daya manusia, maupun menetapkan struktur kelembagaan yang definitif. Akibatnya, fungsi-fungsi krusial yang semestinya dijalankan oleh lembaga independen ini, seperti audit kepatuhan, penerimaan pengaduan masyarakat, investigasi pelanggaran, dan penjatuhan sanksi administratif praktis lumpuh total. Dalam situasi ini, UU PDP hanya menjadi "norma di atas kertas" tanpa daya eksekusi. Pelanggaran terhadap kewajiban perlindungan data terus terjadi tanpa ada mekanisme pengawasan yang sistematis, sementara ancaman sanksi administratif yang dirancang untuk menciptakan efek jera termasuk denda hingga dua persen dari pendapatan tahunan pelaku usaha, tidak dapat direalisasikan karena tidak ada otoritas yang berwenang menjatuhkannya. Ironisnya, meskipun publik menyaksikan rentetan kasus kebocoran data berskala besar, tidak ada satu pun institusi yang secara resmi dapat dimintai pertanggungjawaban atas kelalaian menjaga data warga negara.

Ketiadaan lembaga ini juga dikecam oleh berbagai pihak. Misalnya, LBH Jakarta mencatat rekam jejak kebocoran data besar di Indonesia: data pemilih (2,3 juta Rekap DPT 2014), data eHAC (1,3 juta pengguna COVID-19), data pinjaman online, data PLN/IndiHome/SIM serta informasi pejabat publik bocor tanpa penindakan memadai. Dalam salah satu laporan resmi DPR, kasus-kasus bocornya 6 juta data NPWP, 1,3 miliar data registrasi SIM, serta 4,7 juta data PNS diperjualbelikan di forum siber. Pakar di lembaga riset keamanan siber CISSReC, Pratama Persadha, bahkan menyatakan bahwa keterlambatan pembentukan lembaga PDP ini telah membuka celah kejahatan digital terorganisir dan menyebabkan Indonesia berada dalam krisis perlindungan digital (Alfianto, 2025). Kondisi ini memberi gambaran minimnya perlindungan data: sementara kasus bocor terus menerus, tidak ada otoritas pengawas yang menindak.

Fenomena kemandekan pembentukan lembaga pengawas ini menggarisbawahi urgensi kajian untuk menjawab dua pertanyaan fundamental: mengapa amanat konstitusional dan legal

sebagaimana dinyatakan dalam UU PDP belum terwujud? dan bagaimana dampaknya terhadap efektivitas perlindungan data pribadi di Indonesia? Dari perspektif konstitusional, Pasal 28G UUD 1945 menjamin hak setiap orang atas perlindungan diri pribadi, sehingga pembentukan lembaga pengawas sejatinya merupakan kewajiban negara untuk memenuhi hak konstitusional warganya. Dari perspektif kelembagaan, pengawasan yang efektif mensyaratkan adanya otoritas independen yang bebas dari konflik kepentingan dan memiliki kewenangan memadai, prinsip yang dikenal dalam doktrin *independent regulatory agencies* dan telah menjadi standar internasional melalui ketentuan *adequacy decision* dalam GDPR. Sementara dari perspektif teori pencegahan (*deterrence theory*), efektivitas penegakan hukum sangat bergantung pada tiga elemen: kepastian deteksi (*certainty of detection*), kecepatan penindakan (*swiftness*), dan beratnya sanksi (*severity*). Tanpa lembaga pengawas, ketiga elemen tersebut tidak mungkin terpenuhi: pelanggar merasa aman karena kecil kemungkinan terdeteksi dan hampir pasti tidak akan dikenai sanksi administratif. Akibatnya, insentif untuk berinvestasi pada keamanan data menjadi rendah, dan siklus pelanggaran terus berulang, sebuah kondisi yang oleh pakar hukum administrasi disebut sebagai *regulatory failure* atau kegagalan regulasi dalam mencapai tujuannya.

2. KAJIAN TEORITIS

Perlindungan data pribadi dalam perspektif hukum tata negara berakar pada pengakuan hak privasi sebagai bagian dari hak asasi manusia yang dijamin konstitusi. Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 secara tegas menyatakan bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya." Ketentuan ini menjadi fondasi konstitusional yang mewajibkan negara tidak hanya untuk menghormati (*to respect*) hak privasi warga negara, tetapi juga untuk melindungi (*to protect*) dan memenuhinya (*to fulfill*). Dalam kerangka hukum hak asasi manusia, kewajiban protektif negara berarti negara harus membentuk regulasi dan institusi yang mampu mencegah pelanggaran hak privasi oleh pihak lain, baik korporasi maupun sesama warga negara. Dengan demikian, pembentukan undang-undang perlindungan data pribadi beserta lembaga pengawasnya bukanlah kebijakan diskresioner yang dapat ditunda atas dasar pertimbangan politis atau administratif semata, melainkan merupakan amanat konstitusional yang mengikat dan harus direalisasikan. Kegagalan membentuk lembaga yang diamanatkan UU PDP dapat dipandang sebagai bentuk kelalaian negara dalam memenuhi kewajiban konstitusionalnya, yang pada akhirnya merugikan hak-hak fundamental warga negara.

Dalam kerangka teori regulasi modern, efektivitas suatu peraturan perundang-undangan sangat bergantung pada keberadaan institusi pelaksana yang memiliki kewenangan memadai. (Breyer, 1982) dalam teorinya tentang *regulation and its reform*, menekankan bahwa regulasi teknis yang kompleks, seperti perlindungan data pribadi, memerlukan lembaga pengawas khusus yang berada di luar struktur birokrasi konvensional. Lembaga ini idealnya memiliki karakteristik sebagai *independent regulatory agency*: bebas dari intervensi politik, memiliki keahlian teknis, dan diberi kewenangan diskresioner untuk menetapkan standar, melakukan inspeksi, serta menjatuhkan sanksi. Pengalaman global membuktikan pentingnya desain kelembagaan semacam ini. General Data Protection Regulation (GDPR) di Uni Eropa, misalnya, mewajibkan setiap negara anggota membentuk otoritas pengawas independen yang disebut *Supervisory Authority* dengan kewenangan luas, termasuk menjatuhkan denda administratif hingga 20 juta euro atau 4% dari omzet global perusahaan. Demikian pula Singapura melalui Personal Data Protection Act (PDPA) membentuk Personal Data Protection Commission (PDPC) yang berfungsi tidak hanya sebagai regulator tetapi juga penegak hukum yang aktif melakukan audit dan investigasi. Bahkan Perserikatan Bangsa-Bangsa, melalui laporan *Special Rapporteur on the Right to Privacy*, secara konsisten menyatakan bahwa keberadaan lembaga pengawas data independen merupakan prasyarat mutlak (*sine qua non*) bagi efektivitas perlindungan privasi di era digital. Tanpa lembaga semacam ini, pengawasan cenderung bersifat fragmentaris, parsial, dan sangat bergantung pada institusi penegak hukum umum yang tidak memiliki spesialisasi dan kapasitas memadai untuk menangani kompleksitas persoalan perlindungan data.

Dari perspektif kriminologi dan hukum pidana, teori pencegahan atau *deterrence theory* yang dikemukakan oleh (Nagin, 2013) memberikan kerangka analisis penting untuk memahami fungsi sanksi dalam perlindungan data. Teori ini berargumen bahwa efektivitas pencegahan kejahatan bergantung pada tiga elemen kunci: kepastian (*certainty*), kecepatan (*swiftness*), dan beratnya sanksi (*severity*). Dalam konteks perlindungan data pribadi, fungsi ini terbagi menjadi dua dimensi. Pertama, fungsi preventif, yaitu upaya mencegah terjadinya pelanggaran melalui pengawasan yang konsisten dan audit kepatuhan yang sistematis. Dengan pengawasan rutin, potensi pelanggaran dapat dideteksi sejak dini dan celah keamanan dapat ditutup sebelum dieksploitasi pelaku kejahatan. Kedua, fungsi represif, yaitu menciptakan efek jera melalui penjatuhan sanksi yang tegas dan proporsional bagi pihak yang terbukti lalai atau sengaja melanggar kewajiban perlindungan data. Sanksi administratif seperti denda persentase pendapatan, pencabutan izin, atau larangan sementara beroperasi dirancang untuk memberikan insentif ekonomi agar korporasi mematuhi standar keamanan data. Jika penegakan hukum

lemah dan sanksi tidak pernah dijatuhkan, maka hukum perlindungan data hanya bersifat normatif semata, ia hadir sebagai teks tetapi tidak memiliki daya gentar nyata. Dalam situasi demikian, pelaku usaha tidak memiliki insentif untuk berinvestasi pada keamanan data karena biaya kepatuhan (*compliance cost*) lebih tinggi dibandingkan risiko sanksi yang nyaris nol. Oleh karena itu, teori hukum administrasi menekankan pentingnya institusi yang memiliki kewenangan auditor dan pemberi sanksi secara terintegrasi. Jika kewenangan ini tercecer di berbagai Lembaga misalnya audit oleh kementerian teknis, penindakan pidana oleh kepolisian, dan sanksi administratif oleh lembaga lain, maka efektivitas pencegahan akan sangat terbatas karena koordinasi yang rumit dan tumpang tindih kewenangan.

Dalam perspektif kebijakan publik dan administrasi negara, implementasi regulasi teknis seperti perlindungan data pribadi menuntut penerapan prinsip-prinsip *good governance* (Haris), yaitu transparansi, akuntabilitas, partisipasi, dan efektivitas. Undang-undang yang kompleks dengan dampak lintas sektoral memerlukan badan khusus yang memiliki kapasitas teknis dan legitimasi untuk mengoordinasikan berbagai pemangku kepentingan. Lembaga yang dibentuk idealnya ditempatkan di luar cabang kekuasaan eksekutif, legislatif, dan yudikatif konvensional, sebuah posisi *independent* yang bertujuan menghindari intervensi politik jangka pendek dan memastikan pengambilan keputusan berdasarkan keahlian dan kebutuhan publik. Desain kelembagaan seperti ini lazim disebut sebagai *independent regulatory body* atau *non-majoritarian institution*. Desain kelembagaan Lembaga Pelindungan Data Pribadi (LPDP) dalam UU PDP menuai kritik karena pengaturannya yang menempatkan lembaga tersebut "di bawah Presiden" dengan pembentukan melalui Peraturan Pemerintah. Ketentuan Pasal 59 ayat (1) UU PDP yang menyatakan bahwa "Lembaga sebagaimana dimaksud dalam Pasal 58 berkedudukan di bawah Presiden dan bertanggung jawab kepada Presiden" menimbulkan kekhawatiran tentang independensinya. Dalam praktik global, negara-negara maju seperti Jerman dengan *Federal Commissioner for Data Protection and Freedom of Information* atau Inggris dengan *Information Commissioner's Office* memilih model lembaga yang independen dan bertanggung jawab langsung kepada parlemen, bukan kepada eksekutif. Hal ini untuk memastikan bahwa fungsi pengawasan terhadap institusi public, termasuk kementerian dan lembaga pemerintah, dapat berjalan tanpa tekanan hierarkis. Dengan demikian, ketiadaan lembaga pengawas yang efektif di Indonesia tidak hanya persoalan keterlambatan pembentukan, tetapi juga menyangkut desain fundamental yang berpotensi melemahkan independensi dan kapasitas lembaga itu sendiri ketika nantinya terbentuk.

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yuridis normatif, yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur yang berkaitan dengan permasalahan yang diteliti (Soekanto & Mamudji, Penelitian Hukum Normatif, 2012). Pendekatan yuridis normatif dipilih karena fokus penelitian ini adalah pada analisis norma hukum, khususnya mengenai kewajiban pembentukan lembaga pengawas independen dalam UU PDP serta dampak ketiadaan lembaga tersebut terhadap efektivitas perlindungan data pribadi di Indonesia.

Penelitian ini menggunakan tiga pendekatan utama (Soekanto, 2019) pertama, pendekatan perundang-undangan (*statute approach*), yaitu dengan menelaah semua peraturan perundang-undangan yang berkaitan dengan isu hukum yang ditangani. Dalam konteks ini, peraturan yang dikaji meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (khususnya Pasal 28G), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta peraturan pelaksana terkait lainnya. Kedua, pendekatan konseptual (*conceptual approach*), yaitu dengan merujuk pada prinsip-prinsip hukum, doktrin, dan teori-teori hukum yang relevan, seperti teori regulasi independen, teori pencegahan (*deterrence theory*), dan prinsip *good governance* dalam pembentukan lembaga pengawas. Pendekatan ini digunakan untuk membangun argumentasi hukum mengenai urgensi lembaga pengawas independen dalam perlindungan data pribadi. Ketiga, pendekatan perbandingan (*comparative approach*), yaitu dengan membandingkan pengaturan dan implementasi lembaga pengawas perlindungan data di negara lain, khususnya GDPR di Uni Eropa dan PDPA di Singapura. Pendekatan ini bertujuan untuk menemukan praktik terbaik (*best practices*) yang dapat menjadi referensi bagi Indonesia.

Sumber bahan hukum dalam penelitian ini terdiri atas tiga kategori. Pertama, bahan hukum primer yaitu bahan hukum yang bersifat otoritatif berupa peraturan perundang-undangan, meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, GDPR Uni Eropa, PDPA Singapura, serta peraturan perundang-undangan terkait lainnya. Kedua, bahan hukum sekunder yaitu bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, berupa buku-buku teks dan literatur hukum yang membahas perlindungan data pribadi, hukum tata negara, dan teori regulasi, jurnal ilmiah nasional dan internasional yang relevan, hasil penelitian sebelumnya dan laporan-laporan lembaga terkait, serta artikel dari pakar dan praktisi hukum. Ketiga, bahan hukum tersier yaitu bahan hukum yang memberikan petunjuk atau penjelasan

terhadap bahan hukum primer dan sekunder, seperti kamus hukum, ensiklopedia, dan sumber-sumber digital terpercaya yang relevan dengan topik penelitian.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan teknik dokumentasi, yaitu mengumpulkan, mengklasifikasikan, dan mensistematisasikan bahan-bahan hukum yang relevan dengan permasalahan penelitian (Mardalis, 1999). Penelusuran bahan hukum dilakukan secara manual dengan membaca literatur fisik, maupun secara digital melalui basis data jurnal ilmiah, portal perundang-undangan, dan sumber-sumber daring yang kredibel.

Bahan hukum yang telah terkumpul dianalisis menggunakan metode interpretasi hukum (*legal interpretation*) dan konstruksi hukum (*legal construction*). Interpretasi hukum digunakan untuk menafsirkan makna norma-norma dalam UU PDP, khususnya terkait mandat pembentukan Lembaga Pelindungan Data Pribadi dan mekanisme sanksi administratif. Konstruksi hukum digunakan untuk membangun argumentasi mengenai konsekuensi yuridis dari ketiadaan lembaga pengawas terhadap efektivitas perlindungan data pribadi. Analisis dilakukan secara kualitatif dengan logika deduktif, yaitu menarik kesimpulan dari hal-hal yang bersifat umum (norma hukum dan teori) menuju hal-hal yang bersifat khusus (permasalahan konkret ketiadaan lembaga pengawas). Hasil analisis kemudian disajikan secara deskriptif-analitis, yaitu menggambarkan fakta-fakta hukum yang ditemukan dan menganalisisnya menggunakan kerangka teoretis yang telah dibangun untuk menjawab rumusan masalah penelitian.

4. HASIL DAN PEMBAHASAN FAKTOR PENYEBAB BELUM TERWUJUDNYA AMANAT PEMBENTUKAN LEMBAGA PELINDUNGAN DATA PRIBADI

Hasil kajian menunjukkan bahwa mandat pembentukan Lembaga Pelindungan Data Pribadi (LPDP) sebagaimana diamanatkan dalam Pasal 58 UU PDP hingga pertengahan tahun 2025 belum direalisasikan. Berdasarkan analisis terhadap dokumen legislatif dan pernyataan resmi DPR RI, penyebab utama kemandekan institusional ini adalah ketiadaan Peraturan Pemerintah (PP) sebagai payung hukum pelaksanaan yang mengatur struktur organisasi, mekanisme kerja, pendanaan, serta tata hubungan lembaga tersebut dengan kementerian/lembaga lain. Tanpa PP dimaksud, pemerintah tidak memiliki dasar hukum untuk mengalokasikan anggaran dalam APBN, merekrut sumber daya manusia, maupun menetapkan struktur kelembagaan yang definitif. Akibatnya, fungsi-fungsi krusial yang semestinya dijalankan oleh lembaga independen ini praktis lumpuh total.

Dari perspektif hukum tata negara, kondisi ini menunjukkan adanya kelalaian negara dalam memenuhi kewajiban konstitusionalnya. Sebagaimana diuraikan dalam kerangka teoretis, Pasal 28G ayat (1) UUD 1945 menjamin hak setiap orang atas perlindungan diri pribadi, yang mengimplikasikan kewajiban negara tidak hanya untuk menghormati (*to respect*) tetapi juga untuk melindungi (*to protect*) dan memenuhinya (*to fulfill*). Pembentukan lembaga pengawas independen merupakan instrumen kunci dalam memenuhi kewajiban protektif tersebut. Kegagalan membentuk lembaga yang diamanatkan UU PDP dapat dipandang sebagai bentuk constitutional disobedience atau ingkar janji konstitusional, yang pada akhirnya merugikan hak-hak fundamental warga negara.

Apabila ditelaah menggunakan teori regulasi dari (Breyer, 1982), regulasi teknis yang kompleks seperti perlindungan data pribadi memerlukan lembaga pengawas khusus yang berada di luar struktur birokrasi konvensional. Lembaga ini idealnya memiliki karakteristik sebagai *independent regulatory agency*: bebas dari intervensi politik, memiliki keahlian teknis, dan diberi kewenangan diskresioner. Namun, realitas di Indonesia justru menunjukkan sebaliknya. Desain kelembagaan LPDP dalam UU PDP sendiri menuai kritik karena pengaturannya yang menempatkan lembaga tersebut "di bawah Presiden" dengan pembentukan melalui Peraturan Pemerintah (Pasal 59 ayat 1). Ketentuan ini menimbulkan kekhawatiran tentang independensinya, karena dalam praktik global, negara-negara maju seperti Jerman dengan *Federal Commissioner for Data Protection and Freedom of Information* atau Inggris dengan *Information Commissioner's Office* memilih model lembaga yang independen dan bertanggung jawab langsung kepada parlemen, bukan kepada eksekutif. Hal ini untuk memastikan bahwa fungsi pengawasan terhadap institusi publik, termasuk kementerian dan lembaga pemerintah, dapat berjalan tanpa tekanan hierarkis.

Data dari proses legislasi menunjukkan bahwa sejak UU PDP disahkan pada Oktober 2022, pemerintah belum juga menerbitkan PP yang menjadi prasyarat pembentukan lembaga. Padahal, tanpa PP tersebut, tidak ada kejelasan mengenai struktur organisasi, mekanisme kerja, pendanaan, serta tata hubungan lembaga dengan kementerian/lembaga lain. Akibatnya, pemerintah tidak memiliki dasar hukum untuk mengalokasikan anggaran dalam APBN, merekrut sumber daya manusia, maupun menetapkan struktur kelembagaan yang definitif. Hal ini mengindikasikan lemahnya political will dari pemerintah untuk segera merealisasikan amanat UU PDP, meskipun berbagai pihak terus mendesak.

Dampak Ketiadaan Lembaga Pengawas Terhadap Efektivitas Perlindungan Data Pribadi Di Indonesia

Krisis digital dan kepercayaan publik: Dampak lebih luas dari situasi ini adalah krisis keamanan digital dan menurunnya kepercayaan publik. Pasar gelap data pribadi berkembang pesat di Indonesia. Tabel 1 menampilkan contoh insiden besar kebocoran data dalam satu dekade terakhir. Kasus-kasus tersebut misalnya 1,3 miliar data registrasi SIM pada 2022, 6 juta data NPWP tahun 2024, dan jutaan data PNS tahun 2024 memberikan gambaran suram lemahnya perlindungan data di lapangan. Kondisi demikian menunjukkan bahwa pelanggaran data tidak hanya terus-menerus tetapi juga melibatkan data warga sipil dan instansi pemerintah. Pakar menyatakan bahwa situasi ini "akan makin memburuk" tanpa pengawasan dan penegakan hukum yang tegas. Jika kelemahan institusi ini tidak segera diatasi, kepercayaan masyarakat terhadap keamanan digital terancam menurun signifikan, menghambat pembangunan ekosistem digital yang sehat.

Pembandingan Internasional: Secara kontras, yurisdiksi seperti Uni Eropa (GDPR) dan Singapura (PDPA) telah menunjukkan bahwa lembaga pengawas independen dapat menekan tingkat kebocoran data. Pengalaman global menunjukkan bahwa keberadaan otoritas khusus (dengan sumber daya teknis dan wewenang kuat) berperan penting menjaga standar kepatuhan tinggi. Ketiadaan lembaga setara di Indonesia membuatnya tertinggal dalam perlindungan privasi dibanding negara lain. Hal ini diperparah oleh tren global kejahatan data yang terus maju, seperti rekayasa sosial dan *AI-based scams* yang sulit dideteksi menuntut kebijakan proteksi data yang proaktif.

Tabel 1. Insiden Kebocoran Data Pribadi Signifikan di Indonesia (2014–2024).

Kasus	Tahun	Skala Data Terdampak	Sumber
Daftar Pemilih Tetap (Pemilu 2014)	2014	2,3 juta penduduk (nama, ktp)	Komisi Pemilihan Umum (bocor)
Aplikasi e-HAC (Kemenkes)	2020	1,3 juta pengguna (nama, KTP)	VPNMentor (temuan)
Data Registrasi Kartu SIM Prabayar	2022	1,3 miliar nomor	Forum Breachforums
Data NPWP (Terjual di forum siber)	2024	6 juta NPWP	Forum Breachforums
Data Pegawai Negeri Sipil (BKN)	2024	4,759,218 baris data	Forum Breachforums

Tabel tersebut mengilustrasikan betapa luasnya data pribadi masyarakat Indonesia yang pernah terungkap, mencakup data KPU, kesehatan, telekomunikasi, pajak, dan kepegawaian. Kasus-kasus di atas belum mendapat penindakan serius karena lembaga pengawas belum ada. Misalnya, ribuan warga hanya dapat melapor ke polisi atau Kominfo, padahal UU PDP mengamanatkan otoritas tersendiri. Tanpa alternatif penyelesaian sengketa ekstra-peradilan yang disediakan lembaga PDP, para korban kebocoran sering mengalami hambatan dalam memulihkan haknya. Sehingga kerugian, baik finansial maupun sosial, sulit diminimalisir.

Dampak lainnya dari ketiadaan lembaga pengawas adalah lumpuhnya mekanisme penjatuhan sanksi administratif. Pasal 57 UU PDP mengatur sanksi administratif yang tegas, termasuk denda administratif hingga dua persen dari pendapatan tahunan pelaku usaha terhadap pelanggaran. Namun, Pasal 60 ayat (c) UU PDP secara eksplisit menempatkan kewenangan penjatuhan sanksi administratif pada lembaga pengawas. Tanpa lembaga tersebut, sanksi administratif tidak dapat ditegakkan, sehingga ancaman sanksi hanya menjadi "pasal tidur" tanpa daya eksekusi.

Kasus kebocoran data BPJS Kesehatan pada tahun 2021 yang melibatkan 279 juta data penduduk menjadi contoh paling gamblang bagaimana ketiadaan lembaga pengawas menyebabkan penegakan hukum berjalan di tempat. Saat itu, Menteri PANRB secara terbuka mengakui bahwa aparat penegak hukum kesulitan menjatuhkan sanksi pidana yang tegas karena payung hukum yang ada belum memberikan sanksi yang memadai. Ironisnya, meskipun UU PDP telah disahkan pada tahun 2022, pola yang sama kembali terulang. Ketika data nasabah Bank Syariah Indonesia (BSI) diduga bocor dan dijual di *dark web* pada tahun 2023, pakar keamanan siber langsung mengingatkan bahwa sanksi administratif belum dapat dijatuhkan karena lembaga pengawas belum terbentuk.

Dampak lanjutan dari lemahnya penegakan sanksi ini adalah rendahnya kesadaran pelaku usaha, terutama di sektor UMKM, terhadap kewajiban perlindungan data. Sebuah riset (Astuti, Hidayanto, Nurwardani, & Salsabila, 2024) mengungkap bahwa tingkat kesadaran hukum terhadap UU PDP masih rendah, dengan skor rata-rata 3,13. Banyak pelaku bisnis masih beroperasi dengan mentalitas reaktif, baru berbenah setelah insiden terjadi, dan menganggap kepatuhan hukum hanya sebagai kewajiban administratif belaka, bukan sebagai strategi bisnis yang mitigatif. Kondisi ini persis seperti yang diprediksi oleh teori pencegahan: ketika pelaku usaha merasa aman karena hampir pasti tidak akan dikenai sanksi, insentif untuk berinvestasi pada keamanan data menjadi sangat rendah.

Dampak ketiga yang tidak kalah penting adalah kesenjangan pemulihan hak bagi korban kebocoran data. UU PDP dalam Pasal 59 ayat (d) mengamanatkan lembaga pengawas untuk memfasilitasi penyelesaian sengketa perlindungan data pribadi di luar pengadilan melalui mekanisme mediasi atau ajudikasi. Tanpa lembaga tersebut, masyarakat yang menjadi korban kebocoran data tidak memiliki jalur pengaduan yang jelas dan terlembaga untuk memperoleh pemulihan atas kerugian yang mereka alami.

Dalam praktiknya, ribuan warga hanya dapat melapor ke polisi atau Kominfo, padahal kedua institusi tersebut tidak memiliki kewenangan dan kapasitas khusus untuk menangani sengketa perlindungan data secara komprehensif. Akibatnya, banyak kasus kebocoran data

tidak pernah berujung pada pemulihan hak korban. Data dari OJK dan *Indonesia Anti Scam Center* (IASC) mencatat total kerugian akibat penipuan *online* telah mencapai lebih dari Rp2,6 triliun hingga Mei 2025. Kerugian finansial yang masif ini membuktikan bahwa tanpa mekanisme pemulihan yang efektif, masyarakat sebagai subjek data menjadi pihak yang paling dirugikan.

Kondisi ini menunjukkan bahwa negara gagal memenuhi kewajibannya untuk menyediakan akses keadilan bagi warga negara yang hak privasinya dilanggar. Padahal, dalam kerangka hukum HAM, kewajiban protektif negara tidak hanya berhenti pada pembentukan regulasi, tetapi juga mencakup penyediaan mekanisme pemulihan yang efektif (*effective remedy*) bagi korban pelanggaran hak.

Secara kontras, yurisdiksi seperti Uni Eropa (GDPR) dan Singapura (PDPA) telah menunjukkan bahwa lembaga pengawas independen dapat menekan tingkat kebocoran data. GDPR mewajibkan setiap negara anggota membentuk otoritas pengawas independen yang disebut *Supervisory Authority* dengan kewenangan luas, termasuk menjatuhkan denda administratif hingga 20 juta euro atau 4% dari omzet global perusahaan. Demikian pula Singapura melalui PDPA membentuk Personal Data Protection Commission (PDPC) yang berfungsi tidak hanya sebagai regulator tetapi juga penegak hukum yang aktif melakukan audit dan investigasi.

Pengalaman global menunjukkan bahwa keberadaan otoritas khusus dengan sumber daya teknis dan wewenang kuat berperan penting dalam menjaga standar kepatuhan tinggi. Ketiadaan lembaga setara di Indonesia membuatnya tertinggal dalam perlindungan privasi dibanding negara lain. Hal ini diperparah oleh tren global kejahatan data yang terus maju, seperti rekayasa sosial dan *AI-based scams* yang sulit dideteksi, yang menuntut kebijakan proteksi data yang proaktif.

Secara keseluruhan, hasil analisis menunjukkan bahwa ketidakberadaan Lembaga Pelindungan Data Pribadi signifikan melemahkan tujuan UU PDP. Regulasi yang sudah ada di tingkat undang-undang menjadi terhambat implementasinya. Tanpa lembaga pengawas resmi, komitmen hukum perlindungan data sulit diukur dan ditegakkan secara berkesinambungan. Hal ini menuntut evaluasi kebijakan lebih lanjut dan tindakan cepat dari pemerintah untuk menutup celah hukum yang ada.

5. KESIMPULAN DAN SARAN

Bahwa belum terwujudnya amanat konstitusional dan legal pembentukan Lembaga Pelindungan Data Pribadi disebabkan oleh dua faktor utama: faktor prosedural-administratif, yaitu ketiadaan Peraturan Pemerintah sebagai landasan hukum pembentukan dan penganggaran; serta faktor desain kelembagaan, yaitu pengaturan dalam UU PDP yang menempatkan lembaga di bawah Presiden berpotensi menciptakan konflik kepentingan dan menunda proses pembentukan karena bergantung pada prioritas politik eksekutif.

Bahwa ketiadaan Lembaga Pelindungan Data Pribadi berdampak sangat signifikan terhadap efektivitas perlindungan data di Indonesia, yang terwujud dalam tiga kesenjangan kritis (pengawasan, penegakan sanksi, dan pemulihan hak), yang pada akhirnya melahirkan krisis kepercayaan publik dan kerugian ekonomi masif. Kondisi ini membuktikan bahwa tanpa lembaga pengawas, UU PDP hanya menjadi "norma di atas kertas" tanpa daya eksekusi, dan tujuan luhurnya untuk memberikan perlindungan nyata bagi warga negara tidak akan pernah tercapai.

DAFTAR PUSTAKA

Alfianto, R. (2025, October 21). Keterlambatan Badan PDP: Ancaman terhadap keamanan data warga. *JawaPos*.

Astuti, E. F., Hidayanto, A. N., Nurwardani, S., & Salsabila, A. Z. (2024). Assessing Indonesian MSMEs' awareness of personal data protection by PDP Law and ISO/IEC 27001:2013. *IIETA Journal*. https://doi.org/10.18280/ijsse.140523

Badan Legislasi DPR RI. (2024). Analisis yuridis terhadap ketiadaan lembaga penyelenggara perlindungan data pribadi. *Pusat Penelitian dan Pengabdian Masyarakat DPR RI*.

Breyer, S. (1982). *Regulation and its reform*. Harvard University Press. https://doi.org/10.4159/9780674028760

Djafar, W., et al. (2019). Studi perbandingan GDPR dan otoritas perlindungan data. *LP3TI Press*.

Haris, A. (2021). *Good governance*. Zahir Publishing.

Komisi Pemilihan Umum. (2014). *Laporan kebocoran data pribadi pemilih (sekitar 2,3 juta data)*. Jakarta: KPU.

Laelaturramadani, R. (2023). Tinjauan terhadap efektivitas regulasi perlindungan data pribadi di Indonesia. *Mandalika Law Journal*, *4*(1), 263-275.

Lukman, A., & Agustini, V. A. (2023). *Penerapan manajemen nutrisi pada asuhan keperawatan diabetes melitus tipe II dengan masalah keperawatan defisit nutrisi*. Jurnal Aisyiyah Palembang, 8.

Mardalis. (1999). *Metode penelitian suatu pendekatan proposal*. Bumi Aksara.

Marzuki, P. M. (2016). *Penelitian hukum: Edisi revisi*. Kencana Prenada Media Group.

Nafisah, S., & Diniyanto, A. (2024). Independensi lembaga perlindungan data pribadi di Indonesia. *Manabia*, *7*(1), 1-20. https://doi.org/10.28918/manabia.v4i01.8664

Nagin, D. S. (2013). Deterrence in the twenty-first century. *The University of Chicago Press*. https://doi.org/10.1086/670398

PeriksaData (Tim Periksa Data). (2021, September 3). *Rilis media: Dugaan kebocoran data aplikasi eHAC*.

Persadha, P. (2025, October 22). Data pribadi jadi komoditas gelap, pakar nilai Indonesia krisis perlindungan digital di tengah mandeknya UU PDP. *JawaPos*.

Republik Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara RI Tahun 2022 Nomor 196. Sekretariat Negara. Jakarta.

Soekanto, S. (2019). *Pengantar penelitian hukum*. UI Press.

Soekanto, S., & Mamudji, S. (2012). *Penelitian hukum normatif: Suatu tinjauan singkat*. Raja Grafindo Persada.

Sugiarto, N., Yuliawan, I., & Irawati, A. C. (2026). Perlindungan data pribadi sebagai instrumen hukum dalam menanggulangi kejahatan perbankan. *Pendas: Jurnal Ilmiah Pendidikan Dasar*, *11*(1), 260-275.

Wahyudi Djafar, dkk. (2019). Studi perbandingan GDPR dan otoritas perlindungan data. *LP3TI Press*.