BANJARESE
PACIFIC INDONESIA
Journal of International Multidisciplinary Research

Tanggung Jawab Negara sebagai Pengendali Data Pribadi atas Serangan Ransomware Pusat Data Nasional Sementara: Analisis Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Fajar Rachmad Dwi Miarsa[1], M. Zamroni[2], Muhammad Alief Nur[3]
Program Studi Ilmu Hukum, Universitas Maarif Hasyim Latif, Sidoarjo, Indonesia[123]
Email: *fajar_rahmad@dosen.umaha.ac.id*, zamroni@dosen.umaha.ac.id, muhammad_alief_nur@student.umaha.ac.id*

Informasi Artikel
E-ISSN : 3026-6874
Vol: 1 No: 2 Desember 2023
Halaman : 702-710

Keywords:
Personal Data Protection
State Liability
National Data Center

Abstract
This study analyses the position and obligations of the state as a personal data controller in operating the Temporary National Data Center (PDNS), as well as the forms of state liability and remedies available to data subjects following the ransomware attack on PDNS 2 in June 2024. It employs normative legal research with statutory, conceptual, case, and GDPR comparative approaches, supported by materials up to August 2024. The findings show that user institutions act as personal data controllers, the Ministry of Communication and Informatics may qualify as a joint controller or processor, and the infrastructure provider acts as a processor, so ultimate responsibility remains with the state. Law Number 27 of 2022 requires controllers to secure data, prevent unauthorised access, and notify data protection failures within 72 hours. The minimal data backup admitted by the government makes a force majeure defence difficult to sustain. State liability may be pursued through administrative, civil, and administrative court routes, but is currently hindered by the transition period, the absence of a data protection authority, the lack of compensation procedures, and evidentiary difficulties. The novelty lies in analysing the state's position in a shared data center and mapping liability routes during the transition period.

Abstrak
Penelitian ini bertujuan menganalisis kedudukan dan kewajiban negara sebagai pengendali data pribadi dalam penyelenggaraan Pusat Data Nasional Sementara (PDNS), serta bentuk tanggung jawab dan mekanisme pemulihan hak subjek data atas serangan ransomware PDNS 2 pada Juni 2024. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan dengan GDPR, didukung bahan hukum hingga Agustus 2024. Hasil penelitian menunjukkan bahwa instansi pengguna berkedudukan sebagai pengendali data pribadi, Kementerian Komunikasi dan Informatika dapat dikualifikasikan sebagai pengendali bersama atau prosesor, dan penyedia infrastruktur sebagai prosesor, sehingga tanggung jawab akhir tetap berada pada negara sebagai pengendali. Undang-Undang Nomor 27 Tahun 2022 mewajibkan pengendali menjamin keamanan data, mencegah akses tidak sah, dan memberitahukan kegagalan pelindungan data dalam 3 x 24 jam. Rendahnya rekam cadang yang diakui pemerintah membuat dalih keadaan memaksa sulit diterima. Tanggung jawab negara dapat ditempuh melalui jalur administratif, perdata, dan tata usaha negara, tetapi terhambat oleh masa transisi, belum terbentuknya lembaga pelindungan data pribadi, belum adanya peraturan tentang tata cara ganti rugi, dan kesulitan pembuktian. Kebaruan penelitian ini terletak pada analisis kedudukan negara dalam pusat data bersama dan pemetaan jalur pertanggungjawabannya selama masa transisi. Implikasinya, pembentukan lembaga pelindungan data pribadi yang independen dan standar rekam cadang wajib menjadi kebutuhan mendesak.

Kata Kunci : Pelindungan Data Pribadi; Tanggung Jawab Negara; Pusat Data Nasional

PENDAHULUAN

Transformasi digital pemerintahan menjadikan data pribadi warga negara sebagai aset yang dikelola negara dalam jumlah sangat besar. Melalui Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), instansi pusat dan pemerintah daerah diwajibkan menggunakan Pusat Data Nasional, yang penyelenggaraannya antara lain melalui pusat data milik

kementerian di bidang komunikasi dan informatika. Konsolidasi ini meningkatkan efisiensi, tetapi sekaligus memusatkan risiko. Ketika satu pusat data gagal diamankan, dampaknya langsung dirasakan oleh banyak instansi dan jutaan warga yang datanya tersimpan di dalamnya.

Risiko tersebut terwujud pada Juni 2024. Pusat Data Nasional Sementara (PDNS) 2 di Surabaya diserang *ransomware* Brain Cipher. Aktivitas berbahaya mulai berlangsung pada 20 Juni 2024 dan berdampak pada 239 instansi pengguna, terdiri atas 30 kementerian/lembaga, 15 provinsi, 148 kabupaten, dan 48 kota, termasuk layanan keimigrasian (Rochman, 2024). Peretas meminta tebusan sebesar 8 juta dolar Amerika Serikat atau sekitar Rp131 miliar (Rakhmayanti, 2024). Dalam rapat kerja dengan Komisi I DPR, Kepala Badan Siber dan Sandi Negara (BSSN) mengakui bahwa hanya sekitar 2 persen data PDNS 2 yang memiliki cadangan di Batam, dan menyebut tata kelola serta ketiadaan cadangan data sebagai persoalan utama (Anggraeni, 2024).

Peristiwa ini terjadi ketika Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) masih berada dalam masa transisi. UU PDP diundangkan pada 17 Oktober 2022, tetapi Pasal 74 memberi waktu paling lama dua tahun bagi pengendali dan prosesor data pribadi untuk menyesuaikan diri, yaitu sampai 17 Oktober 2024. Hingga Agustus 2024, lembaga penyelenggara pelindungan data pribadi yang diamanatkan Pasal 58 juga belum terbentuk, karena rancangan peraturan presidennya masih menunggu keputusan Presiden (CNN Indonesia, 2024a). Kondisi ini memunculkan pertanyaan mendasar: sejauh mana negara dapat dimintai pertanggungjawaban sebagai pengendali data pribadi, dan melalui mekanisme apa warga dapat memulihkan haknya.

Kajian terdahulu menunjukkan bahwa hak atas privasi merupakan bagian dari hak asasi manusia yang dilindungi melalui UU PDP, dan politik hukum pembentukannya dinilai responsif terhadap perkembangan teknologi (Fauzy & Shandy, 2022; Rizqiyanto et al., 2024). Badar et al. (2023) menilai UU PDP sebagai langkah preventif negara untuk melindungi masyarakat dari ancaman kebocoran data, tetapi ketentuan mengenai lembaga pengawasnya masih perlu ditinjau. Syailendra et al. (2024) juga mencatat bahwa UU PDP merupakan kemajuan penting, tetapi implementasinya masih menghadapi banyak hambatan. Di sektor publik, persoalan ini nyata: sepanjang 2023, sektor publik menyumbang 69 persen atau 71 insiden kebocoran data di Indonesia (Evandio, 2024a).

Namun, kajian-kajian tersebut belum membahas insiden yang menimpa infrastruktur data milik negara sendiri, dengan skala lintas instansi seperti PDNS 2. Kebaruan penelitian ini terletak pada analisis kedudukan negara sebagai pengendali dan prosesor data pribadi dalam penyelenggaraan pusat data bersama, serta pemetaan jalur pertanggungjawaban yang tersedia bagi warga dalam masa transisi UU PDP. Berdasarkan uraian tersebut, rumusan masalah penelitian ini adalah: (1) bagaimana kedudukan dan kewajiban negara sebagai pengendali data pribadi dalam penyelenggaraan PDNS menurut UU PDP dan peraturan terkait; dan (2) bagaimana bentuk tanggung jawab negara serta mekanisme pemulihan hak subjek data atas serangan *ransomware* PDNS 2.

METODE

Penelitian ini merupakan penelitian hukum normatif, yaitu penelitian yang mengkaji norma hukum positif beserta asas dan doktrin yang melandasinya (Marzuki, 2014). Penelitian menggunakan empat pendekatan. Pendekatan perundang-undangan *(statute approach)* digunakan untuk menelaah UU PDP, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan, Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE, Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, serta Peraturan Mahkamah Agung Nomor 2 Tahun 2019. Pendekatan konseptual *(conceptual approach)* digunakan untuk menelaah konsep pengendali dan prosesor data pribadi serta tanggung jawab negara atas perbuatan melanggar hukum oleh pemerintah. Pendekatan kasus *(case approach)* digunakan untuk menganalisis insiden serangan *ransomware* PDNS 2 sebagai peristiwa hukum. Pendekatan perbandingan *(comparative approach)* digunakan untuk membandingkan pengaturan tanggung jawab pengendali dalam UU PDP dengan *General Data Protection Regulation* Uni Eropa.

Bahan hukum primer terdiri atas peraturan perundang-undangan tersebut. Bahan hukum sekunder meliputi buku, artikel jurnal ilmiah, keterangan resmi pemerintah, dan pemberitaan media,

termasuk keterangan Menteri Komunikasi dan Informatika serta Kepala BSSN dalam rapat kerja dengan Komisi I DPR. Bahan hukum dikumpulkan melalui studi kepustakaan, lalu dianalisis secara kualitatif-preskriptif dengan menghubungkan fakta insiden dengan kewajiban hukum pengendali data pribadi untuk menilai bentuk tanggung jawab dan mekanisme pemulihan yang tersedia.

HASIL DAN PEMBAHASAN

1. Kronologi dan Dampak Serangan Ransomware PDNS 2

Serangan terhadap PDNS 2 tidak terjadi secara tiba-tiba. Menteri Komunikasi dan Informatika menjelaskan bahwa gangguan pertama terdeteksi pada 17 Juni 2024, ketika penyerang berupaya menonaktifkan fitur keamanan Windows Defender. Pada 20 Juni 2024 pukul 00.54 WIB, aktivitas berbahaya dimulai, antara lain pemasangan berkas berbahaya, penghapusan berkas sistem penting, dan penonaktifan layanan yang sedang berjalan (Rochman, 2024). Rangkaian peristiwa berikutnya dirangkum dalam Tabel 1.

Tabel 1. Kronologi Serangan Ransomware PDNS 2 dan Respons Pemerintah

Waktu	Peristiwa
17 Juni 2024	Gangguan pertama terdeteksi; penyerang berupaya menonaktifkan Windows Defender (Rochman, 2024)
20 Juni 2024	Aktivitas berbahaya dimulai: pemasangan berkas berbahaya, penghapusan berkas sistem, dan penonaktifan layanan (Rochman, 2024)
27 Juni 2024	Rapat kerja Komisi I DPR: 239 instansi terdampak; tebusan 8 juta dolar AS; hanya 2 persen data memiliki cadangan (Rochman, 2024; Rakhmayanti, 2024; Anggraeni, 2024)
28 Juni 2024	Presiden meminta BPKP mengaudit tata kelola dan keuangan Pusat Data Nasional (Evandio, 2024b)
2–3 Juli 2024	Kelompok Brain Cipher menyatakan akan memberikan kunci dekripsi secara gratis dan merilis tautan unduhannya (CNN Indonesia, 2024b)
3 Juli 2024	Presiden menegaskan seluruh data nasional harus memiliki rekam cadang (BPMI Setpres, 2024)
4 Juli 2024	Direktur Jenderal Aplikasi Informatika menyatakan mundur sebagai bentuk tanggung jawab moral (Indiraphasa, 2024)
2 Agustus 2024	Komunitas Konsumen Indonesia menggugat Menteri Komunikasi dan Informatika ke PTUN Jakarta atas tindakan faktual (Kontan.co.id, 2024)

Sumber: diolah dari berbagai pemberitaan, Juni–Agustus 2024.

Tabel 1 menunjukkan tiga hal penting. Pertama, terdapat jeda waktu antara deteksi gangguan pertama pada 17 Juni dan dimulainya serangan pada 20 Juni 2024, yang menimbulkan pertanyaan mengenai efektivitas pemantauan keamanan. Kedua, pemulihan layanan sangat bergantung pada kunci dekripsi yang justru diberikan oleh peretas, bukan pada cadangan data milik negara. Ketiga, respons pemerintah lebih banyak berupa langkah politik dan administratif, seperti audit, instruksi rekam cadang, dan pengunduran diri pejabat, sedangkan pemulihan hak warga sebagai subjek data belum menjadi fokus.

Dampak serangan ini bersifat lintas sektor. Dari 282 instansi yang menggunakan PDNS 2, sebanyak 239 instansi terdampak, sedangkan 43 instansi lainnya tidak terdampak karena hanya menyimpan cadangan data di PDNS 2 (Rochman, 2024). Telkomsigma, selaku penyedia infrastruktur PDNS, menyatakan bahwa pihaknya hanya menyediakan infrastruktur sesuai kerangka acuan kerja dari Kementerian Komunikasi dan Informatika dan mengikuti audit forensik yang dilakukan BSSN (Evandio, 2024c). Fakta ini penting untuk menentukan siapa yang memikul tanggung jawab sebagai pengendali dan prosesor data pribadi.

2. Kedudukan dan Kewajiban Negara sebagai Pengendali Data Pribadi

UU PDP tidak membedakan sektor publik dan swasta dalam hal kewajiban pelindungan data. Pasal 1 angka 4 mendefinisikan pengendali data pribadi sebagai setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan

melakukan kendali pemrosesan data pribadi. Adapun prosesor data pribadi menurut Pasal 1 angka 5 adalah pihak yang melakukan pemrosesan data pribadi atas nama pengendali. Pasal 1 angka 9 kemudian mendefinisikan badan publik antara lain sebagai lembaga eksekutif, legislatif, yudikatif, dan badan lain yang sebagian atau seluruh dananya bersumber dari anggaran pendapatan dan belanja negara dan/atau daerah. Dengan demikian, instansi pemerintah yang memproses data warga tunduk pada kewajiban yang sama dengan korporasi.

Dalam penyelenggaraan PDNS, terdapat beberapa pihak dengan peran berbeda. Pemetaan peran tersebut disajikan dalam Tabel 2.

Tabel 2. Pemetaan Peran Para Pihak dalam Penyelenggaraan PDNS menurut UU PDP

Pihak	Peran dalam PDNS	Kualifikasi menurut UU PDP
Instansi pengguna (kementerian/lembaga dan pemerintah daerah)	Menentukan tujuan pengumpulan dan pemrosesan data warga untuk layanan publik masing-masing	Pengendali data pribadi (Pasal 1 angka 4)
Kementerian Komunikasi dan Informatika	Menyelenggarakan Pusat Data Nasional dan menetapkan kerangka acuan kerja infrastruktur	Pengendali bersama (Pasal 18) atau prosesor (Pasal 1 angka 5), bergantung pada tingkat kendalinya atas pemrosesan
Penyedia infrastruktur	Menyediakan infrastruktur sesuai kerangka acuan kerja dari kementerian	Prosesor yang wajib bertindak berdasarkan perintah pengendali (Pasal 51 ayat (1))
BSSN	Melakukan koordinasi keamanan siber dan audit forensik	Bukan pengendali; berperan dalam keamanan SPBE dan manajemen krisis siber

Sumber: diolah dari UU Nomor 27 Tahun 2022, Perpres Nomor 95 Tahun 2018, dan Evandio (2024c).

Tabel 2 menunjukkan bahwa tanggung jawab dalam PDNS bersifat berlapis. Instansi pengguna merupakan pengendali karena menentukan tujuan pemrosesan data warga. Kementerian Komunikasi dan Informatika tidak sekadar menyewakan ruang penyimpanan, tetapi menetapkan spesifikasi infrastruktur dan mengelola layanan pusat data. Karena itu, kementerian dapat dikualifikasikan sebagai pengendali bersama apabila turut menentukan cara pemrosesan, atau setidaknya sebagai prosesor. Kualifikasi ini penting karena Pasal 18 ayat (2) mensyaratkan pengendali bersama memiliki perjanjian yang mengatur peran dan tanggung jawab masing-masing, sedangkan Pasal 51 ayat (3) menegaskan bahwa pemrosesan oleh prosesor tetap menjadi tanggung jawab pengendali. Dalam kedua kemungkinan tersebut, negara tidak dapat melepaskan diri dari tanggung jawab.

UU PDP membebankan sejumlah kewajiban yang relevan dengan insiden PDNS 2. Pasal 35 mewajibkan pengendali melindungi dan memastikan keamanan data pribadi melalui langkah teknis operasional serta menentukan tingkat keamanan dengan memperhatikan sifat dan risiko data. Pasal 39 mewajibkan pengendali mencegah akses tidak sah terhadap data pribadi dengan sistem keamanan yang andal dan bertanggung jawab. Pasal 46 ayat (1) mewajibkan pengendali menyampaikan pemberitahuan tertulis paling lambat 3 x 24 jam kepada subjek data dan lembaga apabila terjadi kegagalan pelindungan data pribadi, dengan memuat data yang terungkap, waktu dan cara terungkapnya, serta upaya penanganan dan pemulihan. Dalam hal tertentu, Pasal 46 ayat (3) juga mewajibkan pemberitahuan kepada masyarakat. Selanjutnya, Pasal 47 menegaskan bahwa pengendali bertanggung jawab atas pemrosesan data pribadi dan wajib menunjukkan pertanggungjawabannya dalam memenuhi prinsip pelindungan data.

Kewajiban serupa telah ada sebelum UU PDP. Pasal 15 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mewajibkan setiap penyelenggara sistem elektronik menyelenggarakan sistemnya secara andal dan aman serta bertanggung jawab atas penyelenggaraannya. Pengecualian hanya diberikan dalam Pasal 15 ayat (3), yaitu apabila dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik. Peraturan Presiden Nomor 95 Tahun 2018 juga mewajibkan setiap instansi pusat dan

pemerintah daerah menerapkan keamanan SPBE dengan berkoordinasi bersama lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Dalam konteks PDNS 2, dalih keadaan memaksa sulit diterima. Serangan *ransomware* merupakan risiko yang dapat diperkirakan dalam pengelolaan pusat data, sehingga penyelenggara wajib menyiapkan langkah mitigasi, terutama rekam cadang. Pengakuan BSSN bahwa hanya 2 persen data yang memiliki cadangan, serta penegasan bahwa persoalan utamanya adalah tata kelola (Anggraeni, 2024), menunjukkan bahwa kerugian terutama timbul dari tidak dipenuhinya standar keamanan yang patut, bukan semata dari kekuatan di luar kendali. Instruksi Presiden setelah insiden agar seluruh data nasional direkam cadang (BPMI Setpres, 2024) justru menegaskan bahwa langkah tersebut seharusnya telah menjadi standar sejak awal.

3. Bentuk Tanggung Jawab Negara dan Mekanisme Pemulihan Hak Subjek Data

a. Tanggung jawab administratif

UU PDP menyediakan sanksi administratif dalam Pasal 57 ayat (2), berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda administratif. Pasal 57 ayat (1) memasukkan pelanggaran terhadap Pasal 35, Pasal 39 ayat (1), Pasal 46 ayat (1) dan ayat (3), serta Pasal 47 sebagai pelanggaran yang dapat dikenai sanksi administratif (Rizki, 2022). Pasal 57 ayat (3) menetapkan denda administratif paling tinggi 2 persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran, sehingga secara normatif dapat diterapkan pula pada badan publik. Namun, penerapannya terhadap badan publik menghadapi tiga kendala. Pertama, denda yang dijatuhkan kepada instansi pemerintah pada akhirnya bersumber dari anggaran negara atau daerah, sehingga efek jeranya terhadap pejabat yang lalai patut dipertanyakan. Kedua, Pasal 57 ayat (4) menentukan bahwa sanksi administratif dijatuhkan oleh lembaga, sementara lembaga tersebut belum terbentuk hingga Agustus 2024 (CNN Indonesia, 2024a). Ketiga, Pasal 57 ayat (5) mendelegasikan tata cara pengenaan sanksi administratif kepada peraturan pemerintah yang juga belum ditetapkan.

Dalam praktiknya, pertanggungjawaban yang muncul setelah insiden lebih bersifat politik dan administratif internal. Presiden meminta Badan Pengawasan Keuangan dan Pembangunan mengaudit tata kelola dan keuangan Pusat Data Nasional (Evandio, 2024b), dan Direktur Jenderal Aplikasi Informatika mengundurkan diri sebagai bentuk tanggung jawab moral (Indiraphasa, 2024). Langkah-langkah ini penting bagi akuntabilitas pemerintahan, tetapi tidak secara langsung memulihkan hak warga yang datanya terdampak.

b. Tanggung jawab perdata dan tata usaha negara

Pasal 12 ayat (1) UU PDP memberi hak kepada subjek data pribadi untuk menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadinya. Namun, Pasal 12 ayat (2) mendelegasikan ketentuan lebih lanjut mengenai pelanggaran dan tata cara pengenaan ganti rugi kepada peraturan pemerintah yang belum ditetapkan. Akibatnya, gugatan terhadap negara harus bertumpu pada rezim perbuatan melanggar hukum oleh penguasa *(onrechtmatige overheidsdaad)*.

Sejak berlakunya Peraturan Mahkamah Agung Nomor 2 Tahun 2019, sengketa perbuatan melanggar hukum oleh badan dan/atau pejabat pemerintahan menjadi kewenangan Peradilan Tata Usaha Negara (PTUN), setelah upaya administratif ditempuh (Munawaroh, 2022). Perbuatan pemerintah yang dapat digugat tidak terbatas pada keputusan tertulis, tetapi juga tindakan administrasi pemerintahan, yaitu perbuatan pejabat pemerintahan atau penyelenggara negara lainnya untuk melakukan dan/atau tidak melakukan perbuatan konkret dalam rangka penyelenggaraan pemerintahan sebagaimana dimaksud Pasal 1 angka 8 Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan. Tidak dilakukannya langkah pengamanan yang patut atas pusat data, seperti rekam cadang, dapat dipandang sebagai bentuk tidak melakukan perbuatan konkret tersebut. Jalur inilah yang ditempuh Komunitas Konsumen Indonesia, yang pada 2 Agustus 2024 menggugat Menteri Komunikasi dan Informatika ke PTUN Jakarta dengan Nomor Perkara 269/G/TF/2024/PTUN.JKT, dengan dalil kegagalan melindungi Pusat Data Nasional dan ketiadaan rekam cadang (Kontan.co.id, 2024). Meski demikian, penelitian Asimah et al. (2020) menunjukkan bahwa penanganan perkara tindakan faktual di pengadilan belum konsisten, sehingga kepastian hasil gugatan semacam ini masih terbatas.

Jalur lain juga tersedia. Badan Perlindungan Konsumen Nasional menyatakan konsumen yang dirugikan dapat mengajukan gugatan perwakilan kelompok *(class action)* berdasarkan Undang-Undang Perlindungan Konsumen (Mardatillah, 2024). Sementara itu, gugatan warga negara *(citizen lawsuit)* dinilai sebagai langkah yang tepat untuk mendorong perbaikan kebijakan keamanan data karena tidak mensyaratkan pembuktian kerugian individual dan memungkinkan tuntutan berupa perbaikan regulasi (Hakim, 2024).

c. Perbandingan dengan General Data Protection Regulation

UU PDP banyak mengadopsi konsep dari *General Data Protection Regulation* (GDPR) Uni Eropa, yaitu Regulation (EU) 2016/679. Perbandingan keduanya membantu menilai celah pengaturan tanggung jawab badan publik dalam UU PDP. Perbandingan tersebut disajikan dalam Tabel 3.

Tabel 3. Perbandingan Pengaturan Tanggung Jawab Pengendali dalam UU PDP dan GDPR

Aspek	UU PDP	GDPR
Badan publik sebagai pengendali	Termasuk dalam definisi pengendali (Pasal 1 angka 4)	Termasuk dalam definisi pengendali (Article 4(7))
Pengendali bersama dan prosesor	Perjanjian pengendali bersama (Pasal 18); prosesor bertindak atas perintah pengendali (Pasal 51)	Pengaturan pengendali bersama (Article 26); kontrak dengan prosesor (Article 28)
Pemberitahuan kegagalan pelindungan	Paling lambat 3 x 24 jam kepada subjek data dan lembaga (Pasal 46)	Paling lambat 72 jam kepada otoritas pengawas (Article 33); kepada subjek data jika berisiko tinggi (Article 34)
Ganti rugi	Hak menggugat dan menerima ganti rugi; tata cara diatur peraturan pemerintah (Pasal 12)	Hak atas kompensasi dari pengendali atau prosesor (Article 82)
Denda bagi badan publik	Tidak dibedakan dari korporasi; denda paling tinggi 2 persen dari pendapatan tahunan atau penerimaan tahunan (Pasal 57 ayat (3))	Negara anggota menentukan apakah dan sejauh mana denda dikenakan pada badan publik (Article 83(7))
Otoritas pengawas	Lembaga ditetapkan oleh dan bertanggung jawab kepada Presiden (Pasal 58)	Otoritas pengawas yang independen (Article 52)

Sumber: diolah dari UU Nomor 27 Tahun 2022 dan Regulation (EU) 2016/679.

Tabel 3 menunjukkan dua perbedaan penting. Pertama, GDPR secara tegas menyerahkan kepada negara anggota pengaturan apakah dan sejauh mana denda dikenakan pada badan publik, sedangkan UU PDP tidak membedakan badan publik dari korporasi. Rumusan penerimaan tahunan dalam Pasal 57 ayat (3) memang memungkinkan denda dikenakan pada instansi pemerintah, tetapi UU PDP tidak mengatur bentuk pertanggungjawaban lain yang lebih efektif bagi badan publik, seperti sanksi terhadap pejabat yang lalai atau kewajiban pemulihan kepada subjek data. Kedua, GDPR mensyaratkan otoritas pengawas yang independen, sedangkan lembaga dalam UU PDP ditetapkan oleh dan bertanggung jawab kepada Presiden. Ketika pengendali yang melanggar adalah kementerian, kedudukan lembaga di bawah Presiden berpotensi menimbulkan konflik kepentingan dalam pengawasan dan penegakan hukum terhadap sesama instansi pemerintah.

d. Hambatan pemulihan hak subjek data

Berdasarkan analisis di atas, terdapat empat hambatan utama. Pertama, masa transisi UU PDP hingga 17 Oktober 2024 membuat sebagian pihak menganggap kewajiban UU PDP belum dapat ditegakkan sepenuhnya, padahal kewajiban keamanan sistem elektronik telah lama ada dalam UU ITE. Kedua, ketiadaan lembaga pelindungan data pribadi menyebabkan tidak ada otoritas independen yang dapat menerima pengaduan, melakukan pemeriksaan, dan menjatuhkan sanksi administratif. Para peneliti kebijakan karena itu mendorong agar lembaga tersebut segera dibentuk dan berada di luar struktur pemerintah agar netral, mengingat sektor publik justru menjadi penyumbang terbesar insiden kebocoran data (Evandio, 2024a). Ketiga, belum adanya peraturan pemerintah tentang tata cara ganti rugi membuat hak dalam Pasal 12 sulit dijalankan. Keempat, subjek data menghadapi kesulitan

membuktikan kerugian dan hubungan kausal, terutama apabila tidak menerima pemberitahuan mengenai data apa saja yang terdampak sebagaimana diwajibkan Pasal 46.

e. Rekomendasi penguatan

Berdasarkan hambatan tersebut, terdapat beberapa langkah yang perlu dilakukan:

1. Presiden perlu segera membentuk lembaga pelindungan data pribadi sesuai Pasal 58 UU PDP dengan jaminan independensi dari kementerian yang juga berperan sebagai pengendali data.
2. Pemerintah perlu menetapkan peraturan pemerintah tentang pelaksanaan UU PDP, termasuk tata cara pengenaan ganti rugi dalam Pasal 12 ayat (2) dan tata cara pengenaan sanksi administratif dalam Pasal 57 ayat (5) yang memuat bentuk pertanggungjawaban efektif bagi badan publik.
3. Kementerian Komunikasi dan Informatika dan seluruh instansi pengguna perlu menyusun perjanjian pengendali bersama atau perjanjian pemrosesan data yang menegaskan pembagian tanggung jawab, sesuai Pasal 18 dan Pasal 51 UU PDP.
4. Setiap instansi pengguna PDNS perlu menyampaikan pemberitahuan kepada subjek data yang terdampak sebagaimana diwajibkan Pasal 46 UU PDP, disertai informasi upaya pemulihan yang dilakukan.
5. Pemerintah perlu menjadikan rekam cadang, uji keamanan berkala, dan rencana pemulihan bencana sebagai standar wajib yang diaudit bagi seluruh pusat data pemerintah, termasuk pusat data milik pemerintah daerah di Jawa Timur.

KESIMPULAN

Pertama, dalam penyelenggaraan PDNS, negara berkedudukan sebagai pengendali data pribadi melalui instansi pengguna yang menentukan tujuan pemrosesan, sedangkan Kementerian Komunikasi dan Informatika dapat dikualifikasikan sebagai pengendali bersama atau prosesor, dan penyedia infrastruktur sebagai prosesor. Dalam setiap kualifikasi tersebut, tanggung jawab akhir tetap berada pada negara sebagai pengendali. UU PDP mewajibkan pengendali menjamin keamanan data, mencegah akses tidak sah, memberitahukan kegagalan pelindungan data dalam 3 x 24 jam, dan menunjukkan akuntabilitasnya. Rendahnya rekam cadang dan persoalan tata kelola yang diakui pemerintah menunjukkan bahwa kewajiban tersebut belum dipenuhi secara patut, sehingga dalih keadaan memaksa sulit diterima.

Kedua, tanggung jawab negara atas serangan *ransomware* PDNS 2 dapat ditempuh melalui jalur administratif, perdata, dan tata usaha negara. Namun, hingga Agustus 2024, efektivitasnya terhambat oleh masa transisi UU PDP, belum terbentuknya lembaga pelindungan data pribadi, belum adanya peraturan pemerintah tentang tata cara ganti rugi, serta kesulitan pembuktian oleh subjek data. Dibandingkan dengan GDPR, UU PDP juga belum mengatur secara khusus sanksi bagi badan publik dan belum menjamin independensi lembaga pengawasnya. Akibatnya, pertanggungjawaban yang muncul lebih bersifat politik dan administratif internal, sedangkan pemulihan hak warga bergantung pada inisiatif gugatan masyarakat ke PTUN.

Berdasarkan simpulan tersebut, pemerintah disarankan segera membentuk lembaga pelindungan data pribadi yang independen, menetapkan peraturan pelaksana UU PDP, dan mewajibkan standar rekam cadang serta audit keamanan bagi seluruh pusat data pemerintah. Penelitian selanjutnya disarankan mengkaji putusan PTUN atas gugatan yang berkaitan dengan insiden PDNS 2 dan menilai efektivitas lembaga pelindungan data pribadi setelah terbentuk.

REFERENCES

Anggraeni, R. (2024, 27 Juni). BSSN sebut hanya 2% data PDSN Surabaya yang terbackup di Batam. *Bisnis.com*. https://teknologi.bisnis.com/read/20240627/101/1777669/bssn-sebut-hanya-2-data-pdsn-surabaya-yang-terbackup-di-batam

Asimah, D., Muttaqin, Z., & Sugiharti, D. K. (2020). Implementasi perluasan kompetensi PTUN dalam mengadili tindakan faktual (onrechtmatige overheidsdaad/OOD). *Acta Diurnal: Jurnal Ilmu Hukum Kenotariatan, 4*(1), 152–170. https://doi.org/10.23920/acta.v4i1.531

Badar, E. S., Fauzi, A., & Jazuli, A. (2023). Personal data protection policy in Law Number 27 of 2022 in

the perspective of positive law and Islamic law. *Hukum Islam, 23*(1), 61–74. https://doi.org/10.24014/jhi.v23i1.20465

BPMI Setpres. (2024, 3 Juli). *Evaluasi peretasan PDNS, Presiden: Semua data nasional harus direkam cadang*. Kementerian Sekretariat Negara Republik Indonesia. https://setneg.go.id/baca/index/evaluasi_peretasan_pdns_presiden_semua_data_nasional_harus_direkam_cadang

CNN Indonesia. (2024a, 9 Agustus). 'Deadline' sebentar lagi, sudah ada hilal lembaga PDP? *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20240809144129-192-1131211/deadline-sebentar-lagi-sudah-ada-hilal-lembaga-pdp

CNN Indonesia. (2024b, 4 Juli). Kominfo sudah uji coba kunci dari Brain Cipher, berhasil di spesimen. *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20240704095401-192-1117417/kominfo-sudah-uji-coba-kunci-dari-brain-cipher-berhasil-di-spesimen

Evandio, A. (2024a, 6 Juli). Alarm bahaya peretasan PDNS, lembaga perlindungan data perlu dibentuk. *Bisnis.com*. https://teknologi.bisnis.com/read/20240706/84/1779980/alarm-bahaya-peretasan-pdns-lembaga-perlindungan-data-perlu-dibentuk

Evandio, A. (2024b, 28 Juni). Imbas peretasan, Jokowi minta BPKP audit tata kelola dan finansial PDN. *Bisnis.com*. https://teknologi.bisnis.com/read/20240628/84/1777891/imbas-peretasan-jokowi-minta-bpkp-audit-tata-kelola-dan-finansial-pdn

Evandio, A. (2024c, 29 Juni). Telkomsigma siap ikuti rekomendasi untuk pulihkan PDN. *Bisnis.com*. https://teknologi.bisnis.com/read/20240629/84/1777892/telkomsigma-siap-ikuti-rekomendasi-untuk-pulihkan-pdn

Fauzy, E., & Shandy, N. A. R. (2022). Hak atas privasi dan politik hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Lex Renaissance, 7*(3), 445–461. https://doi.org/10.20885/JLR.vol7.iss3.art1

Hakim, L. N. (2024, 9 Juli). Ahli sebut citizen lawsuit langkah tepat gugat pemerintah terkait keamanan data. *Bisnis.com*. https://kabar24.bisnis.com/read/20240709/15/1780861/ahli-sebut-citizen-lawsuit-langkah-tepat-gugat-pemerintah-terkait-keamanan-data

Indiraphasa, N. S. (2024, 4 Juli). Gagal tangani serangan ransomware PDNS, Dirjen Aptika Kominfo mundur. *NU Online*. https://www.nu.or.id/nasional/gagal-tangani-serangan-ransomware-pdns-dirjen-aptika-kominfo-mundur-RL25g

Kontan.co.id. (2024, 6 Agustus). Menkominfo Budi Arie digugat ke PTUN buntut peretasan PDN. *Kontan*. https://nasional.kontan.co.id/news/menkominfo-budi-arie-digugat-ke-ptun-buntut-peretasan-pdn

Mardatillah, A. (2024, 15 Juli). BPKN: Konsumen bisa ajukan gugatan class action bila dirugikan dalam kasus PDNS. *Hukumonline*. https://www.hukumonline.com/berita/a/bpkn--konsumen-bisa-ajukan-gugatan-class-action-bila-dirugikan-dalam-kasus-pdns-lt6694f0d6735c6/

Marzuki, P. M. (2014). *Penelitian hukum* (Edisi revisi). Prenada Media.

Munawaroh, N. (2022, 23 Desember). Perbuatan melawan hukum oleh penguasa (onrechtmatige overheidsdaad). *Klinik Hukumonline*. https://www.hukumonline.com/klinik/a/perbuatan-melawan-hukum-oleh-penguasa-ionrechtmatige-overheidsdaad-i-lt4d1cdbcfd06b6

Peraturan Mahkamah Agung Nomor 2 Tahun 2019 tentang Pedoman Penyelesaian Sengketa Tindakan Pemerintahan dan Kewenangan Mengadili Perbuatan Melanggar Hukum oleh Badan dan/atau Pejabat Pemerintahan (Onrechtmatige Overheidsdaad).

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182).

Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen

Krisis Siber (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99).

Rakhmayanti, I. (2024, 28 Juni). Terungkap motif hacker serang Pusat Data Nasional minta bayar Rp 131 M. *CNBC Indonesia*. https://www.cnbcindonesia.com/tech/20240628105333-37-550147/terungkap-motif-hacker-serang-pusat-data-nasional-minta-bayar-rp-131-m

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.

Rizki, M. J. (2022, 4 Oktober). Ancaman sanksi administratif hingga pidana dalam UU Pelindungan Data Pribadi. *Hukumonline*. https://www.hukumonline.com/berita/a/ancaman-sanksi-administratif-hingga-pidana-dalam-uu-pelindungan-data-pribadi-lt633c69ce2de5c/

Rizqiyanto, N., Rohman, A. F., & Raya, F. A. M. (2024). Politik hukum pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Media Hukum Indonesia, 2*(2), 1–14. https://doi.org/10.5281/zenodo.10995150

Rochman, F. (2024, 27 Juni). Menkominfo jelaskan kronologi serangan siber PDNS 2. *ANTARA News Kalimantan Selatan*. https://kalsel.antaranews.com/berita/419220/menkominfo-jelaskan-kronologi-serangan-siber-pdns-2

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review, 14*(2), 56–72. https://doi.org/10.15742/ilrev.v14n2.4

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905).

Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601) sebagaimana telah diubah dengan Undang-Undang Nomor 6 Tahun 2023.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).