Socius: Jurnal Penelitian Ilmu-Ilmu Sosial
Volume 4, Issue 2, September 2026, p 681-695
E-ISSN: 3025-6704
DOI: https://doi.org/10.5281/zenodo.23789800

Pertanggungjawaban Administratif Instansi Pemerintah atas Kebocoran Data Pribadi dalam Layanan Publik Digital: Kajian UU Pelindungan Data Pribadi

Administrative Liability of Government Agencies for Personal Data Breaches in Digital Public Services: A Study of the Personal Data Protection Law

Ardhiwinda[1], Vayqueen Humairah Mayangkara[2], Danish Khaira Syahrain[3], Rio Efendi[4]

[1,2,3,4]Program Studi Hukum, Fakultas Hukum Universitas Wijaya Kusuma, Surabaya

ARTICLE INFO
Article history:
Received 17 September 2026
Revised 25 September 2026
Accepted 28 September 2026
Available online 05 October 2026

Keywords
administrative liability; personal data; digital public services; personal data protection; data breach; administrative sanctions.

This is an open access article under the CC BY-SA license.
Copyright © 2026 by Author. Published by Yayasan Daarul Huda

ABSTRACT

Digital transformation in public service delivery has increased the use of electronic systems to collect, store, and process citizens' personal data. This development creates legal responsibilities for government agencies to ensure the security and protection of personal data under their control. This study examines the administrative liability of government agencies as personal data controllers under Law No. 27 of 2022 on Personal Data Protection and Law No. 25 of 2009 on Public Services. It also proposes an administrative sanction-aggravation framework for government agencies that fail to fulfill their personal data protection obligations. This research employs a normative legal method using statutory, conceptual, and case approaches. Legal materials are analyzed qualitatively through grammatical and systematic interpretation. The 2024 ransomware incident involving the Temporary National Data Center (PDNS) is used as an illustration of the application of relevant legal norms. The findings indicate that the PDP Law and the Public Services Law establish complementary liability regimes. The PDP Law regulates the obligations of personal data controllers and processors, while the Public Services Law governs the responsibilities of public service providers and personnel. The determination of liability must be based on the actual functions, processing purposes, system control, and allocation of responsibilities among the parties involved. Furthermore, Article 57 of the PDP Law does not provide sufficiently detailed criteria for aggravating administrative sanctions.

ABSTRAK

Transformasi digital dalam penyelenggaraan pelayanan publik meningkatkan penggunaan sistem elektronik untuk mengumpulkan, menyimpan, dan memproses data pribadi masyarakat. Kondisi tersebut menimbulkan tanggung jawab hukum bagi instansi pemerintah untuk menjamin keamanan dan pelindungan data pribadi yang dikelolanya. Penelitian ini bertujuan menganalisis bentuk pertanggungjawaban administratif instansi pemerintah sebagai pengendali data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik, serta merumuskan mekanisme pemberatan sanksi administratif terhadap instansi yang lalai melaksanakan kewajiban pelindungan data pribadi. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Bahan hukum dianalisis secara kualitatif melalui penafsiran gramatikal dan sistematis. Insiden serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) pada 2024 digunakan sebagai ilustrasi penerapan norma. Hasil penelitian menunjukkan bahwa UU PDP dan UU Pelayanan Publik membentuk rezim pertanggungjawaban yang saling melengkapi. UU PDP mengatur kewajiban pengendali dan prosesor data pribadi, sedangkan UU Pelayanan Publik mengatur tanggung jawab penyelenggara dan pelaksana pelayanan kepada masyarakat. Penentuan pihak yang bertanggung jawab harus didasarkan pada fungsi, tujuan pemrosesan, penguasaan sistem, dan pembagian kewajiban dalam hubungan pengelolaan data. Penelitian ini juga menemukan bahwa Pasal 57 UU PDP belum memberikan parameter terperinci mengenai pemberatan sanksi administratif.

Corresponding Author
Email: [1]ardhiwinda_fh@uwks.ac.id, [2]ratumayangkara022006@gmail.com, [3]danishkhaira9@gmail.com , [4]ryoefendii@gmail.com,

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong perubahan dalam penyelenggaraan pemerintahan, khususnya dalam pemberian pelayanan publik kepada masyarakat. Pemanfaatan sistem elektronik memungkinkan instansi pemerintah menyelenggarakan pelayanan secara lebih cepat, efisien, dan terintegrasi. Berbagai pelayanan administrasi kependudukan, kesehatan, perpajakan, pendidikan, dan keimigrasian kini memanfaatkan teknologi digital sebagai sarana pengumpulan, penyimpanan, serta pemrosesan data masyarakat. Perubahan tersebut merupakan bagian dari perkembangan pemerintahan berbasis elektronik atau *electronic government* yang bertujuan meningkatkan kualitas pelayanan dan efektivitas penyelenggaraan pemerintahan.

Meskipun memberikan kemudahan, digitalisasi pelayanan publik juga menimbulkan risiko terhadap keamanan informasi dan pelindungan data pribadi. Data yang dikelola oleh instansi pemerintah sering kali mencakup informasi penting, seperti nama, alamat, Nomor Induk Kependudukan (NIK), data kesehatan, informasi keuangan, dan informasi lain yang dapat mengidentifikasi seseorang. Apabila data tersebut diakses, diungkapkan, diubah, atau dimusnahkan tanpa kewenangan, dampaknya tidak hanya berkaitan dengan kerugian individual, tetapi juga dapat memengaruhi kepercayaan masyarakat terhadap penyelenggaraan pemerintahan.

Pelindungan data pribadi merupakan bagian dari hak konstitusional warga negara. Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 memberikan jaminan perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, dan harta benda seseorang. Jaminan tersebut menjadi dasar konstitusional bagi negara untuk membentuk pengaturan yang memberikan perlindungan terhadap data pribadi masyarakat. Dalam konteks negara hukum, kewajiban pemerintah tidak hanya terbatas pada penyediaan pelayanan, tetapi juga mencakup perlindungan terhadap hak-hak masyarakat yang berkaitan dengan penggunaan teknologi informasi.

Sebelum lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), pengaturan pelindungan data pribadi di Indonesia tersebar dalam berbagai peraturan sektoral. Yuniarti (2019) menjelaskan bahwa perkembangan teknologi informasi meningkatkan kerentanan terhadap privasi individu sehingga diperlukan pengaturan hukum yang memberikan perlindungan lebih menyeluruh. Kehadiran UU PDP kemudian memberikan dasar hukum yang lebih komprehensif mengenai hak subjek data pribadi, kewajiban pengendali dan prosesor data pribadi, serta mekanisme pertanggungjawaban atas pelanggaran pelindungan data pribadi.

UU PDP memberikan kedudukan hukum kepada instansi pemerintah sebagai badan publik yang dapat bertindak sebagai pengendali maupun prosesor data pribadi. Pasal 1 angka 4 menjelaskan bahwa pengendali data pribadi merupakan pihak yang menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Sementara itu, Pasal 1 angka 5 mengatur prosesor data pribadi sebagai pihak yang melakukan pemrosesan data pribadi atas nama pengendali. Selanjutnya, Pasal 19 secara tegas memungkinkan badan publik berkedudukan sebagai pengendali maupun prosesor data pribadi. Dengan demikian, instansi pemerintah tidak dikecualikan dari kewajiban hukum dalam penyelenggaraan pelindungan data pribadi.

Kewajiban tersebut antara lain mencakup pelaksanaan pemrosesan data sesuai dengan dasar hukum yang sah, menjaga keamanan dan kerahasiaan data, mencegah akses yang tidak sah, serta memberikan pemberitahuan apabila terjadi kegagalan pelindungan data pribadi. Pasal 35 UU PDP mewajibkan pengendali melakukan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan yang bertentangan dengan ketentuan peraturan perundang-

undangan. Pasal 39 juga mengatur kewajiban mencegah akses yang tidak sah terhadap data pribadi. Selain itu, Pasal 46 mewajibkan pengendali menyampaikan pemberitahuan tertulis paling lambat 3 x 24 jam kepada subjek data pribadi dan lembaga apabila terjadi kegagalan pelindungan data pribadi.

Di sisi lain, tanggung jawab instansi pemerintah juga harus dilihat berdasarkan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik. Undang-undang tersebut mengatur kewajiban penyelenggara pelayanan publik untuk memberikan pelayanan sesuai standar pelayanan, menjamin kepastian hukum, serta memenuhi hak masyarakat sebagai penerima pelayanan. Pasal 15 mengatur kewajiban penyelenggara pelayanan publik, termasuk menyediakan sarana dan prasarana pelayanan yang memadai serta memberikan pelayanan sesuai standar yang telah ditetapkan. Dengan demikian, keamanan data pribadi yang digunakan dalam proses pelayanan digital merupakan salah satu aspek penting dalam menjamin kualitas dan kepastian pelayanan publik.

Persoalan pertanggungjawaban administratif tersebut dapat dilihat melalui insiden serangan siber terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024. Serangan ransomware terhadap PDNS 2 di Surabaya menyebabkan terganggunya sejumlah sistem elektronik pemerintah, termasuk layanan keimigrasian. Kementerian Komunikasi dan Informatika bersama Badan Siber dan Sandi Negara serta pihak pengelola infrastruktur melakukan langkah pemulihan terhadap sistem yang terdampak. Insiden tersebut menunjukkan bahwa gangguan keamanan pada infrastruktur digital pemerintah dapat menimbulkan dampak luas terhadap keberlangsungan pelayanan publik.

Dalam perkembangannya, BSSN menyampaikan bahwa salah satu persoalan utama dalam insiden PDNS 2 adalah tidak tersedianya cadangan data yang memadai pada sistem yang terdampak. Informasi mengenai serangan tersebut juga menunjukkan pentingnya penerapan sistem pencadangan dan pemulihan data sebagai bagian dari tata kelola keamanan sistem elektronik. Meskipun serangan dilakukan oleh pihak eksternal, keadaan tersebut tidak secara otomatis menghapus tanggung jawab hukum penyelenggara sistem elektronik. Penilaian tanggung jawab tetap harus memperhatikan apakah kewajiban pencegahan, pengamanan, pencadangan, dan penanganan insiden telah dilaksanakan secara layak (Badan Siber dan Sandi Negara, 2024; Kementerian Komunikasi dan Informatika, 2024).

Insiden PDNS dalam penelitian ini digunakan sebagai ilustrasi penerapan norma hukum, bukan sebagai objek pemeriksaan forensik ataupun penilaian terhadap kesalahan individu tertentu. Fokus penelitian diarahkan pada bagaimana ketentuan hukum mengalokasikan tanggung jawab antara instansi pengguna layanan, pengelola infrastruktur, dan pihak lain yang terlibat dalam pemrosesan data pribadi. Hal ini penting karena dalam sistem pengelolaan data secara terpusat, satu instansi dapat menentukan tujuan pemrosesan data, sedangkan instansi lain atau penyedia infrastruktur menjalankan fungsi teknis penyimpanan dan pengelolaan sistem.

Persoalan lain yang perlu diperhatikan adalah dasar hukum pemrosesan data pribadi oleh instansi pemerintah. Dalam pelayanan publik, pemrosesan data tidak selalu didasarkan pada persetujuan subjek data sebagaimana lazim ditemukan pada layanan komersial. Pasal 20 ayat (2) UU PDP memberikan beberapa dasar pemrosesan data pribadi, antara lain persetujuan yang sah, pemenuhan kewajiban perjanjian, pemenuhan kewajiban hukum pengendali, pelaksanaan tugas untuk kepentingan umum atau pelayanan publik, serta kepentingan lain yang diatur undang-undang. Dengan demikian, pemrosesan data oleh instansi pemerintah dapat didasarkan pada kewajiban hukum atau pelaksanaan tugas pelayanan publik tanpa selalu memerlukan persetujuan sebagai dasar pemrosesan.

Keadaan tersebut menimbulkan konsekuensi bahwa masyarakat tidak selalu memiliki kebebasan untuk menolak penyerahan data yang diperlukan dalam pelayanan administrasi pemerintahan. Oleh sebab itu, kewajiban instansi pemerintah dalam melindungi data pribadi harus dilaksanakan secara sungguh-sungguh. Penyerahan data oleh masyarakat untuk memperoleh pelayanan tidak dapat dimaknai sebagai pelepasan hak atas pelindungan data pribadi maupun sebagai pembebasan tanggung jawab instansi pemerintah apabila terjadi pelanggaran.

Penelitian mengenai pelindungan data pribadi dan tanggung jawab pemerintah telah dilakukan oleh beberapa peneliti sebelumnya. Yuniarti (2019) mengkaji pelindungan hukum data pribadi di Indonesia sebelum terbentuknya pengaturan yang komprehensif melalui UU PDP. Sugiantari et al. (2024) membahas sanksi hukum dan pertanggungjawaban pemerintah dalam insiden kebocoran data pada Pusat Data Nasional. Kajian tersebut memberikan gambaran mengenai pentingnya penegakan hukum terhadap kegagalan pelindungan data pribadi dalam penyelenggaraan pemerintahan.

Namun, pembahasan mengenai hubungan antara pertanggungjawaban berdasarkan UU PDP dan UU Pelayanan Publik masih perlu diperdalam. Kedua undang-undang tersebut memiliki ruang lingkup pengaturan yang berbeda, tetapi dapat diterapkan secara bersamaan terhadap penyelenggaraan pelayanan publik digital. Selain itu, pembagian tanggung jawab antara pengendali dan prosesor data pribadi dalam penggunaan infrastruktur bersama serta hubungan antara sanksi kelembagaan dan sanksi terhadap aparatur pemerintah perlu dianalisis secara lebih sistematis.

Berdasarkan permasalahan tersebut, penelitian ini memiliki dua rumusan masalah. Pertama, bagaimana pengaturan pertanggungjawaban administratif instansi pemerintah sebagai pengendali data pribadi berdasarkan UU PDP dan UU Pelayanan Publik? Kedua, bagaimana mekanisme pemberatan sanksi administratif terhadap instansi pemerintah yang lalai melindungi data pribadi dalam penyelenggaraan pelayanan publik digital?

Penelitian ini diharapkan memberikan kontribusi dalam pengembangan hukum administrasi negara, khususnya mengenai pertanggungjawaban instansi pemerintah dalam penyelenggaraan pelayanan publik berbasis elektronik. Selain itu, penelitian ini diharapkan dapat memberikan rekomendasi normatif mengenai penguatan mekanisme pengawasan, penjatuhan sanksi administratif, dan perlindungan hukum bagi masyarakat sebagai subjek data pribadi.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif atau *normative legal research*, yaitu penelitian yang mengkaji hukum sebagai norma dan kaidah yang berlaku dalam sistem hukum. Penelitian hukum normatif digunakan karena permasalahan yang dibahas berkaitan dengan pengaturan kewajiban, kewenangan, dan pertanggungjawaban administratif instansi pemerintah dalam melindungi data pribadi masyarakat. Fokus penelitian bukan pada pengukuran perilaku aparatur pemerintah atau masyarakat secara empiris, melainkan pada analisis kecukupan, keselarasan, dan penerapan norma hukum positif.

Penelitian ini menggunakan tiga pendekatan. Pertama, pendekatan perundang-undangan (*statute approach*) digunakan untuk mengkaji ketentuan dalam UU PDP, UU Pelayanan Publik, Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan, Undang-Undang Informasi dan Transaksi Elektronik, serta peraturan mengenai penyelenggaraan sistem elektronik dan pemerintahan berbasis elektronik. Pendekatan ini bertujuan mengidentifikasi

hubungan antarnorma, pembagian kewajiban, serta dasar hukum penjatuhan sanksi administratif.

Kedua, pendekatan konseptual (*conceptual approach*) digunakan untuk menganalisis konsep pertanggungjawaban administratif, pengendali dan prosesor data pribadi, kepastian hukum, asas legalitas, Asas-Asas Umum Pemerintahan yang Baik (AUPB), akuntabilitas, kelalaian administratif, dan perlindungan hukum. Konsep-konsep tersebut digunakan sebagai landasan untuk menilai apakah kewajiban instansi pemerintah dalam melindungi data pribadi telah dirumuskan secara jelas dan dapat dilaksanakan secara efektif.

Ketiga, pendekatan kasus (*case approach*) digunakan dengan menjadikan insiden serangan ransomware terhadap PDNS pada Juni 2024 sebagai ilustrasi penerapan ketentuan hukum. Insiden tersebut tidak dianalisis melalui pemeriksaan forensik maupun pengumpulan data lapangan, tetapi digunakan untuk menguji relevansi norma mengenai keamanan sistem elektronik, tanggung jawab pengendali data, dan keberlangsungan pelayanan publik.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi UUD NRI Tahun 1945, UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, UU Nomor 25 Tahun 2009 tentang Pelayanan Publik, UU Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan, UU Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, serta peraturan lain yang relevan.

Bahan hukum sekunder meliputi buku hukum administrasi negara, buku metodologi penelitian hukum, artikel jurnal ilmiah, hasil penelitian terdahulu, dan publikasi resmi pemerintah mengenai pelindungan data pribadi serta insiden PDNS. Bahan hukum tersier berupa kamus hukum dan ensiklopedia hukum digunakan untuk membantu menjelaskan istilah hukum yang relevan.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan menelusuri peraturan perundang-undangan melalui Jaringan Dokumentasi dan Informasi Hukum (JDIH), basis data peraturan Badan Pemeriksa Keuangan, serta publikasi resmi lembaga pemerintah. Bahan hukum sekunder ditelusuri melalui basis data jurnal ilmiah, termasuk Google Scholar, Garuda, dan SINTA, dengan menggunakan kata kunci pertanggungjawaban administratif, pelindungan data pribadi, kebocoran data, pelayanan publik digital, pengendali data pribadi, dan sanksi administratif.

Seluruh bahan hukum dianalisis secara kualitatif dengan sifat preskriptif-analitis. Penafsiran gramatikal digunakan untuk memahami makna ketentuan berdasarkan rumusan norma, sedangkan penafsiran sistematis digunakan untuk menghubungkan ketentuan UU PDP dengan UU Pelayanan Publik dan peraturan terkait. Selanjutnya, hasil analisis digunakan untuk mengidentifikasi persoalan pengaturan dan merumuskan rekomendasi normatif mengenai indikator pemberatan sanksi administratif terhadap instansi pemerintah yang lalai melindungi data pribadi.

HASIL DAN PEMBAHASAN

Pengaturan Pertanggungjawaban Administratif Instansi Pemerintah sebagai Pengendali Data Pribadi Berdasarkan UU PDP dan UU Pelayanan Publik

a. Kedudukan Instansi Pemerintah sebagai Pengendali dan Prosesor Data Pribadi

UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan dasar hukum bagi pengaturan hubungan antara subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi. Pengaturan tersebut merupakan bagian penting dalam membangun sistem pelindungan

data yang menempatkan tanggung jawab pemrosesan pada pihak yang memiliki kewenangan untuk menentukan tujuan dan cara pemrosesan data.

Berdasarkan Pasal 1 angka 4 UU PDP, pengendali data pribadi merupakan setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Sementara itu, Pasal 1 angka 5 menjelaskan bahwa prosesor data pribadi merupakan pihak yang melakukan pemrosesan data pribadi atas nama pengendali. Ketentuan Pasal 19 menegaskan bahwa pengendali dan prosesor dapat berasal dari unsur badan publik.

Pengaturan tersebut menunjukkan bahwa instansi pemerintah memiliki kewajiban hukum dalam setiap kegiatan pemrosesan data pribadi yang dilakukannya. Status sebagai badan publik tidak menghilangkan tanggung jawab untuk memastikan bahwa data masyarakat diproses berdasarkan dasar hukum yang sah, sesuai tujuan pelayanan, dan dilindungi dari akses maupun penggunaan yang tidak berwenang.

Dalam praktik pelayanan publik digital, satu sistem elektronik dapat digunakan oleh beberapa instansi sekaligus. Misalnya, suatu kementerian atau pemerintah daerah menentukan tujuan pengumpulan data masyarakat untuk pelayanan tertentu, sedangkan penyedia infrastruktur teknologi bertugas menyimpan dan mengelola sistem elektronik. Dalam hubungan tersebut, penentuan kedudukan pengendali dan prosesor tidak dapat dilakukan hanya berdasarkan lokasi penyimpanan data.

Instansi yang menentukan tujuan dan kendali pemrosesan dapat berkedudukan sebagai pengendali data pribadi. Sementara itu, pihak yang hanya menjalankan pemrosesan berdasarkan instruksi pengendali dapat berkedudukan sebagai prosesor. Namun, apabila suatu pihak secara mandiri menentukan tujuan dan cara pemrosesan tertentu, kedudukannya harus dinilai berdasarkan fungsi aktual tersebut.

Pembagian peran ini penting karena setiap pihak memiliki kewajiban hukum yang berbeda. Pengendali bertanggung jawab memastikan adanya dasar pemrosesan yang sah, menentukan kebijakan keamanan, dan memastikan terpenuhinya hak subjek data. Prosesor wajib memproses data sesuai instruksi pengendali dan memenuhi kewajiban keamanan yang berlaku. Hubungan kontraktual antara kedua pihak tidak dengan sendirinya menghapus tanggung jawab hukum masing-masing.

b. Kewajiban Pengendali Data Pribadi Menurut UU PDP

UU PDP mengatur beberapa kewajiban yang harus dipenuhi pengendali data pribadi dalam melaksanakan pemrosesan data.

Pertama, pemrosesan data pribadi harus memiliki dasar hukum sebagaimana ditentukan dalam Pasal 20 ayat (2). Dasar pemrosesan tersebut meliputi persetujuan yang sah, pemenuhan kewajiban perjanjian, pemenuhan kewajiban hukum pengendali, pelaksanaan tugas untuk kepentingan umum atau pelayanan publik, serta kepentingan lain yang diatur dalam undang-undang.

Dalam konteks pelayanan publik, instansi pemerintah dapat menggunakan dasar pemrosesan berupa kewajiban hukum atau pelaksanaan tugas untuk kepentingan umum dan pelayanan publik. Oleh karena itu, persetujuan bukan satu-satunya dasar pemrosesan data pribadi. Meskipun demikian, penggunaan dasar pemrosesan tersebut tetap harus memenuhi prinsip pembatasan tujuan, transparansi, dan pertanggungjawaban.

Kedua, pengendali wajib melakukan pelindungan keamanan data pribadi. Pasal 35 UU PDP mewajibkan pengendali melakukan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan yang bertentangan dengan ketentuan hukum. Kewajiban

tersebut diperkuat oleh Pasal 39 yang mengatur pencegahan akses yang tidak sah terhadap data pribadi.

Kewajiban keamanan tidak cukup dipenuhi melalui penyusunan kebijakan tertulis semata. Instansi pemerintah perlu menerapkan langkah teknis dan organisatoris yang sesuai dengan tingkat risiko pemrosesan data. Langkah tersebut dapat berupa pembatasan hak akses, autentikasi, enkripsi, pencadangan data, pemantauan aktivitas sistem, audit keamanan, pembaruan perangkat lunak, serta penyusunan prosedur penanganan insiden.

Ketiga, pengendali wajib memberikan pemberitahuan apabila terjadi kegagalan pelindungan data pribadi. Pasal 46 UU PDP mewajibkan pemberitahuan tertulis paling lambat 3 x 24 jam kepada subjek data pribadi dan lembaga. Pemberitahuan tersebut harus memuat informasi mengenai data pribadi yang terungkap, waktu dan cara terjadinya kegagalan pelindungan, serta upaya penanganan dan pemulihan yang dilakukan.

Kewajiban pemberitahuan memiliki fungsi penting karena memungkinkan masyarakat mengetahui risiko yang timbul terhadap data pribadinya. Melalui pemberitahuan tersebut, subjek data dapat mengambil langkah pencegahan, seperti mengamankan akun, mengganti kredensial, dan mewaspadai penyalahgunaan identitas.

Keempat, pengendali wajib mempertanggungjawabkan pemrosesan data pribadi sebagaimana diatur dalam Pasal 47 UU PDP. Ketentuan tersebut mencerminkan prinsip akuntabilitas, yaitu pengendali tidak cukup hanya menyatakan telah melaksanakan kewajiban pelindungan data, tetapi juga harus dapat menunjukkan bukti kepatuhannya.

Dengan demikian, tanggung jawab pengendali tidak berhenti pada saat data berhasil dikumpulkan atau disimpan. Tanggung jawab tersebut berlangsung selama seluruh rangkaian pemrosesan data pribadi, mulai dari perolehan, penggunaan, penyimpanan, pengungkapan, hingga penghapusan atau pemusnahan data.

c. Pertanggungjawaban Instansi Pemerintah Berdasarkan UU Pelayanan Publik

UU Nomor 25 Tahun 2009 tentang Pelayanan Publik mengatur kewajiban penyelenggara dan pelaksana pelayanan dalam memberikan pelayanan kepada masyarakat. Dalam konteks pelayanan digital, kewajiban tersebut mencakup penyediaan sistem yang dapat menjamin keamanan, kepastian, dan keberlangsungan pelayanan.

Pasal 15 UU Pelayanan Publik menetapkan kewajiban penyelenggara, antara lain menyusun dan menetapkan standar pelayanan, menyediakan sarana dan prasarana yang memadai, memberikan pelayanan berkualitas, serta melaksanakan pelayanan sesuai ketentuan peraturan perundang-undangan.

Selain itu, Pasal 34 mengatur perilaku pelaksana pelayanan publik yang harus profesional, tidak mempersulit masyarakat, dan tidak menyalahgunakan kewenangan. Ketentuan ini relevan ketika kelalaian aparatur dalam mengelola sistem elektronik mengakibatkan terganggunya pelayanan atau tidak terlindunginya data masyarakat.

Pertanggungjawaban berdasarkan UU Pelayanan Publik juga berkaitan dengan hak masyarakat untuk memperoleh pelayanan yang berkualitas dan menyampaikan pengaduan atas penyelenggaraan pelayanan. Pasal 18 memberikan hak kepada masyarakat untuk mengetahui standar pelayanan, mengawasi pelaksanaan pelayanan, serta memperoleh tanggapan terhadap pengaduan yang disampaikan.

Dalam hal terjadi kebocoran data pribadi, masyarakat tidak hanya mengalami risiko penyalahgunaan informasi, tetapi juga dapat mengalami kerugian akibat terganggunya akses terhadap layanan pemerintahan. Oleh karena itu, kegagalan menjaga keamanan sistem elektronik dapat berhubungan langsung dengan kualitas pelayanan publik.

Pasal 54 UU Pelayanan Publik mengatur jenis sanksi administratif terhadap penyelenggara atau pelaksana yang melanggar ketentuan tertentu. Bentuk sanksinya meliputi teguran tertulis, pembebasan dari jabatan, penurunan gaji sebesar satu kali kenaikan gaji berkala untuk paling lama satu tahun, penurunan pangkat, hingga pemberhentian, sesuai dengan jenis pelanggaran yang disebutkan dalam pasal tersebut.

Ketentuan ini memperlihatkan bahwa UU Pelayanan Publik tidak hanya mengatur tanggung jawab kelembagaan, tetapi juga menyediakan instrumen pertanggungjawaban terhadap penyelenggara dan pelaksana pelayanan. Meskipun demikian, penjatuhan sanksi tetap harus didasarkan pada unsur pelanggaran yang sesuai dengan ketentuan undang-undang dan prosedur kepegawaian yang berlaku.

d. Hubungan UU PDP dengan UU Pelayanan Publik

UU PDP dan UU Pelayanan Publik memiliki objek pengaturan yang berbeda, tetapi keduanya saling melengkapi dalam penyelenggaraan pelayanan publik digital.

UU PDP menitikberatkan pada perlindungan hak subjek data dan kewajiban pihak yang melakukan pemrosesan data pribadi. Sementara itu, UU Pelayanan Publik menitikberatkan pada tanggung jawab penyelenggara dalam memenuhi standar dan hak masyarakat sebagai penerima layanan.

Hubungan kedua undang-undang tersebut dapat dilihat melalui tiga aspek.

Pertama, aspek kewajiban keamanan. UU PDP mewajibkan pengendali dan prosesor melakukan langkah pelindungan data pribadi, sedangkan UU Pelayanan Publik mewajibkan penyelenggara memberikan pelayanan sesuai standar dan ketentuan hukum.

Kedua, aspek akuntabilitas. UU PDP menempatkan pengendali sebagai pihak yang harus dapat menunjukkan pertanggungjawaban atas pemrosesan data. UU Pelayanan Publik menempatkan penyelenggara dan pelaksana sebagai pihak yang bertanggung jawab atas penyelenggaraan pelayanan kepada masyarakat.

Ketiga, aspek penegakan hukum. UU PDP menyediakan sanksi administratif terhadap pelanggaran kewajiban pelindungan data pribadi. Sementara itu, UU Pelayanan Publik menyediakan sanksi administratif terhadap pelanggaran kewajiban penyelenggara dan pelaksana pelayanan.

Dengan demikian, pelanggaran pelindungan data pribadi dalam pelayanan publik digital dapat dianalisis melalui kedua rezim hukum tersebut sepanjang unsur pelanggaran masing-masing terpenuhi. Penerapan kedua undang-undang secara bersamaan tidak berarti menjatuhkan sanksi secara otomatis, melainkan memerlukan pemeriksaan terhadap dasar kewenangan, bentuk pelanggaran, pihak yang bertanggung jawab, dan prosedur penjatuhan sanksi.

Analisis Pertanggungjawaban Administratif dalam Insiden Pusat Data Nasional Sementara Tahun 2024

a. Kedudukan Insiden PDNS dalam Kerangka Hukum Pelindungan Data Pribadi

Insiden serangan ransomware terhadap PDNS 2 pada Juni 2024 merupakan contoh penting mengenai risiko keamanan dalam penyelenggaraan pelayanan publik digital. Serangan tersebut mengakibatkan gangguan terhadap sejumlah layanan pemerintah, termasuk layanan keimigrasian. Pemerintah melalui Kominfo, BSSN, dan pihak pengelola infrastruktur melakukan isolasi sistem serta pemulihan layanan yang terdampak.

Insiden tersebut memperlihatkan bahwa keamanan infrastruktur digital merupakan unsur penting dalam keberlangsungan pelayanan publik. Gangguan terhadap satu pusat data

dapat menimbulkan dampak terhadap berbagai instansi yang menggunakan infrastruktur tersebut.

Dalam perspektif hukum, perlu dibedakan antara terjadinya serangan siber dan adanya pelanggaran kewajiban administratif. Serangan oleh pihak ketiga merupakan peristiwa yang dapat menimbulkan kegagalan sistem, tetapi tidak serta-merta membuktikan bahwa penyelenggara telah melakukan kelalaian. Penilaian kelalaian memerlukan pemeriksaan terhadap standar keamanan yang berlaku, kebijakan pencadangan, pengawasan sistem, serta tindakan mitigasi sebelum dan setelah serangan terjadi.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik memberikan dasar kewajiban tersebut. Pasal 3 mewajibkan penyelenggara sistem elektronik menyelenggarakan sistem secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem sebagaimana mestinya. Pasal 24 juga mewajibkan penyelenggara menyediakan prosedur dan sarana pengamanan untuk mencegah serta menanggulangi ancaman dan serangan yang dapat menimbulkan gangguan, kegagalan, dan kerugian.

Selain itu, Pasal 40 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik mengatur keamanan SPBE, termasuk penjaminan kerahasiaan, keutuhan, ketersediaan, dan keaslian data serta informasi. Penjaminan ketersediaan dilakukan melalui penyediaan cadangan dan pemulihan.

Berdasarkan ketentuan tersebut, pencadangan data bukan sekadar pilihan teknis, tetapi bagian dari tata kelola keamanan sistem pemerintahan berbasis elektronik.

b. Pembagian Tanggung Jawab antara Instansi Pengguna dan Pengelola Infrastruktur

Penggunaan pusat data bersama menimbulkan persoalan mengenai penentuan pihak yang bertanggung jawab ketika terjadi kegagalan pelindungan data pribadi.

Dalam sistem pengelolaan data terpusat, instansi pengguna dapat menentukan tujuan pengumpulan dan pemrosesan data masyarakat sesuai dengan tugas serta kewenangannya. Di sisi lain, pengelola pusat data dapat menjalankan fungsi penyimpanan, pemeliharaan, dan pengamanan infrastruktur elektronik.

Oleh karena itu, penentuan kedudukan para pihak harus dilakukan berdasarkan fungsi aktual dalam pemrosesan data.

Instansi pengguna layanan dapat berkedudukan sebagai pengendali data pribadi apabila menentukan tujuan dan kendali pemrosesan data masyarakat. Pengelola infrastruktur dapat berkedudukan sebagai prosesor apabila menjalankan pemrosesan atas nama dan berdasarkan instruksi instansi pengguna.

Namun, apabila pengelola infrastruktur turut menentukan tujuan atau cara pemrosesan secara mandiri, kedudukan hukumnya perlu dinilai lebih lanjut berdasarkan ketentuan UU PDP.

Pembagian tersebut berpengaruh terhadap penentuan kewajiban pemberitahuan, pengamanan, dan pertanggungjawaban. Pengendali tidak dapat sepenuhnya mengalihkan tanggung jawab kepada prosesor hanya karena penyimpanan data dilakukan melalui infrastruktur pihak lain. Sebaliknya, prosesor juga tidak dapat mengabaikan kewajiban keamanan yang melekat pada kegiatan pemrosesan yang dilakukannya.

Dalam hubungan tersebut, diperlukan dokumentasi pembagian tugas, perjanjian pemrosesan data, standar operasional prosedur, mekanisme audit, dan prosedur penanganan insiden. Dokumen tersebut menjadi dasar untuk menentukan pihak yang bertanggung jawab apabila terjadi kegagalan pelindungan data pribadi.

c. Pengaruh Dasar Pemrosesan Data terhadap Tanggung Jawab Instansi Pemerintah

Pemrosesan data pribadi dalam pelayanan publik memiliki karakteristik berbeda dengan pemrosesan data dalam kegiatan komersial. Instansi pemerintah sering kali memproses data

masyarakat karena diwajibkan oleh undang-undang atau karena diperlukan untuk melaksanakan tugas pelayanan publik.

Pasal 20 ayat (2) UU PDP mengatur bahwa pemrosesan data pribadi dapat dilakukan berdasarkan beberapa dasar pemrosesan, termasuk pemenuhan kewajiban hukum pengendali serta pelaksanaan tugas untuk kepentingan umum atau pelayanan publik.

Penggunaan dasar pemrosesan tersebut menunjukkan bahwa instansi pemerintah tidak selalu memerlukan persetujuan sebagai dasar utama pemrosesan data. Akan tetapi, hal tersebut tidak berarti instansi pemerintah memperoleh kebebasan tanpa batas dalam menggunakan dan menyimpan data masyarakat.

Pemrosesan tetap harus memenuhi prinsip pelindungan data pribadi, termasuk pembatasan tujuan, ketepatan data, keamanan, transparansi, dan akuntabilitas.

Dengan demikian, tidak adanya persetujuan sebagai dasar pemrosesan tidak dapat dijadikan alasan untuk mengurangi tanggung jawab instansi pemerintah. Justru karena masyarakat dalam banyak pelayanan administrasi tidak memiliki alternatif yang sebanding untuk menolak penyerahan data, instansi pemerintah harus memastikan adanya perlindungan yang memadai terhadap data yang dikelolanya.

Dalam konteks ini, pelindungan data pribadi merupakan bagian dari kewajiban negara dalam menjamin hak masyarakat. Instansi pemerintah tidak hanya bertindak sebagai penyedia pelayanan, tetapi juga sebagai pihak yang memiliki kewajiban untuk menjaga kepercayaan masyarakat dalam penggunaan sistem digital pemerintahan.

d. Kedudukan UU PDP terhadap Insiden PDNS Tahun 2024

UU PDP diundangkan pada 17 Oktober 2022 dan memuat ketentuan penyesuaian dalam Pasal 74 yang memberikan waktu paling lama dua tahun kepada pengendali, prosesor, dan pihak terkait untuk menyesuaikan kegiatan pemrosesannya.

Insiden PDNS terjadi pada Juni 2024, sebelum berakhirnya periode penyesuaian tersebut. Oleh karena itu, analisis terhadap penerapan kewajiban dan sanksi UU PDP perlu memperhatikan tanggal terjadinya peristiwa, ketentuan transisi, serta prinsip legalitas dan larangan pemberlakuan sanksi secara surut.

Hal tersebut tidak berarti bahwa seluruh kewajiban keamanan sistem elektronik pada saat insiden terjadi tidak berlaku. Pada periode tersebut, kewajiban penyelenggara sistem elektronik tetap dapat dianalisis berdasarkan PP Nomor 71 Tahun 2019, UU Informasi dan Transaksi Elektronik, UU Pelayanan Publik, serta ketentuan lain yang relevan.

Dengan demikian, PDNS digunakan sebagai ilustrasi untuk menguji hubungan antarrejim hukum, bukan sebagai dasar untuk menyatakan bahwa suatu instansi atau pejabat tertentu telah terbukti melakukan pelanggaran UU PDP.

Mekanisme Pemberatan Sanksi Administratif terhadap Instansi Pemerintah yang Lalai Melindungi Data Pribadi

a. Pengaturan Sanksi Administratif dalam Pasal 57 UU PDP

Pasal 57 UU PDP mengatur sanksi administratif terhadap pelanggaran terhadap kewajiban tertentu dalam undang-undang tersebut. Bentuk sanksinya meliputi:

1. Peringatan tertulis.
2. Penghentian sementara kegiatan pemrosesan data pribadi.
3. Penghapusan atau pemusnahan data pribadi.
4. Denda administratif.

Pasal 57 ayat (3) menentukan bahwa denda administratif paling tinggi sebesar 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran. Selanjutnya, Pasal

57 ayat (4) menentukan bahwa penjatuhan sanksi administratif dilakukan oleh lembaga sebagaimana dimaksud dalam UU PDP.

Pengaturan tersebut menunjukkan bahwa UU PDP telah menyediakan instrumen sanksi administratif untuk menegakkan kepatuhan pengendali dan prosesor data pribadi. Namun, ketentuan mengenai penentuan tingkat beratnya sanksi masih perlu diperjelas melalui parameter yang dapat diterapkan secara konsisten.

Pasal 57 ayat (2) tidak secara khusus menyebutkan indikator pemberatan sanksi. Oleh karena itu, perlu dirumuskan pedoman yang mempertimbangkan sifat pelanggaran, tingkat kesalahan, dampak terhadap subjek data, dan tindakan yang dilakukan setelah insiden terjadi.

Pemberatan sanksi tidak boleh didasarkan semata-mata pada besarnya dampak kebocoran data. Penilaian juga harus mempertimbangkan apakah instansi telah melakukan tindakan pencegahan yang layak, apakah risiko telah diketahui sebelumnya, dan apakah instansi melakukan pemulihan secara cepat setelah insiden terjadi.

b. Hubungan Sanksi UU PDP dengan Sanksi UU Pelayanan Publik

Sanksi administratif dalam UU PDP perlu dianalisis bersama dengan ketentuan sanksi dalam UU Pelayanan Publik.

UU PDP berorientasi pada kepatuhan terhadap kewajiban pelindungan data pribadi. Sementara itu, UU Pelayanan Publik mengatur pertanggungjawaban penyelenggara dan pelaksana dalam memberikan pelayanan kepada masyarakat.

Pasal 54 UU Pelayanan Publik menyediakan beberapa bentuk sanksi yang ditujukan kepada penyelenggara atau pelaksana sesuai jenis pelanggarannya. Ketentuan tersebut dapat menjadi dasar penegakan tanggung jawab terhadap aparatur yang terbukti melanggar kewajiban penyelenggaraan pelayanan publik.

Selain itu, pertanggungjawaban aparatur pemerintah juga perlu memperhatikan ketentuan disiplin kepegawaian, termasuk Peraturan Pemerintah Nomor 94 Tahun 2021 tentang Disiplin Pegawai Negeri Sipil bagi aparatur yang termasuk dalam cakupan peraturan tersebut.

Dengan demikian, terdapat dua ranah pertanggungjawaban yang perlu dibedakan.

Pertama, pertanggungjawaban kelembagaan terhadap pelanggaran kewajiban pengendali atau prosesor data pribadi. Kedua, pertanggungjawaban pejabat atau aparatur yang secara individual terbukti melakukan pelanggaran kewajiban jabatan atau disiplin.

Kedua bentuk pertanggungjawaban tersebut dapat berjalan secara terkoordinasi sepanjang terdapat dasar hukum dan terpenuhinya unsur pelanggaran masing-masing. Penjatuhan sanksi terhadap instansi tidak otomatis membuktikan kesalahan pribadi seluruh pejabat yang berada di dalamnya. Sebaliknya, penjatuhan hukuman disiplin kepada pejabat juga tidak serta-merta menghapus tanggung jawab kelembagaan.

c. Indikator Pemberatan Sanksi Administratif

Untuk meningkatkan efektivitas penegakan hukum, penelitian ini mengusulkan empat indikator pemberatan sanksi administratif.

Skala dampak dan tingkat kerugian

Indikator pertama adalah besarnya dampak yang ditimbulkan oleh kegagalan pelindungan data pribadi. Penilaian dapat mempertimbangkan jumlah subjek data yang terdampak, jenis data yang terungkap, tingkat sensitivitas data, serta dampak terhadap keberlangsungan pelayanan publik.

Kebocoran data kesehatan, data keuangan, dan data identitas kependudukan dapat memiliki risiko yang berbeda dengan terungkapnya informasi umum. Oleh karena itu, tingkat sensitivitas data perlu menjadi pertimbangan dalam menentukan beratnya sanksi.

Selain dampak terhadap individu, perlu diperhatikan pula apakah insiden menyebabkan terganggunya layanan publik yang bersifat penting, seperti pelayanan kesehatan, keimigrasian, administrasi kependudukan, dan pelayanan sosial.

Tingkat kesalahan atau kelalaian instansi

Indikator kedua adalah tingkat kesalahan atau kelalaian dalam melaksanakan kewajiban keamanan data pribadi.

Kelalaian dapat dinilai berdasarkan tidak dilaksanakannya standar operasional prosedur, pengabaian rekomendasi keamanan, tidak adanya pencadangan data yang memadai, lemahnya pengendalian akses, serta tidak dilaksanakannya audit keamanan secara berkala.

Dalam hal instansi telah mengetahui adanya kerentanan sistem tetapi tidak mengambil tindakan perbaikan yang diperlukan, keadaan tersebut dapat menjadi faktor yang memperberat pertanggungjawaban.

Sebaliknya, apabila instansi telah menerapkan langkah pengamanan yang layak dan melakukan penanganan insiden secara tepat, keadaan tersebut perlu dipertimbangkan dalam menentukan proporsionalitas sanksi.

Tingkat kepatuhan terhadap standar keamanan

Indikator ketiga adalah tingkat kepatuhan instansi terhadap standar keamanan sistem elektronik dan tata kelola pelindungan data pribadi.

Penilaian dapat dilakukan melalui pemeriksaan terhadap kebijakan keamanan informasi, pembatasan akses, pencatatan aktivitas sistem, enkripsi, pencadangan, pengujian keamanan, audit berkala, serta pembagian tanggung jawab antara pengendali dan prosesor.

Kepatuhan terhadap standar keamanan menjadi penting karena tanggung jawab pengendali bukan hanya merespons kebocoran, tetapi juga melakukan tindakan pencegahan yang wajar dan sesuai dengan risiko pemrosesan.

Kualitas respons dan pemulihan setelah insiden

Indikator keempat adalah kualitas tindakan instansi setelah mengetahui adanya kegagalan pelindungan data pribadi.

Penilaian dapat meliputi kecepatan mendeteksi dan mengisolasi gangguan, pemenuhan kewajiban pemberitahuan kepada subjek data, koordinasi dengan lembaga terkait, pemulihan sistem, serta pemberian informasi yang transparan kepada masyarakat.

Instansi yang menyembunyikan insiden, terlambat memberikan pemberitahuan tanpa alasan yang sah, atau tidak melakukan tindakan pemulihan dapat dinilai memiliki tingkat pertanggungjawaban yang lebih berat dibandingkan instansi yang segera mengambil langkah mitigasi.

Keempat indikator tersebut diharapkan dapat menjadi dasar penilaian yang lebih objektif dalam menentukan jenis dan tingkat sanksi administratif.

d. Model Pemberatan Sanksi yang Proporsional

Penerapan pemberatan sanksi perlu memperhatikan prinsip proporsionalitas. Sanksi yang dijatuhkan harus sebanding dengan tingkat pelanggaran dan dampak yang ditimbulkan, tetapi tetap mempertimbangkan tujuan pemulihan dan pencegahan pelanggaran berulang.

Model pemberatan yang diusulkan dalam penelitian ini dapat dilakukan melalui tiga tahapan.

Tahap pertama adalah pemeriksaan kepatuhan. Pada tahap ini, otoritas yang berwenang melakukan pemeriksaan terhadap kewajiban pengendali dan prosesor, termasuk standar keamanan, dasar pemrosesan, dokumentasi, dan mekanisme pengawasan.

Tahap kedua adalah penilaian tingkat pelanggaran. Penilaian dilakukan dengan menggunakan empat indikator, yaitu skala dampak, tingkat kesalahan atau kelalaian, kepatuhan terhadap standar keamanan, serta kualitas respons dan pemulihan.

Tahap ketiga adalah penentuan sanksi. Sanksi dipilih berdasarkan tingkat pelanggaran, mulai dari peringatan tertulis, penghentian sementara kegiatan pemrosesan, penghapusan atau pemusnahan data apabila sesuai dengan ketentuan, hingga denda administratif berdasarkan persyaratan dan batasan yang diatur undang-undang.

Dalam hal pelanggaran juga menunjukkan adanya kesalahan pejabat atau aparatur, hasil pemeriksaan dapat menjadi dasar bagi instansi yang berwenang untuk melakukan proses pertanggungjawaban kepegawaian sesuai peraturan yang berlaku.

Model tersebut perlu dituangkan dalam peraturan pelaksana atau pedoman penegakan hukum agar tidak menimbulkan perbedaan penafsiran antarlembaga. Pengaturan lebih lanjut juga harus memastikan adanya hak bagi instansi yang diperiksa untuk memberikan klarifikasi, mengajukan bukti, dan menggunakan upaya administratif atau hukum yang tersedia.

e. Penguatan Kelembagaan dan Perlindungan Hukum bagi Subjek Data

Efektivitas sanksi administratif tidak hanya ditentukan oleh kelengkapan norma, tetapi juga oleh keberadaan lembaga pengawas yang memiliki kewenangan jelas dan mampu melaksanakan fungsi pengawasan secara independen.

Pasal 58 UU PDP mengamanatkan pembentukan lembaga yang bertanggung jawab dalam penyelenggaraan pelindungan data pribadi. Pasal 59 memberikan fungsi kepada lembaga tersebut untuk merumuskan kebijakan, melakukan pengawasan, menegakkan hukum administratif, dan memfasilitasi penyelesaian sengketa di luar pengadilan.

Keberadaan lembaga tersebut penting untuk memastikan bahwa kewajiban pengendali dan prosesor data pribadi tidak hanya menjadi ketentuan formal, tetapi dapat diawasi dan ditegakkan secara efektif.

Selain itu, penguatan kelembagaan harus disertai dengan mekanisme pengaduan masyarakat yang mudah diakses. Subjek data pribadi perlu memperoleh informasi mengenai pihak yang mengendalikan data, tujuan pemrosesan, serta prosedur yang dapat ditempuh apabila terjadi pelanggaran.

Dalam konteks pelayanan publik, mekanisme pengaduan juga dapat dihubungkan dengan pengawasan Ombudsman Republik Indonesia berdasarkan UU Nomor 37 Tahun 2008 tentang Ombudsman Republik Indonesia, sepanjang persoalan yang dilaporkan termasuk dalam ruang lingkup kewenangannya dan memenuhi unsur maladministrasi.

Dengan demikian, perlindungan hukum terhadap masyarakat tidak hanya diwujudkan melalui pemberian sanksi kepada instansi, tetapi juga melalui pemenuhan hak atas informasi, pemberitahuan insiden, mekanisme pengaduan, pemulihan kerugian, dan akses terhadap penyelesaian sengketa.

SIMPULAN

Pertama, instansi pemerintah memiliki kedudukan hukum sebagai pengendali atau prosesor data pribadi berdasarkan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Kedudukan tersebut ditentukan berdasarkan fungsi dan kewenangan nyata dalam menentukan tujuan serta melakukan pemrosesan data pribadi. Sebagai pengendali, instansi pemerintah wajib memastikan adanya dasar pemrosesan yang sah, menjaga keamanan dan kerahasiaan data, mencegah akses yang tidak sah, memberikan pemberitahuan apabila terjadi kegagalan pelindungan data pribadi, serta mempertanggungjawabkan seluruh kegiatan pemrosesan. Kewajiban tersebut dilengkapi oleh UU Nomor 25 Tahun 2009 tentang Pelayanan Publik yang

mengatur tanggung jawab penyelenggara dan pelaksana dalam memberikan pelayanan sesuai standar dan menjamin hak masyarakat. Dengan demikian, keamanan data pribadi merupakan bagian yang tidak terpisahkan dari kualitas pelayanan publik digital.

Kedua, mekanisme pemberatan sanksi administratif terhadap instansi pemerintah yang lalai melindungi data pribadi masih memerlukan pengaturan yang lebih terperinci. Pasal 57 UU PDP telah menyediakan jenis sanksi administratif, tetapi belum merumuskan indikator pemberatan secara khusus. Oleh karena itu, penelitian ini mengusulkan empat indikator, yaitu skala dampak terhadap subjek data dan pelayanan publik, tingkat kesalahan atau kelalaian instansi, tingkat kepatuhan terhadap standar keamanan, serta kualitas respons dan pemulihan setelah insiden. Penerapan sanksi kelembagaan berdasarkan UU PDP perlu dikoordinasikan dengan pertanggungjawaban pejabat dan aparatur berdasarkan UU Pelayanan Publik serta peraturan disiplin kepegawaian apabila unsur pelanggarannya terpenuhi. Penguatan lembaga pengawas, pedoman pemberian sanksi, dan mekanisme pengaduan masyarakat diperlukan untuk menjamin kepastian hukum, akuntabilitas pemerintahan, serta perlindungan hak masyarakat sebagai subjek data pribadi.

REFERENSI

Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat di Indonesia: Sebuah studi tentang prinsip-prinsipnya, penanganannya oleh pengadilan dalam lingkungan peradilan umum dan pembentukan peradilan administrasi negara*. Bina Ilmu.

Marzuki, P. M. (2017). *Penelitian hukum* (Edisi revisi). Kencana.

Ridwan HR. (2018). *Hukum administrasi negara*. Rajawali Pers.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Sugiantari, A., Wiryawan, I. W., Hengki, I. G., Asrita, N. N., & Putra, I. K. (2024). Analisis sanksi hukum atas pertanggungjawaban pemerintah terhadap insiden bocornya data pribadi masyarakat dari Pusat Data Nasional (PDN) Indonesia. *Jurnal Hukum Saraswati, 6*(2), 728–741. https://ejournal.unmas.ac.id/index.php/JHS/article/view/9979

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS), 1*(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030

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

Republik Indonesia. (2008). *Undang-Undang Nomor 37 Tahun 2008 tentang Ombudsman Republik Indonesia*.

Republik Indonesia. (2009). *Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik*.

Republik Indonesia. (2014). *Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan*.

Republik Indonesia. (2018). *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*.

Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

Republik Indonesia. (2021). *Peraturan Pemerintah Nomor 94 Tahun 2021 tentang Disiplin Pegawai Negeri Sipil*.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Republik Indonesia. (2023). *Undang-Undang Nomor 20 Tahun 2023 tentang Aparatur Sipil Negara*.

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Badan Siber dan Sandi Negara. (2024). *Informasi dan keterangan resmi mengenai insiden serangan ransomware pada Pusat Data Nasional Sementara 2*.

Kementerian Komunikasi dan Informatika. (2024, 24 Juni). *BSSN identifikasi Pusat Data Nasional Sementara diserang ransomware*.

Kementerian Komunikasi dan Informatika. (2024, 27 Juni). *Percepat pemulihan, Kominfo, BSSN dan Telkom operasikan server baru pengganti*.