



## Bentuk Pertanggungjawaban Pemerintah Terhadap Lumpuhnya Pusat Data Nasional Berdasarkan Hukum Administrasi Negara

Husein Muhammad Iqbal<sup>1\*</sup>, Supto Hermawan<sup>2</sup>, Asianto Nugroho<sup>3</sup>

<sup>1-3</sup>Fakultas Hukum Universitas Sebelas Maret, Indonesia

Alamat: Universitas Sebelas Maret, Jl. Ir. Sutami 36A, Ketingan, Surakarta, Jawa Tengah

Korespondensi penulis: [huseiniqbal@student.uns.ac.id](mailto:huseiniqbal@student.uns.ac.id)\*

**Abstract.** *This study examines the government's accountability for the collapse of the National Data Center (Pusat Data Nasional, PDN) due to a cyber attack from an Administrative Law perspective. The increasing reliance on digital technology has made e-government systems more vulnerable to cyber threats, as evidenced by the PDN Surabaya incident in June 2024. The objective of this research is to analyze the government's responsibility in safeguarding personal data and ensuring the continuity of public services. This study explores key legal frameworks, including the Personal Data Protection Law, Presidential Regulations on the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik, SPBE), and other relevant regulations governing cybersecurity and administrative responsibility. The research employs a normative legal research method with a statutory approach, analyzing legal provisions and their application in addressing cyber incidents affecting government-operated databases. The findings reveal that the government can be held accountable through various administrative measures, including the imposition of administrative sanctions, mandatory public notifications, and legal proceedings in administrative courts. However, the study also identifies significant challenges in implementing these measures due to the absence of a dedicated supervisory agency responsible for overseeing the security and resilience of e-government infrastructure. The lack of clear mechanisms for enforcement further complicates accountability efforts. Therefore, this study highlights the urgency of strengthening cybersecurity governance, establishing an independent supervisory body, and enhancing legal frameworks to ensure better protection of personal data and the reliability of digital public services. By addressing these gaps, the government can improve public trust and minimize future cyber risks.*

**Keywords:** *Administrative Law, Government Accountability, National Data Center*

**Abstrak.** Penelitian ini mengkaji akuntabilitas pemerintah atas runtuhnya Pusat Data Nasional (PDN) akibat serangan siber dari perspektif Hukum Administrasi. Ketergantungan yang semakin meningkat pada teknologi digital membuat sistem pemerintahan elektronik (e-government) semakin rentan terhadap ancaman siber, seperti yang terlihat dalam insiden PDN Surabaya pada Juni 2024. Tujuan dari penelitian ini adalah untuk menganalisis tanggung jawab pemerintah dalam melindungi data pribadi serta memastikan kelangsungan layanan publik. Studi ini meneliti kerangka hukum utama, termasuk Undang-Undang Perlindungan Data Pribadi, Peraturan Presiden tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), serta regulasi lain yang mengatur keamanan siber dan tanggung jawab administratif. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, menganalisis ketentuan hukum dan penerapannya dalam menangani insiden siber yang berdampak pada basis data yang dikelola pemerintah. Hasil penelitian menunjukkan bahwa pemerintah dapat dimintai pertanggungjawaban melalui berbagai langkah administratif, termasuk penerapan sanksi administratif, kewajiban pemberitahuan publik, serta proses hukum di pengadilan administrasi. Namun, penelitian ini juga mengidentifikasi tantangan signifikan dalam penerapan langkah-langkah tersebut akibat ketiadaan lembaga pengawas independen yang bertanggung jawab atas keamanan dan ketahanan infrastruktur e-government. Kurangnya mekanisme yang jelas untuk penegakan hukum semakin memperumit upaya akuntabilitas. Oleh karena itu, penelitian ini menekankan pentingnya memperkuat tata kelola keamanan siber, membentuk badan pengawas independen, serta meningkatkan kerangka hukum guna memastikan perlindungan data pribadi yang lebih baik dan keandalan layanan publik digital. Dengan mengatasi kesenjangan ini, pemerintah dapat meningkatkan kepercayaan publik serta meminimalkan risiko serangan siber di masa mendatang.

**Kata kunci:** Hukum Administrasi Negara, Pertanggungjawaban Pemerintah, Pusat Data Nasional

## 1. LATAR BELAKANG

Di era digital seperti saat ini, saat penggunaan teknologi semakin masif, dan berkembang pesatnya teknologi komunikasi banyak sekali aspek kehidupan manusia yang terdampak. Setiap sendi-sendi kehidupan manusia tidak dapat terhindarkan dari perkembangan teknologi yang ada. Semua aktivitas manusia saat ini tidak dapat dilepaskan dari adanya teknologi dan digitalisasi. Hampir semua kegiatan manusia saat ini akan berhubungan dengan yang namanya internet. Perkembangan digital yang ada saat ini tentunya sangat bagus dan berguna bagi kehidupan manusia. Dengan berkembangnya teknologi segala kegiatan manusia dapat berjalan lebih mudah. Namun, dengan adanya perkembangan teknologi ini ada harga yang harus dibayar. Perkembangan teknologi yang saat ini berkaitan erat dengan keberadaan internet dan dalam prosesnya membutuhkan data pribadi dikarenakan banyak aktivitas yang dilakukan secara daring (Anggen Suari and Sarjana 2023). Di dunia digital saat ini data pribadi bukan hanya sekedar kumpulan tulisan saja, tetapi merupakan benda yang sangat berharga. Bahkan, saking berharganya data pribadi di era digital saat ini seorang matematikawan sampai melabeli data pribadi sebagai “*the new oil*” perkataan ini disampaikan oleh Clive Humby, matematikawan asal Inggris pada tahun 2006 (Michael Kershner 2021).

Data pribadi yang sangat penting bagi masyarakat juga memiliki peran krusial dalam konteks kehidupan bernegara. Dalam menjalankan pemerintahan, khususnya dalam hal pelayanan kepada masyarakat, pemerintah sangat memerlukan data pribadi warganya. Pentingnya data pribadi semakin meningkat seiring dengan penerapan *e-government* di Indonesia. Pelayanan publik berbasis elektronik (*e-government*) memanfaatkan teknologi digital untuk meningkatkan efisiensi interaksi antara pemerintah dan masyarakat, dengan cara memanfaatkan teknologi informasi, media, dan komunikasi melalui internet (Iswandari 2022). Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government memulai implementasi *e-government* di Indonesia. Ini didasarkan pada keyakinan bahwa teknologi informasi, media, dan komunikasi dapat memberikan manfaat besar bagi pemerintahan yang beroperasi secara *online*. Dampak positif yang dihasilkan bersifat multidimensi, meliputi: peningkatan standar pelayanan publik, optimalisasi transparansi dan akuntabilitas penyelenggaraan pemerintahan, minimalisasi anggaran untuk transaksi dan komunikasi pemerintahan, sekaligus percepatan terwujudnya masyarakat informasi yang unggul (Indrajit, Zinuddin, and Rudianto 2005). Selain itu penerapan teknologi informasi, media, dan komunikasi (*e-government*) dapat digunakan untuk meningkatkan akses masyarakat terhadap penyelenggaraan negara dan memudahkan masyarakat dalam mengakses pelayanan yang disediakan pemerintah (Laoly 2019). Penerapan

*e-government* juga dianggap sebagai langkah konkret untuk meningkatkan lambatnya proses birokrasi yang disediakan oleh pemerintah.(Roziqin et al. 2022) Selain untuk meningkatkan kualitas pelayanan pemerintah, pelaksanaan *e-government* juga diarahkan kepada peningkatan upaya pemerintah dalam persaingan global (Purwanto 2018).

Dalam penerapan *e-government* di Indonesia terdapat satu permasalahan yang sangat mendasar, yakni perihal keamanan informasi. Isu mengenai keamanan informasi dalam pelaksanaan *e-government* di Indonesia sangatlah penting, sebab pelaksanaan *e-government* sangatlah berkaitan dengan informasi yang merupakan objek pengelolaan *e-government*.(Setiawan 2013) Untuk menjamin keamanan pengolahan data pribadi dalam pelaksanaan e-government, pemerintah melakukan berbagai langkah, mulai dari menyiapkan instrumen hukum melalui UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi hingga membangun infrastruktur penyimpanan data yang dikenal sebagai Pusat Data. Sesuai dengan Peraturan Presiden Nomor 95 Tahun 2018 mengenai Sistem Pemerintahan Berbasis Elektronik, Pusat Data didefinisikan sebagai “fasilitas yang digunakan untuk menampung sistem elektronik dan komponen terkait lainnya untuk tujuan penempatan, penyimpanan, pengolahan data, serta pemulihan data.”

Pusat Data nasional merupakan salah satu instrumen infrastruktur dalam pelaksanaan Sistem Pemerintahan Berbasis Elektronik (SPBE) yang berdasarkan penjelasan Pasal 27 ayat (4) Peraturan Presiden Nomor 95 Tahun 2018 adalah “... sekumpulan Pusat Data yang digunakan secara bagi pakai oleh Instansi Pusat dan Pemerintah Daerah, dan saling terhubung.” Seperti yang telah dijelaskan sebelumnya, Pusat Data nasional merupakan salah satu infrastruktur penting dalam penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE). Oleh karena itu, keberadaan Pusat Data nasional sangat krusial dalam proses pelaksanaan SPBE. Pusat Data nasional memiliki peran penting, terutama dalam sistem pemerintahan dan pelayanan publik. Infrastruktur ini mendukung penyelenggaraan negara dan mewujudkan program pemerintah Satu Data Indonesia. Keberadaan Pusat Data nasional membantu mencapai tujuan Satu Data Indonesia, yaitu menyediakan tata kelola data pemerintah yang akurat, terkini, terintegrasi, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagikan antar instansi pusat dan daerah melalui pemenuhan standar data, metadata, interoperabilitas data, serta penggunaan kode referensi dan data induk. Saat ini, pembangunan Pusat Data nasional masih dalam tahap pengembangan. Pemerintah berencana untuk membangun empat Pusat Data nasional yang akan berlokasi di Cikarang, Batam, Balikpapan, dan Labuan Bajo. Selama proses pembangunan Pusat Data nasional berlangsung, peran Pusat

Data nasional saat ini diakomodir oleh Pusat Data nasional sementara yang terletak di Jakarta dan Surabaya.

Pelaksanaan Pusat Data Nasional Sementara (PDNS) menghadapi tantangan besar akibat serangan siber yang menargetkan PDNS 2. Berdasarkan keterangan dari juru bicara Badan Siber dan Sandi Negara (BSSN), Ariandi Putra, serangan ini pertama kali terdeteksi pada 17 Juni 2024 pukul 23:15 WIB, ketika terjadi upaya menonaktifkan fitur keamanan Windows Defender. Serangan berlanjut hingga 20 Juni 2024 pukul 00:55 WIB, di mana fitur keamanan tersebut berhasil dinonaktifkan sepenuhnya. (Nurani 2024) Serangan siber terhadap Pusat Data Nasional Sementara (PDNS 2) mengejutkan Indonesia karena berhasil meretas salah satu infrastruktur utama dalam pelaksanaan Sistem Pemerintahan Berbasis Elektronik (SPBE), Insiden ini menyebabkan terganggunya berbagai layanan publik strategis. Dua sektor yang paling terdampak adalah pelayanan imigrasi di Bandara Internasional Soekarno-Hatta serta 47 jenis layanan di bawah Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, mencakup sistem pengadaan elektronik (SPSE), program beasiswa, KIP Kuliah, hingga proses perizinan perfilman.

Serangan siber terhadap Pusat Data Nasional Sementara 2 (PDNS 2) menimbulkan kekhawatiran di kalangan masyarakat mengenai keamanan data pribadi mereka. Seperti yang telah dibahas sebelumnya, masyarakat cenderung sensitif terhadap pelaksanaan e-government, yang berkaitan erat dengan penggunaan data pribadi. Kejadian ini membuat masyarakat semakin waspada dan meragukan kemampuan pemerintah dalam melindungi data pribadi mereka. Harapan masyarakat akan perlindungan data pribadi mereka adalah wujud dari amanat konstitusi. Dari perspektif filosofis-konstitusional, amanat Pembukaan UUD 1945 Alinea IV secara tegas mewajibkan negara untuk memberikan perlindungan menyeluruh terhadap bangsa dan wilayah Indonesia. Dalam konteks kekinian, kewajiban konstitusional ini harus dimaknai termasuk perlindungan atas data pribadi warga negara sebagai bagian dari hak dasar dalam era digital. Secara yuridis, negara wajib melindungi diri pribadi setiap individu masyarakat, sebagaimana diamanatkan oleh Pasal 28G ayat (1) UUD NRI Tahun 1945.

Selain itu, dalam konteks operasional Pusat Data Nasional, yang bertugas memproses data pribadi pemerintah, Kementerian Komunikasi dan Digital sebagai pengendali data pribadi memiliki kewajiban untuk melindungi dan memastikan keamanan data tersebut sesuai dengan Undang-Undang Perlindungan Data Pribadi. Terkait dengan serangan siber yang menyebabkan lumpuhnya Pusat Data Nasional, pemerintah memiliki tanggung jawab untuk menangani situasi ini. Pertanggungjawaban pemerintah sangat penting, namun saat ini belum jelas bentuk pertanggungjawaban apa yang dapat diberikan oleh pemerintah.

Maka dari itu berdasarkan latar belakang yang telah dipaparkan, tulisan ini akan membahas dan menganalisis mengenai bentuk pertanggungjawaban pemerintah dalam kasus lumpuhnya pusat data nasional menurut Hukum Administrasi Negara.

## **2. KAJIAN TEORITIS**

Dalam penelitian ini penulis menggunakan teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon. Philipus M. Hadjon mengemukakan bahwa “perlindungan hukum adalah perlindungan akan harkat dan martabat, serta pengakuan terhadap hak-hak asasi manusia yang dimiliki oleh subyek hukum berdasarkan ketentuan hukum dari kesewenangan atau sebagai kumpulan peraturan atau kaidah yang akan dapat melindungi suatu hal dari hal lainnya” (Hadjon 1987). Jika dikontekstualkan dengan keberadaan data pribadi, maka hukum ada untuk melindungi data pribadi setiap individu yang mana hal tersebut merupakan hak asasi manusia bagi setiap individu, sehingga hukum dapat memberikan perlindungan terhadap hak-hak individu dari sesuatu yang dapat mengakibatkan hak-hak tersebut tidak dapat terpenuhi.

## **3. METODE PENELITIAN**

Penelitian ini menerapkan metode penelitian hukum normatif atau doktrinal. Menurut Terry Hutchinson, yang mengutip Peter Mahmud Marzuki, tujuan dari metode ini adalah untuk mengidentifikasi asas hukum, regulasi, atau doktrin yang dapat menjadi solusi untuk masalah hukum tertentu (Marzuki 2011). Sifat penelitian yang digunakan dalam penulisan hukum ini adalah penulisan hukum yang bersifat Preskriptif. Penelitian hukum normatif bersifat preskriptif yang artinya objek ilmu hukum merupakan koherensi antara norma hukum dan prinsip hukum, antara hukum dan norma hukum, serta antara tingkah laku individu dengan norma hukum (Marzuki 2021). Dalam penelitian ini, dalam memecahkan masalah hukum yang ada digunakan pendekatan perundang-undangan (*statute approach*). Pendekatan perundang-undangan (*statute approach*) dilakukan dengan menelaah berbagai macam peraturan perundang-undangan yang berkaitan dengan isu hukum yang diteliti (Marzuki 2021).

## **4. HASIL DAN PEMBAHASAN**

### **Kronologi Lumpuhnya Pusat Data Nasional**

Pengoperasian Pusat Data Nasional memiliki dasar hukum dalam Perpres No. 95 Tahun 2018 mengenai Sistem Pemerintahan Berbasis Elektronik, sekaligus berperan sebagai infrastruktur pendukung implementasi kebijakan Satu Data Indonesia yang diamanatkan

Perpres No. 39 Tahun 2019. Kementerian Komunikasi dan Digital (sebelumnya Kominfo) bertindak sebagai pengelola fasilitas ini, yang berfungsi sebagai wadah penyimpanan sistem elektronik beserta seluruh komponen pendukungnya untuk keperluan penyimpanan, pengolahan, hingga *recovery* data. Fungsi utamanya adalah memfasilitasi integrasi pengelolaan data antara pemerintah pusat dan daerah. Saat ini pelaksanaan Pusat Data Nasional belum berjalan secara maksimal dikarenakan fasilitas Pusat Data Nasional masih dilakukan pembangunan, sehingga perannya saat ini difasilitasi oleh Pusat Data Nasional Sementara yang terletak di Jakarta dan Surabaya.

Dalam pelaksanaan Pusat Data Sementara, tepatnya Pusat Data Sementara Surabaya terjadi insiden penyerangan siber. Insiden ini pertama kali terjadi pada tanggal 17 Juni 2024 pukul 23.15 WIB. Serangan ini dilakukan dengan percobaan untuk menonaktifkan fitur keamanan Windows Defender oleh *ransomware*. Aktivitas berbahaya terdeteksi pada 20 Juni 2024 pukul 00:54 WIB, yang mencakup pengizinan pemasangan file berbahaya, penghapusan file penting, dan penghentian layanan yang sedang berjalan. File-file terkait penyimpanan seperti VSS, Hyper V Volume, VirtualDisk, dan Veam vPower NFS mulai dinonaktifkan dan tidak dapat berfungsi. Selanjutnya, pada pukul 00:55 WIB, Windows Defender berhasil dilumpuhkan sepenuhnya (Nurani 2024).

Serangan siber terhadap PDNS Surabaya dilakukan oleh ransomware BrainCipher, yang menyebabkan pemasangan file berbahaya serta penghapusan file penting. Serangan ini juga mengakibatkan data yang ada terenkripsi dan tersandera (Mono and Lewiandy 2024). Serangan siber ini mengakibatkan layanan pada imigrasi di Bandara Internasional Soekarno-Hatta pada hari Kamis, 20 Juni 2024 terganggu (Nurani, 2024). Serangan siber ini mengakibatkan gangguan operasional di 282 instansi pemerintah. Berdasarkan keterangan PT Telkom sebagai operator PDNS Surabaya, sebagian besar data yang terkena dampak tidak memungkinkan untuk di-*recovery*, kecuali bagi 44 instansi yang telah menyiapkan sistem *backup* data sebelumnya (Makdori 2024).

### **Pengertian Pertanggungjawaban Pemerintah Menurut Hukum Administrasi Negara**

Konsep pertanggungjawaban secara mendasar mengandung pengertian tentang kewajiban hukum untuk menanggung akibat dari suatu tindakan, yang dapat berupa tuntutan, pembuktian kesalahan, atau penyelesaian perkara (Ridwan 2011). Dalam literatur hukum, pertanggungjawaban dapat diklasifikasikan menjadi dua jenis berdasarkan istilah teknisnya, yakni *liability* (the state of being liable) sebagai tanggung jawab hukum, dan *responsibility* (the state or fact being responsible) sebagai tanggung jawab moral atau fungsional (Ridwan 2011).

Dalam pengertian dan penggunaan praktis, istilah *liability* merujuk pada tanggung jawab hukum, yaitu kewajiban untuk bertanggung jawab (tanggung gugat) atas kesalahan yang dilakukan oleh subjek hukum, sedangkan istilah *responsibility* mengacu pada tanggung jawab politik (Ridwan 2011). Secara komparatif, sistem hukum Belanda mengenal dikotomi istilah *aansprakelijk* (pertanggungjawaban hukum semata) dan *verantwoordelijk* (pertanggungjawaban yang mencakup aspek hukum sekaligus politik dalam penyelenggaraan pemerintahan) (Ridwan 2011).

Dalam teori hukum, *rechtsverkeer* merujuk pada pergaulan hukum yang terdiri dari *rechtshandeling* sebagai perbuatan hukum dan *rechtsbetrekking* sebagai relasi hukum. Seluruh aspek ini memiliki dasar hukum yang jelas sehingga memungkinkan terciptanya hubungan timbal balik berupa hak dan kewajiban antara para pihak yang terlibat (Ridwan 2011). Pemerintah, sebagai subjek hukum yang berfungsi mendukung hak dan kewajiban hukum dengan posisinya sebagai wakil badan hukum dan jabatan pemerintahan, dapat melakukan tindakan hukum. Tindakan hukum tersebut adalah tindakan yang berkaitan dengan hukum atau yang dapat menghasilkan akibat hukum, baik yang bersifat positif maupun negatif (Ridwan 2011). Dalam konteks pertanggungjawaban pemerintah, akibat hukum negatif memiliki relevansi yang signifikan, karena dapat memicu tuntutan dari pihak-pihak yang terkena dampak akibat hukum tersebut. Akibat hukum negatif dapat terjadi akibat adanya pelanggaran hukum, pengabaian kewajiban hukum yang seharusnya dijalankan, atau melakukan larangan hukum yang seharusnya ditinggal yang dilakukan oleh pemerintah, contoh akibat hukum negatif adalah kerugian yang menimpa seseorang atau pelanggaran hak-hak warga negara (Ridwan 2011).

Pertanggungjawaban pemerintah dalam ranah hukum administrasi negara bertumpu pada konsep perbuatan melanggar hukum yang dilakukan oleh penguasa (*onrechmatige overheidsdaad* atau *unlawful acts of the government*). Hal ini terjadi ketika tindakan atau kebijakan pemerintah, terutama yang berupa Keputusan Tata Usaha Negara (KTUN), diambil dengan cara yang melanggar atau tidak sesuai dengan ketentuan peraturan perundang-undangan yang berlaku dan/atau bertentangan dengan asas-asas umum pemerintahan yang baik (AUPB) (Safi 2010). Dengan kata lain, pemerintah dapat dimintai pertanggungjawaban secara hukum jika keputusan atau tindakan yang diambil tidak memenuhi standar legalitas dan prinsip-prinsip pemerintahan yang baik, seperti keadilan, kepastian hukum, dan keseimbangan. Konsep ini menegaskan bahwa setiap penyimpangan dari norma hukum dan prinsip dasar pemerintahan yang baik dapat menjadi dasar untuk mengajukan tuntutan hukum terhadap pemerintah, baik dalam konteks perdata maupun administrasi. Keberadaan

pertanggungjawaban pemerintah ini merupakan suatu keharusan dalam negara yang menganut konsep negara hukum seperti Indonesia (Safi 2010).

Untuk dapat mengetahui kepada siapa pertanggungjawaban pemerintah dapat dibebankan maka perlu diketahui terlebih dahulu kepada siapa kewenangan tersebut diberikan. Pemerintah dalam menjalankan perannya dapat melakukan dua bentuk perbuatan hukum, yakni perbuatan hukum publik dan perbuatan hukum perdata. Dalam konteks penyelenggaraan kenegaraan dan pemerintahan yang merupakan dimensi perbuatan hukum publik, maka pertanggungjawaban dalam menyelenggarakan kenegaraan dan pemerintahan melekat pada jabatan yang secara yuridis dilekati dengan kewenangan.

Dengan diberikannya sebuah kewenangan maka secara langsung terkandung juga beban pertanggungjawaban. Namun, pada praktiknya tidak semua kewenangan yang dijalankan oleh pejabat pemerintah tanggung jawabnya juga dipikul oleh pejabat tersebut. Hal ini dikarenakan bagaimana cara kewenangan tersebut diberikan dan dijalankan. Badan atau pejabat tata usaha negara yang memperoleh kewenangan untuk melakukan suatu tindakan hukum tertentu yang kewenangan itu diperoleh secara atribusi dan delegasi, maka badan atau pejabat tersebutlah yang secara otomatis memikul pertanggungjawaban hukumnya. Sedangkan, untuk badan atau pejabat tata usaha negara yang menerima kewenangan atas dasar mandat tidak berhak untuk memikul tanggung jawab hukumnya, sebab yang berhak untuk memikul tanggung jawab hukum tersebut ialah pemberi mandat (mandans) (Ridwan 2011).

Pejabat adalah perwakilan yang mewakili tindakan dari jabatan. Definisi jabatan itu sendiri merujuk pada suatu lembaga dengan ruang lingkup pekerjaan tertentu yang dibentuk untuk jangka waktu yang lama, di mana diberikan tugas dan wewenang untuk melakukan tindakan hukum (Ridwan 2011). Namun, pada dasarnya jabatan atau organ ini adalah sebuah fiksi yang tidak dapat melakukan perbuatan hukum secara mandiri, sehingga dalam melakukan tindakannya, jabatan diwakili oleh pejabat (Ridwan 2011). Berdasarkan uraian tersebut, definisi pejabat dalam konteks hukum administrasi negara adalah individu yang menjalankan kewenangan secara derivatif dari suatu jabatan, sehingga setiap perbuatan hukum yang dilakukan merupakan perwujudan dari kewenangan jabatan tersebut.

Dalam menganalisis pertanggungjawaban pejabat negara menurut hukum administrasi, Kranenburg dan Vegting mengembangkan dua konsep kunci: (1) teori *fautes personnelles* yang menempatkan tanggung jawab individu pada pejabat pelaku, dan (2) teori *fautes de service* yang membebaskan tanggung jawab kepada institusi tempat pejabat tersebut bekerja (Ridwan 2011). Teori pertama menegaskan bahwa pertanggungjawaban bersifat personal dan melekat pada pejabat sebagai individu. Sebaliknya, teori kedua memandang tanggung jawab sebagai

beban institusional yang melekat pada jabatan. Dalam konteks hukum, subjek hukum sejati adalah jabatan sebagai entitas yang diwakili, sementara pejabat hanyalah pelaksana yang bertindak atas nama jabatan tersebut. Dengan demikian, secara prinsipil tanggung jawab akhirnya berada pada jabatan. Berdasarkan penjelasan di atas, sudah menjadi terang bahwasanya tanggung jawab terhadap tindakan pemerintah/pejabat akan ditanggung oleh jabatan.

Meski telah jelas pembagian tanggung jawabnya, timbul keraguan apakah pejabat sepenuhnya bebas dari pertanggungjawaban pribadi. Menjawab kekhawatiran ini, Kranenburg dan Vegting merumuskan kriteria pembeda: tanggung jawab dibebankan kepada jabatan untuk pelanggaran hukum yang bersifat objektif, sementara pejabat secara pribadi baru bertanggung jawab jika terdapat unsur kesalahan subjektif (mal administrasi) (Ridwan 2011). Kesalahan subjektif yang dimaksud oleh Kranenburg dan Vegting berkaitan dengan mal administrasi. Secara sederhana, dapat disimpulkan bahwa pertanggungjawaban atas tindakan pemerintah atau jabatan akan ditanggung oleh jabatan, selama kesalahan atau kerugian yang muncul akibat tindakan hukum tersebut bersifat objektif. Sementara itu, seorang pejabat hanya dapat dimintai pertanggungjawaban jika ia melakukan kesalahan atau menyebabkan kerugian yang disebabkan oleh tindakan hukum yang bersifat subjektif, yaitu mal administrasi.

### **Bentuk Pertanggungjawaban Pemerintah Terhadap Lumpuhnya Pusat Data Nasional**

Seperti yang telah dijelaskan sebelumnya, pemerintah saat ini berfungsi sebagai perwakilan badan hukum sekaligus perwakilan jabatan. Dalam konteks penyelenggaraan kenegaraan dan pemerintahan, yang termasuk dalam dimensi perbuatan hukum publik, pertanggungjawaban tersebut melekat pada jabatan yang secara yuridis diberikan kewenangan tertentu. Dari sudut pandang hukum publik, kewenangan yang dimiliki oleh pemerintah atau pejabat publik menciptakan kewajiban untuk mempertanggungjawabkan tindakan mereka. Oleh karena itu, dalam peristiwa lumpuhnya pusat data nasional, pemerintah sebagai pemegang kewenangan dapat dikenakan beban pertanggungjawaban. Beban pertanggungjawaban ini dapat diberikan kepada pemerintah karena dalam mengoperasikan pusat data nasional, mereka telah melakukan tindakan hukum yang berdampak negatif dan bertentangan dengan asas-asas umum pemerintahan yang baik.

Dalam Undang-Undang Perlindungan Data Pribadi, pemerintah melalui Kementerian Komunikasi dan Digital sebagai Pengendali Data Pribadi dapat dikenakan tanggung jawab berupa pemberitahuan publik mengenai kegagalan dalam melindungi data pribadi. Ketentuan ini diatur dalam Pasal 46 ayat (3) UU PDP yang menyatakan, "Dalam hal tertentu, Pengendali

Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Pelindungan Data Pribadi." Penjelasan Pasal 46 ayat (3) menyebutkan bahwa "dalam hal tertentu" mencakup situasi di mana kegagalan perlindungan data pribadi mengganggu pelayanan publik dan/atau berdampak serius terhadap kepentingan masyarakat. Hal ini relevan dengan peristiwa lumpuhnya pusat data nasional yang mengakibatkan gangguan pada pelayanan publik. Di samping itu, UU PDP Pasal 57 ayat (1)-(3) mengatur empat jenis sanksi administratif yang dapat dikenakan kepada pemerintah, yaitu: pertama, teguran tertulis; kedua, pembekuan sementara proses pengolahan data; ketiga, penghapusan atau pemusnahan data pribadi; serta keempat, denda administratif. Khusus untuk denda, ayat (3) menetapkan batas maksimal sebesar 2% dari total pendapatan tahunan entitas pelanggar, dengan pengertian pendapatan sebagai seluruh penerimaan bruto dari kegiatan operasional yang menambah ekuitas, tidak termasuk modal penyertaan. Namun, terkait pengenaan sanksi administratif ini belum dapat dijalankan sebab lembaga yang berwenang untuk memberikan sanksi belum dibentuk oleh Presiden Republik Indonesia.

Di samping itu, mekanisme pertanggungjawaban pemerintah juga dapat ditempuh melalui jalur peradilan administrasi. Ketentuan ini sejalan dengan Peraturan Mahkamah Agung Nomor 2 Tahun 2019 yang menegaskan bahwa pemerintah wajib mempertanggungjawabkan tindakan melawan hukum, baik karena bertentangan dengan ketentuan peraturan perundang-undangan maupun asas-asas pemerintahan yang baik (AUPB). Menurut penulis, dalam peristiwa lumpuhnya pusat data nasional, kedua alasan tersebut telah terpenuhi.

## **KESIMPULAN DAN SARAN**

Berdasarkan pemaparan yang telah disampaikan di atas dapat disimpulkan bahwa Pemerintah dalam melakukan perbuatan hukum publik, yakni berupa pelayanan publik maka apabila terjadi kerugian yang menimpa masyarakat dan kerugian tersebut diakibatkan tindakan Pemerintah itu sendiri maka Pemerintah dapat dimintakan pertanggungjawaban. Untuk dapat mengetahui lebih rinci kepada siapa pertanggungjawaban harus diberikan maka harus diperjelas terlebih dahulu siapa pejabat yang mengemban jabatan tersebut, dengan cara apa jabatan tersebut diperoleh, dan kesalahan apa yang diperbuat apakah kesalahan objektif atau subjektif yang berkaitan dengan mal administrasi. Dalam konteks lumpuhnya Pusat Data Nasional sebenarnya sudah jelas bentuk pertanggungjawaban apa yang harus diberikan oleh pemerintah. Hal ini diatur dalam Pasal 47 ayat (3) berkaitan dengan kewajiban pengumuman kegagalan perlindungan data pribadi dan pasal 53 ayat (1) sampai ayat (3) yang menjelaskan sanksi administratif, termasuk di dalamnya adalah denda administratif. Namun, terkait sanksi

belum dapat diberikan dikarenakan belum adanya lembaga yang berwenang memberikan sanksi tersebut. Selain itu, Pemerintah juga dapat dimintakan pertanggungjawaban melalui mekanisme peradilan administrasi negara melalui Pengadilan Tata Usaha Negara.

Saran yang dapat diberikan kepada pemerintah adalah untuk segera membentuk lembaga independen sebagaimana amanat UU PDP agar apabila kejadian seperti ini terulang kembali maka sanksi sebagaimana diatur dalam UU PDP dapat dijatuhkan. Kemudian, untuk penelitian selanjutnya disarankan untuk menggali lebih dalam dengan mengacu pada laporan atau dokumen negara resmi yang berkaitan dengan hal ini.

## DAFTAR REFERENSI

- Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–142. <https://doi.org/10.38043/jah.v6i1.4484>
- 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*. Surabaya: Bina Ilmu.
- Indrajit, R. E., Zinuddin, A., & Rudianto, D. (2005). *E-government in action (Ragam kasus implementasi sukses di berbagai belahan dunia)*. Yogyakarta: Andi.
- Iswandari, B. A. (2022). Jaminan keamanan data pribadi warga negara dalam penyelenggaraan urusan pemerintahan berbasis elektronik (e-government). *Dharmasiswa: Jurnal Program Magister Hukum FHUI*, 2(1), 75–86.
- Kershner, M. (2021, July 15). Data isn't the new oil—Time is. *Forbes*. Retrieved from <https://www.forbes.com/councils/theyec/2021/07/15/data-isnt-the-new-oil--time-is/>
- Laoly, Y. H. (2019). *Birokrasi digital*. Jakarta: Pustaka Alvabet.
- Makdori, Y. (2024, February 18). Dari 282 instansi yang terdampak peretasan PDNS, hanya 44 yang punya backup. *Asumsi.co*. Retrieved from <https://asumsi.co/post/93028/dari-282-instansi-yang-terdampak-peretasan-pdns-hanya-44-yang-punya-back-up/>
- Marzuki, P. M. (2011). *Penelitian hukum*. Jakarta: Kencana Prenada Media Group.
- Marzuki, P. M. (2021). *Penelitian hukum*. Jakarta: Kencana Prenada Media.
- Mono, J. R., & Lewiandy. (2024). Perlindungan hukum terhadap hak privasi subjek data pribadi dalam insiden serangan siber Pusat Data Nasional Sementara. *JIHHP: Jurnal Ilmu Hukum, Humaniora, dan Politik*, 5(1), 467–477.
- Nurani, S. K. (2024). Kronologi Pusat Data Nasional jebol hingga desakan Menkominfo Budi Arie mundur dari jabatannya. *Tempo.co*. Retrieved from <https://www.tempo.co/politik/kronologi-pusat-data-nasional-jebol-hingga-desakan-menkominfo-budi-arie-mundur-dari-jabatannya-44552>

- Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.
- Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
- Purwanto, E. A. (2018). Smart city as an upshot of bureaucratic reform in Indonesia. *International Journal of Electronic Government Research (IJEGR)*, 14(3), 32–43.
- Ridwan. (2011). *Hukum administrasi negara (7th ed.)*. Rajawali: Rajawali Pers.
- Roziqin, A., Kismartini, Fajrina, A. N., Salahudin, & Sulistyaningsih, T. (2022). The development of Indonesian e-government: A bibliometric analysis. *COLLNET Journal of Scientometrics and Information Management*, 16(1), 49–74. <https://doi.org/10.1080/09737766.2021.2007036>
- Safi. (2010). Konsep pertanggungjawaban perbuatan pemerintahan sebagai sarana mewujudkan good governance di Indonesia. *Pamator Journal*, 3(2), 172–178.
- Setiawan, A. B. (2013). Kajian kesiapan keamanan informasi instansi pemerintah dalam penerapan e-government. *Jurnal Masyarakat Telematika dan Informasi*, 4(2), 110.
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.