VISA: Journal of Visions and Ideas
Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

Kelemahan Pertanggungjawaban Negara dalam Kasus Gangguan Pusat Data Nasional Tahun 2024 di Indonesia

Haidar Reynard Akbar[1], Adhining Prabawati Rahmahani[2]
[1,2]Universitas Esa Unggul
haidarnax.94@student.esaunggul.ac.id[1], adhining.pr@esaunggul.ac.id[2]

ABSTRACT

The 2024 National Data Center (Pusat Data Nasional/PDN) disruption caused significant interruptions to digital public services and raised concerns regarding the protection of personal data in Indonesia. This study aims to analyze the legal framework governing state responsibility in personal data protection and electronic systems, as well as to examine the weaknesses of state responsibility in the 2024 National Data Center disruption case. This research employs a normative legal research method using statutory and conceptual approaches. The study relies on primary, secondary, and tertiary legal materials collected through library research and analyzed qualitatively. The findings indicate that Indonesia has established an adequate legal framework for personal data protection and electronic system governance. However, weaknesses remain in cybersecurity implementation, information security governance, risk mitigation, and accountability mechanisms. From an ethical hacker perspective, strengthening national cybersecurity requires the implementation of security by design, defense in depth, and continuous security testing.

Keywords: *state responsibility, national data center, personal data protection, cybersecurity, ethical hacker*

ABSTRAK

Gangguan Pusat Data Nasional (PDN) Tahun 2024 mengakibatkan terganggunya berbagai layanan publik berbasis digital dan menimbulkan kekhawatiran mengenai perlindungan data pribadi masyarakat. Penelitian ini bertujuan untuk menganalisis pengaturan hukum mengenai pertanggungjawaban negara dalam perlindungan data pribadi dan sistem elektronik di Indonesia serta mengkaji kelemahan pertanggungjawaban negara dalam kasus Gangguan Pusat Data Nasional Tahun 2024. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier yang diperoleh melalui studi kepustakaan dan dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa Indonesia telah memiliki dasar hukum yang cukup memadai dalam perlindungan data pribadi dan penyelenggaraan sistem elektronik. Namun, masih terdapat kelemahan pada aspek implementasi keamanan siber, tata kelola keamanan informasi, mitigasi risiko, dan akuntabilitas penyelenggara sistem elektronik. Dari perspektif ethical hacker, diperlukan penerapan security by design, defense in depth, serta pengujian keamanan secara berkelanjutan guna memperkuat ketahanan siber nasional.

Kata Kunci: pertanggungjawaban negara, pusat data nasional, perlindungan data pribadi, keamanan siber, ethical hacker

PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi (TIK) telah secara fundamental mentransformasi berbagai aspek kehidupan sosial, termasuk pula

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

dalam ranah operasional pemerintahan. Merespons dinamika ini, Pemerintah Indonesia secara proaktif menginisiasi transisi menuju paradigma pemerintahan digital, yang diwujudkan melalui kerangka Sistem Pemerintahan Berbasis Elektronik (SPBE). Objektif utama dari upaya ini adalah untuk menjamin penyediaan layanan publik yang lebih efisien, akurat, dan bermutu tinggi bagi masyarakat umum.

Pusat Data Nasional (PDN) diidentifikasi sebagai prasyarat fundamental dalam mendukung akselerasi transformasi digital. Institusi ini berfungsi sebagai inti operasional sistem digital pemerintahan, di mana seluruh aset data krusial negara diakomodasi, dikelola, dan dikonsolidasikan dalam suatu repositori terpusat. Kehadiran PDN diantisipasi dapat memperkuat jaminan keamanan, kontinuitas ketersediaan, serta integritas data dalam fasilitasi layanan publik berbasis elektronik. (Siti Yuniarti, 2023).

Akselerasi perkembangan teknologi digital yang pesat telah turut menciptakan kompleksitas ancaman keamanan siber yang kian signifikan. Insiden keamanan siber dapat berimplikasi pada disrupsi layanan publik, hilangnya data-data esensial, serta kebocoran informasi konfidensial. Esensi keamanan siber, oleh karena itu, melampaui sekadar dimensi teknis. Aspek ini turut berkaitan dengan tanggung jawab negara dalam melindungi hak-hak fundamental masyarakat, khususnya terkait privasi informasi dan data personal. Proteksi data pribadi merupakan bagian integral dari hak privasi yang wajib dijamin oleh negara, baik melalui kerangka regulasi yang kokoh maupun implementasi infrastruktur keamanan digital yang adaptif dan komprehensif (Niffari, 2020).

Pada Juni 2024, Indonesia mengalami gangguan substansial pada Pusat Data Nasional. Insiden ini berimplikasi pada terhentinya operasional sejumlah layanan publik di berbagai institusi pemerintahan. Peristiwa tersebut menyoroti bahwa resiliensi infrastruktur digital pemerintah masih dihadapkan pada tantangan signifikan, khususnya dalam domain keamanan siber dan proteksi data publik (Kriswandaru et al., 2024). Peristiwa ini diduga disebabkan oleh serangan siber berupa ransomware yang menargetkan infrastruktur penyimpanan data krusial milik negara. Dampak dari insiden tersebut mencakup disrupsi operasional pada sejumlah layanan administrasi publik, menimbulkan kerugian substansial bagi masyarakat, serta memunculkan kekhawatiran serius perihal integritas dan kerahasiaan data yang dipegang oleh sistem pemerintah (Putri et al., 2025)

Berdasarkan prinsip-prinsip negara hukum, Indonesia memiliki mandat untuk memastikan perlindungan terhadap hak-hak dasar warga negara, mencakup hak atas kerahasiaan pribadi dan keamanan informasi perseorangan. Prinsip tersebut sejalan dengan Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa Indonesia adalah negara hukum. Selain itu, Pasal 28G ayat (1) UUD NRI Tahun 1945 memberikan jaminan kepada setiap orang atas perlindungan diri pribadi, kehormatan, martabat, dan rasa aman. Dalam konteks perlindungan data pribadi, negara juga telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai landasan hukum dalam menjamin keamanan dan kerahasiaan data masyarakat.

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

Meskipun demikian, kendati Indonesia telah memiliki kerangka regulasi yang komprehensif untuk mengatur proteksi data pribadi dan keamanan sistem informasi dan elektronik, insiden siber serius yang menimpa Pusat Data Nasional pada tahun 2024 mengindikasikan bahwa realisasi akuntabilitas negara dalam menjamin keamanan infrastruktur digital nasional masih dihadapkan pada sejumlah tantangan substansial.

Dalam konteks keamanan siber, efektivitas perlindungan data tidak semata-mata bergantung pada adanya kerangka regulasi. Sebaliknya, hal tersebut juga ditentukan oleh implementasi strategi manajemen risiko yang solid, pengelolaan proaktif kerentanan sistem, kapasitas respons insiden yang memadai, serta pengawasan keamanan yang berkelanjutan. Para pakar keamanan siber, khususnya yang bergerak di bidang pengujian penetrasi (*ethical hacking*), mengemukakan bahwa postur keamanan suatu sistem memerlukan pengujian dan evaluasi periodik guna mencegah eksploitasi terhadap celah keamanan yang berpotensi menimbulkan kerugian bagi publik. Literatur ilmiah yang ada secara umum mengkaji proteksi data personal, keamanan digital, serta akuntabilitas operator sistem elektronik. Penelitian (Niffari, 2020) berfokus pada tantangan perlindungan data pribadi di Indonesia, sedangkan penelitian (Putri et al., 2025) membahas tanggung jawab prosesor data dalam kasus gangguan Pusat Data Nasional. Namun demikian, Kajian yang secara spesifik menyoroti kelemahan akuntabilitas negara dalam kasus disrupsi Pusat Data Nasional yang terjadi pada tahun 2024, melalui integrasi perspektif yurisprudensi dan keamanan siber, masih relatif langka. Oleh karena itu, investigasi ini menjadi krusial untuk menganalisis format pertanggungjawaban entitas negara serta mengidentifikasi defisiensi yang masih melekat pada implementasinya.

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan metodologi hukum normatif. Menurut Soekanto dan Mamudji, metode penelitian hukum normatif didefinisikan sebagai suatu studi yang menitikberatkan pada penelusuran dan analisis bahan kepustakaan atau data sekunder, yang meliputi kategori bahan hukum primer, bahan hukum sekunder, serta bahan hukum tersier (Soerjono Soekanto; Sri Mamudji, 2015).

HASIL DAN PEMBAHASAN

Pengaturan Hukum Pertanggungjawaban Negara Dalam Perlindungan Data Pribadi dan Sistem Elektronik di Indonesia

Perlindungan data personal merupakan suatu dimensi integral dari hak asasi manusia yang harus dijamin oleh negara sebagai entitas hukum. Dalam kerangka paradigma negara hukum, otoritas negara tidak hanya memiliki wewenang untuk menetapkan tatanan perundang-undangan, melainkan juga mengemban obligasi fundamental untuk memberikan jaminan proteksi terhadap hak-hak konstitusional setiap subjek hukum. Berdasarkan konsepsi Jimly Asshiddiqie, salah satu atribut esensial dari negara hukum adalah adanya kepastian perlindungan terhadap hak-hak dasar individu, yang termanifestasi melalui pelaksanaan tata kelola pemerintahan

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

yang berlandaskan pada kaidah hukum serta asas pertanggungjawaban (Asshiddiqie, 2011).

Secara konstitusional, perlindungan terhadap privasi dan data pribadi dapat ditelusuri dari Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang memberikan hak kepada setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan rasa aman. Ketetapan ini menjadi landasan bagi negara untuk menjamin perlindungan data pribadi masyarakat dalam operasionalisasi sistem elektronik. Dinamika teknologi informasi yang berkelanjutan mensyaratkan pemerintah untuk meningkatkan kapab ilitas pengamanan terhadap informasi dan infrastruktur elektronik yang dimanfaatkan dalam pelayanan publik. Hal ini krusial guna mengantisipasi spektrum risiko keamanan siber yang kian beragam (Dewi et al., 2016).

Pengaturan lebih lanjut mengenai perlindungan data pribadi diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini mengatur hak subjek data pribadi, kewajiban pengendali data, serta tanggung jawab pihak yang melakukan pemrosesan data pribadi. Pemberlakuan Undang Undang Perlindungan Data Pribadi (UU PDP) mengindikasik an bahwa Indonesia telah membentuk kerangka regulasi yang memadai guna menjamin proteksi data personal setiap individu (Niffari, 2020).

Selain UU PDP, tanggung jawab negara dalam penyelenggaraan sistem elektronik juga diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. Regulasi tersebut mewajibkan penyelenggara sistem elektronik untuk menyediakan sistem yang andal, aman, dan bertanggung jawab. Dalam ranah penyediaan layanan publik digital, merupakan keharusan bagi pemerintah untuk menjamin bahwa sistem yang diimplementasikan memiliki kapabilitas untuk memberikan perlindungan yang robust terhadap data masyarakat dari spektrum ancaman siber yang bervariasi.

Berdasarkan perspektif Satjipto Rahardjo, proteksi hukum didefinisikan sebagai suatu mekanisme yang berorientasi pada upaya menjamin perlindungan dan fasilitasi hak-hak fundamental serta kepentingan esensial masyarakat, guna memastikan aktualisasi hak hak tersebut secara paripurna (Satjipto Rahardjo, 2006). Oleh karena itu, tanggung jawab negara tidak hanya termanifestasi melalui penetapan regulasi, namun juga melalui pelaksanaan perlindungan yang efektif bagi masyarakat ketika terjadi anomali pada infrastruktur digital yang digunakan dalam penyediaan layanan publik.

Oleh karena itu, dapat disimpulkan bahwa Indonesia telah memiliki kerangka regulasi yang komprehensif dalam mengelola proteksi data personal serta integritas sistem elektronik. Implikasinya, persoalan fundamental dalam insiden Pusat Data Nasional pada tahun 2024 tidak disebabkan oleh ketiadaan norma hukum, melainkan pada implementasi akuntabilitas negara dalam menjamin keamanan infrastruktur elektronik yang difungsikan untuk pelayanan umum.

VISA: Journal of Visions and Ideas
Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

Kelemahan Pertanggungjawaban Negara Dalam Kasus Gangguan Pusat Data Nasional Tahun 2024

Disrupsi pada Pusat Data Nasional Sementara (PDNS) Indonesia pada tahun 2024 merupakan salah satu insiden keamanan siber paling signifikan yang pernah tercatat di negara tersebut. Serangan *ransomware* yang menargetkan infrastruktur digital pemerintahan telah mengakibatkan terhambatnya berbagai layanan publik esensial yang bergantung pada sistem elektronik. Peristiwa tersebut menyoroti bahwa keberadaan kerangka regulasi belum secara otomatis menjamin implementasi perlindungan yang efektif terhadap data dan layanan publik yang terdigitalisasi.

Secara yuridis, negara mengemban amanat untuk menjamin hak-hak konstitusional warga negara melalui tata kelola pemerintahan yang efektif dan akuntabel. Kendati demikian, insiden operasional yang baru-baru ini terjadi mengindikasikan adanya defisiensi dalam pemenuhan obligasi tersebut.

Defisiensi primer teridentifikasi pada dimensi prevensi dan mitigasi risiko siber. Sebagai pengelola infrastruktur digital strategis nasional, negara semestinya mengimplementasikan mekanisme identifikasi kerentanan, asesmen keamanan seca ra berkala, serta kerangka perlindungan yang komprehensif guna mengantisipasi berbagai potensi ancaman digital.

Defisiensi kedua terletak pada aspek tata kelola keamanan informasi. Ross Anderson mengemukakan bahwa insiden keamanan sistem sering kali tidak semata-mata diakibatkan oleh faktor teknis, melainkan lebih disebabkan oleh inefisiensi dalam tata kelola keamanan dan manajemen risiko yang diimplementasikan oleh entitas (Ross Anderson, 2020). Dalam konteks insiden yang menimpa PDN pada tahun 2024, serangkaian gangguan yang terjadi mengindikasikan bahwa kerangka tata kelola keamanan informasi masih membutuhkan peningkatan yang signifikan, terutama pada aspek pemantauan berkelanjutan, manajemen risiko yang efektif, serta kesigapan dalam merespons insiden keamanan siber.

Dimensi problematik ketiga berkaitan erat dengan proteksi terhadap komunitas yang terimbas. Dalam kerangka teori perlindungan hukum, otoritas negara mengemban mandat untuk menjamin keamanan dan hak-hak warga ketika potensi kerugian mengancam. Namun, disrupsi pada sistem pelayanan publik justru menciptakan hambatan substantif bagi masyarakat dalam merealisasikan akses terhadap layanan yang merupakan hak fundamental mereka. Kondisi ini secara eksplisit menegaskan bahwa perlindungan hukum tidak hanya bergantung pada eksistensi formal regulasi, melainkan juga pada efektivitas aktualisasi serta penegakan kerangka legislatif tersebut.

Selain dimensi hukum, penelitian ini juga mengkaji kasus PDN dari sudut pandang peretas etis, sebuah pendekatan yang membedakannya dengan studi-studi terdahulu. Dalam ranah keamanan siber, peretas etis memiliki fungsi krusial dalam mengidentifikasi kerentanan sistem sebelum potensi eksploitasinya oleh pihak yang tidak berwenang. Stuttard dan Pinto berpendapat bahwa integritas sistem seharusnya dibangun melalui mekanisme pengujian yang berlanjut guna mendeteksi serta menanggulangi kelemahan sebelum dieksploitasi oleh entitas eksternal. (Stuttard & Pinto, 2011).

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

Dari perspektif seorang praktisi keamanan siber, insiden keamanan yang dialami oleh PDN mengindikasikan bahwa integritas sistem tidak dapat semata-mata dijamin melalui solusi teknologi. Sebagaimana diutarakan oleh Von Solms dan Van Niekerk, lingkup keamanan siber melampaui sekadar penggunaan teknologi, meliputi pula dimensi manusiawi, kerangka kebijakan, dan manajemen tata kelola organisasi. Oleh karena itu, efektivitas suatu arsitektur keamanan tidak hanya ditentukan oleh perangkat pengamanan yang diimplementasikan, melainkan juga oleh kapasitas institusional dalam memitigasi risiko dan menerapkan regulasi keamanan secara berkelanjutan (Solms & Niekerk, 2013).

Arsitektur informasi digital yang mengelola data strategis nasional esensial untuk mengadopsi prinsip *security by design*, yaitu mengintegrasikan aspek keamanan secara inheren ke dalam seluruh tahapan perancangan, pengembangan, dan operasionalisasi sistem sejak fase awal. Di samping itu, sistem tersebut juga wajib mengimplementasikan strategi *defense in depth* melalui penerapan mekanisme perlindungan berjenjang (*layered protection*). Tujuannya adalah untuk memitigasi risiko kegagalan tunggal, memastikan bahwa insiden atau kerentanan pada satu lapisan keamanan tidak secara langsung mengakibatkan kompromi atau disfungsi menyeluruh pada keseluruhan sistem.

Penelaahan ekstensif mengindikasikan bahwa salah satu defisiensi krusial dalam insiden yang menimpa PDN terletak pada urgensi implementasi strategi manajemen risiko keamanan informasi yang lebih holistik. Dari sudut pandang seorang profesional keamanan siber *(ethical hacker)*, pencapaian penetrasi ilegal seringkali mengindikasikan eksistensi celah keamanan yang belum terdeteksi atau belum tertangani secara efektif. Dengan demikian, evaluasi keamanan periodik, penilaian kerentanan, pengujian penetrasi, serta asesmen keamanan infrastruktur secara berkesinambungan merupakan komponen esensial dalam upaya mitigasi terulangnya insiden sejenis di kemudian hari.

Berdasarkan doktrin Negara Hukum dan prinsip Perlindungan Hukum, entitas negara memiliki kewajiban yang melampaui sekadar merumuskan kerangka regulasi ia juga bertanggung jawab untuk menjamin efektivitas proteksi terhadap infrastruktur digital dan sistem elektronik yang diakses oleh publik. Oleh karena itu, defisiensi akuntabilitas negara terkait insiden disrupsi Pusat Data Nasional yang terjadi pada tahun 2024 bukan terletak pada ketiadaan landasan normatif. Sebaliknya, kelemahan tersebut berakar pada aspek implementasi keamanan siber, optimalisasi tata kelola keamanan informasi, efektivitas pengelolaan risiko, serta penanganan komprehensif bagi warga negara yang terdampak.

Adapun kelemahan-kelemahan tersebut secara rinci dapat diuraikan dalam beberapa aspek berikut ini.

Kelemahan Dalam Pencegahan dan Mitigasi Ancaman Siber.

Dalam konteks pengelolaan keamanan siber, salah satu tanggung jawab fundamental bagi pihak yang mengelola sistem daring adalah mengantisipasi dan memitigasi beragam potensi ancaman yang dapat mengganggu keberlangsungan atau merusak integritas operasional sistem. Pendekatan ini mencakup pelaksanaan audit

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

keamanan secara berkala, deteksi kerentanan yang inheren dalam arsitektur sistem, evaluasi ketahanan melalui simulasi serangan siber *(penetration testing)*, serta menjamin kepatuhan berkelanjutan terhadap standar keamanan data dan regulasi terkait yang berlaku.

Dalam pandangan para *(ethical hacker)*, setiap sistem yang menyimpan data krusial atau bernilai tinggi secara inheren rentan terhadap kelemahan keamanan. Asumsi ini merupakan premis fundamental dalam metodologi mereka. Oleh karena itu, langkah-langkah keamanan yang kokoh tidak dapat semata-mata mengandalkan aplikasi canggih atau perangkat berteknologi tinggi, melainkan harus didukung oleh proses tinjauan dan evaluasi yang berkelanjutan.

Peristiwa gangguan sistem yang baru-baru ini menimpa Pusat Data Nasional (PDN) secara tegas menggarisbawahi urgensi untuk mengoptimalkan metodologi identifikasi dan penanganan risiko yang berlaku saat ini. Tujuan fundamentalnya adalah untuk memastikan deteksi ancaman siber dapat dilakukan secara proaktif, sehingga mampu mencegah eskalasi kerusakan yang lebih parah dan dampak yang menyebar secara sistemik.

Kelemahan Tata Kelola Keamanan Informasi

Terlepas dari dimensi teknologisnya, insiden yang dialami oleh Pusat Data Nasional (PDN) turut menggarisbawahi urgensi manajemen dan tata kelola keamanan data dalam konteks operasionalisasi sistem digital berskala nasional. Aspek-aspek ini mencakup perumusan kebijakan dan regulasi yang eksplisit, delineasi peran dan akuntabilitas yang transparan, implementasi mekanisme pemantauan dan pengawasan yang efektif, serta penetapan protokol respons insiden dan pemulihan pasca-kejadian yang konkret.

Regulasi pemerintah mengamanatkan bahwa penyediaan layanan kepada masyarakat harus dilaksanakan secara cermat dan akuntabel. Oleh karena itu, menjadi kewajiban pemerintah untuk menjamin bahwa seluruh sistem digital yang digunakan dalam penyelenggaraan layanan publik memiliki kapabilitas keamanan siber yang memadai. Dalam konteks ini, sesuai dengan Kerangka Keamanan Siber NIST 2.0, entitas diwajibkan mengimplementasikan fungsi-fungsi inti Identifikasi, Proteksi, Deteksi, Respons, dan Pemulihan *(Identify, Protect, Detect, Respond,* dan *Recover)* guna memperkuat resiliensi keamanan siber (Pascoe, 2024). Insiden yang terjadi pada PDN menjadi bukti bahwa pengelolaan keamanan informasi kita masih harus ditingkatkan, terutama pada bagian pengawasan dan penanganan risiko.

Kelemahan Dalam Perlindungan Masyarakat yang Terdampak

Apabila terjadi gangguan serius pada infrastruktur pusat data nasional, dampaknya tidak hanya terbatas pada kelancaran operasional pemerintahan, melainkan juga meluas pada seluruh elemen masyarakat yang secara rutin mengandalkan layanan publik. Dalam situasi ketidaktersediaan akses layanan publik yang diakibatkan oleh insiden siber atau permasalahan keamanan data, potensi kerugian yang dialami publik sangat substansial. Hal ini mencakup penundaan dan

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

peningkatan kompleksitas dalam proses administrasi, kerugian finansial, serta disrupsi sosial yang dapat mengganggu kenyamanan dan kualitas hidup.

Menurut Satjipto Rahardjo (Satjipto Rahardjo, 2006), seorang ahli hukum, pada dasarnya aturan hukum itu seharusnya bisa menjadi penjaga sejati bagi siapa pun yang hak-haknya terancam atau sudah mengalami kerugian.

Berdasarkan insiden Pusat Data Nasional (PDN) tahun 2024, upaya perlindungan terhadap masyarakat tidak semata-mata berfokus pada restorasi fungsionalitas layanan publik. Akan tetapi, aspek krusial lainnya adalah jaminan bahwa informasi pribadi warga negara yang terhimpun dalam infrastruktur digital pemerintah benar-benar terjamin keamanan dan integritasnya dari potensi ancaman yang tidak dikehendaki.

Berdasarkan evaluasi, tidak teridentifikasi adanya kerangka regulasi yang eksplisit mengenai penyediaan bantuan bagi masyarakat yang terdampak oleh disrupsi layanan digital pemerintah. Hal ini secara tegas mengindikasikan bahwa dimensi perlindungan warga negara masih merupakan suatu kelalaian dalam pelaksanaan akuntabilitas negara.

Kelemahan Transparansi dan Akuntabilitas

Dalam suatu sistem kenegaraan yang menjunjung tinggi supremasi hukum, esensial bagi otoritas publik untuk menjunjung tinggi prinsip transparansi dan akuntabilitas. Dengan demikian, apabila terjadi disrupsi atau anomali substansial pada infrastruktur digital vital nasional, publik memiliki hak fundamental untuk memperoleh klarifikasi yang komprehensif. Informasi tersebut mencakup analisis akar penyebab insiden, implikasi kolektif yang ditimbulkannya, serta strategi mitigasi dan upaya remediasi konkret yang diimplementasikan oleh pemerintah guna memulihkan stabilitas operasional secara efisien. Mengacu pada insiden-insiden yang terjadi, seperti yang dialami oleh PDN 2024, prinsip keterbukaan menjadi sangat esensial. Hal ini krusial karena berkaitan langsung dengan tingkat kepercayaan publik terhadap sistem digital yang diimplementasikan oleh pemerintah.

Ketersediaan informasi yang transparan dan akuntabel mengenai penanganan suatu insiden adalah esensial. Hal ini bertujuan untuk membangun keyakinan publik dan memastikan pemahaman bahwa otoritas terkait telah mengoptimalkan upaya dalam melaksanakan kewajibannya.

Oleh karena itu, peningkatan transparansi dan akuntabilitas merupakan hal yang sangat krusial, guna menjamin kesiapsiagaan serta kapabilitas negara ini dalam menanggulangi beragam ancaman siber yang berpotensi muncul di masa mendatang.

Analisis Berdasarkan Teori Negara Hukum dan Teori Perlindungan Hukum

Sebagai suatu entitas negara yang menganut prinsip supremasi hukum, lembaga eksekutif memikul mandat krusial untuk menjamin proteksi terhadap hak-hak fundamental segenap warga negaranya. Implementasi tugas tersebut terealisasi melalui praktik tata kelola pemerintahan yang menjunjung tinggi integritas dan akuntabilitas. (Asshiddiqie, 2011).

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

Tanggung jawab utama dalam konteks penanganan insiden, khususnya terkait permasalahan gangguan sistem informasi, direalisasikan melalui serangkaian upaya komprehensif. Upaya-upaya ini mencakup Langkah langkah antisipatif untuk mencegah terulangnya insiden serupa, manajeme n responsive terhadap situasi saat gangguan sedang berlangsung, serta proses resto rasi dan pemulihan fungsionalitas sistem yang terdampak.

(Satjipto Rahardjo, 2006) pernah mengatakan Peran fundamental kerangka hukum adalah menyediakan perlindungan yang substansial dan efektif bagi masyarakat. Oleh karena itu, evaluasi akuntabilitas serius penyelenggara negara seharusnya tidak semata-mata didasarkan pada kuantitas regulasi yang diterbitkan. Kriteria yang lebih krusial adalah sejauh mana efektivitas perlindungan tersebut benar-benar dialami dan dirasakan oleh warga negara, khususnya dalam menghadapi gangguan atau disrupsi pada sistem digital nasional.

Dari hasil kajian yang menyeluruh, terungkap bahwa masalah tanggung jawab pemerintah terkait insiden gangguan di Pusat Data Nasional pada tahun 2024 lalu bukan karena ketiadaan aturan, melainkan pada bagaimana aturan itu dijalankan, cara mengelola keamanan siber, upaya mengurangi risiko, keterbukaan informasi, serta perlindungan bagi masyarakat yang terkena dampaknya.

Dengan demikian, sangat esensial untuk mengukuhkan kerangka kebijakan keamanan siber pada skala nasional, serta meningkatkan kapasitas entitas pemerintah dalam pengelolaan infrastruktur digitalnya, guna mencegah terulangnya insiden sejenis di masa mendatang.

Analisis Kelemahan Pertanggungjawaban Negara Dari Perspektif *Ethical Hacker*

Selain pertimbangan aspek hukum, insiden disrupsi Pusat Data Nasional pada tahun 2024 ini juga krusial untuk dikaji dari sudut pandang keamanan siber. Dalam konteks perlindungan data digital, peran seorang *ethical hacker* (peretas etis) menjadi sangat signifikan. Tugas mereka meliputi penemuan dan pelaporan celah keamanan atau kelemahan dalam sistem, guna mencegah eksploitasi oleh pihak-pihak yang tidak bertanggung jawab.

Dalam konteks profesional keamanan siber yang beretika, fokus esensial mereka tidak terbatas pada keberhasilan penetrasi oleh entitas berbahaya, melainkan lebih kepada analisis mendalam terhadap faktor-faktor penyebab kerentanan sistem yang memungkinkan terjadinya pelanggaran tersebut. Keamanan informasi bukan hanya ditentukan oleh aspek teknologis semata, melainkan juga oleh landasan kebijakan organisasi, metodologi manajemen risiko, serta tingkat kesadaran keaman an pada pengguna akhir (Susanto et al., 2012).

Para pakar keamanan siber, seperti yang diungkap dalam *The Web Application Hacker's Handbook*, menegaskan bahwa Menjamin integritas dan keamanan suatu sistem tidak dapat dicapai hanya melalui penerapan solusi teknologis semata. Sebaliknya, pendekatan ini harus ditopang oleh serangkaian

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

evaluasi dan verifikasi keamanan yang komprehensif, yang dilaksanakan secara berkelanjutan dan iteratif (Stuttard & Pinto, 2011).

Selain itu, infrastruktur yang mengelola data krusial berjumlah besar perlu menjalani audit berkala. Langkah ini bertujuan untuk mengidentifikasi dan mendeteksi potensi celah keamanan atau kerentanan, sebelum entitas tidak bertanggung jawab dapat mengeksploitasinya.

Perspektif ini secara tegas menggarisbawahi bahwa keamanan bukanlah suatu kondisi statis atau pencapaian tunggal yang final, melainkan suatu lintasan atau proses dinamis yang berkelanjutan, yang menuntut pemeliharaan dan pengawasan berkelanjutan.

Dari perspektif para pakar keamanan siber yang beretika, insiden yang terjadi pada Pusat Data Nasional (PDN) pada tahun 2024 lalu secara eksplisit mengindikasikan bahwa strategi proteksi yang diimplementasikan belum sepenuhnya mengintegrasikan prinsip keamanan yang dirancang sejak awal.

Prinsip ini pada dasarnya mengamanatkan bahwa unsur-unsur keamanan harus diintegrasikan secara intrinsik di seluruh tahapan rekayasa dan pengelolaan sistem, dimulai dari fase desain fundamental, alih-alih menjadi tambahan perifer setelah sistem diterapkan. Selain itu, penelitian oleh Ross Anderson menjelaskan bahwa insiden keamanan sering kali timbul bukan utamanya sebagai konsekuensi dari instrumentasi atau komponen teknologi yang substandar, melainkan sebagian besar disebabkan oleh manajemen risiko yang tidak memadai dan kurangnya antisipasi yang cermat terhadap berbagai potensi bahaya di masa depan.

Penelusuran lebih lanjut menunjukkan bahwa salah satu permasalahan krusial dalam kasus PDN tersebut adalah ketergantungan yang berlebihan pada satu sistem terpusat yang mengelola volume data yang sangat besar. Padahal, standar keamanan data internasional mengamanatkan bahwa sistem-sistem yang memiliki tingkat kepentingan tinggi harus dilengkapi dengan redundansi cadangan (backup ganda), replikasi data yang berkelanjutan, serta rencana pemulihan darurat yang efektif. Prinsip-prinsip ini fundamental untuk menjamin keberlangsungan operasional layanan publik, bahkan saat terjadi insiden keamanan atau serangan siber.

Menurut pandangan pakar keamanan siber (*ethical hacker*), keberhasilan suatu serangan siber sering kali mengindikasikan bahwa organisasi terkait belum mengimplementasikan secara komprehensif prinsip *"defense in depth"* (pertahanan berlapis). Hal ini merujuk pada ketiadaan lapisan-lapisan keamanan yang memadai untuk memitigasi dampak serangan, sekalipun salah satu lapisan pertahanan telah berhasil ditembus.

Kerangka Kerja Keamanan Siber yang dirilis oleh National Institute of Standards and Technology (NIST) secara eksplisit menyatakan bahwa implementasi keamanan siber memerlukan konstruksi berdasarkan lima fungsi fundamental, yakni identifikasi, proteksi, deteksi, respons, dan pemulihan (Ross Anderson, 2020).

Analisis terhadap insiden Pusat Data Nasional (PDN) 2024 mengindikasikan bahwa aspek identifikasi risiko, kapasitas deteksi dini, dan kapabilitas pemulihan

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

sistem masih memerlukan penguatan substansial. Konsekuensinya, permasalahan yang dihadapi tidak hanya berpusat pada serangan siber itu sendiri, namun juga pada tingkat kematangan organisasi dalam manajemen risiko keamanan informasi.

Dari sudut pandang hukum, kekurangan ini sangat erat kaitannya dengan tanggung jawab pemerintah. Pemerintah bukan cuma harus bertindak setelah kejadian buruk menimpa, tapi juga punya kewajiban untuk menyiapkan pengamanan yang memadai agar layanan-layanan penting untuk masyarakat tidak terganggu.

Menurut pandangan para pakar keamanan siber etis, isu akuntabilitas pemerintah terkait insiden Pusat Data Nasional (PDN) tahun 2024 dapat diatribusikan pada suboptimalitas kinerja dalam beberapa domain krusial. Hal ini mencakup, antara lain, manajemen Risiko keamanan siber yang belum komprehensif, kurangnya pelaksanaan pengujian keamanan secara berkala, ketidakcukupan infrast ruktur sistem pencadangan, serta pendekatan pengelolaan keamanan data yang belum sepenuhnya berorientasi pada strategi preventif.

KESIMPULAN DAN SARAN

Kesimpulan

Analisis komprehensif terhadap temuan studi dan pembahasan ini mengidentifikasi adanya defisiensi dalam mekanisme akuntabilitas pemerintah terkait insiden gangguan operasional pusat data nasional di Indonesia pada tahun 2024, menunjukkan bahwa:

Secara fundamental, landasan hukum mengenai akuntabilitas negara dalam proteksi data personal dan penyelenggaraan sistem elektronik di yurisdiksi Indonesia telah tercantum melalui beragam instrumen legislatif. Instrumen tersebut meliputi, antara lain, Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi, serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah mengalami amendemen terakhir melalui Undang-Undang Nomor 1 Tahun 2024. Merujuk pada prinsip-prinsip Teori Negara Hukum *(Rechtsstaat)* dan Teori Perlindungan Hukum, negara mengemban obligasi konstitusional untuk menjamin proteksi terhadap hak-hak fundamental warga negara, yang mencakup hak atas privasi, integritas data personal, serta kontinuitas pelayanan publik yang berbasis digital. Oleh karena itu, secara legal-normatif Indonesia telah dilengkapi dengan landasan yuridis yang memadai untuk meregulasi proteksi data personal dan keamanan infrastruktur elektronik.

Kedua, defisiensi dalam akuntabilitas institusional negara terkait insiden Gangguan Pusat Data Nasional (PDN) Tahun 2024 bukan bersumber dari ketiadaan kerangka regulasi, melainkan dari tataran implementasi. Kelemahan ini termanifestasi melalui belum optimalnya inisiatif pencegahan dan mitigasi Risiko keamanan siber, kerapuhan tata Kelola keamanan informasi, ketidakadekuatan proteksi bagi Masyarakat pengguna yang terdampak disrupsi layanan publik, serta urgensi penguatan transparansi dan akuntabilitas dalam manajemen insiden siber.

Dari sudut pandang praktisi keamanan siber etis, insiden PDN 2024 ini menggarisbawahi urgensi penerapan *security by design*, *defense in depth*, audit

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

keamanan secara periodik, penilaian kerentanan *(vulnerability assessment)*, pengujian penetrasi *(penetration testing)*, serta manajemen risiko keamanan siber yang lebih holistik. Dengan demikian, konsolidasi keamanan siber nasional tidak hanya menuntut kerangka regulasi yang adekuat, melainkan pula eksekusi implementasi yang berdaya guna dalam rangka memastikan proteksi data personal dan kesinambungan penyediaan layanan publik dalam lanskap digital.

Saran

Studi ini mengemukakan bahwa peningkatan akuntabilitas negara dalam pengelolaan sistem elektronik nasional tidak dapat semata-mata dicapai melalui pembentukan regulasi baru. Prioritas utama justru terletak pada jaminan bahwa seluruh infrastruktur digital strategis nasional mengimplementasikan mekanisme pengawasan dan validasi keamanan secara berkala yang memiliki parameter terukur serta akuntabilitas yang jelas. Pemerintah seyogyanya mewajibkan pelaksanaan audit keamanan independen, penilaian kerentanan, dan pengujian penetrasi oleh entitas independen yang kompeten sebelum suatu sistem dioperasikan untuk penyimpanan atau pengelolaan data publik dalam skala besar.

Lebih lanjut, esensial bagi pemerintah untuk menginternalisasi suatu paradigma baru yang memandang keamanan siber semata-mata merupakan isu teknologis, melainkan komponen fundamtental dari tata kelola publik yang efektif. Konsekuensinya, insiden kegagalan dalam pengamanan sistem elektronik yang berujung pada disrupsi layanan publik tidak seharusnya hanya dikategorikan sebagai defisiensi teknis, namun juga sebagai manifestasi dari kelalaian administratif yang memerlukan evaluasi melalui kerangka akuntabilitas yang transparan dan terdefinisi. Maka dari itu, setiap entitas pengelola sistem elektronik sektor publik mengemban kewajiban yang terukur terkait dengan pengamanan data serta pemeliharaan keberlanjutan layanan publik.

Dari perspektif seorang pakar keamanan siber, sangatlah penting bagi otoritas nasional untuk mengintegrasikan prinsip-prinsip *security by design* dan *defense in depth* di seluruh ekosistem digital negara. Keamanan tidak boleh lagi diperlakukan sebagai pertimbangan tambahan pasca pengembangan sistem sebalik nya, ia harus menjadi komponen integral sepanjang seluruh siklus hidup sistem, mencakup fase perencanaan, pengembangan, implementasi, dan evaluasi. Insiden baru baru ini yang melibatkan infrastruktur data nasional pada tahun 2024 menggar isbawahi ketidakcukupan metodologi reaktif yang semata-mata berfokus pada pemulihan pasca-insiden. Oleh karena itu, negara harus beralih menuju strategi preventif yang berorientasi pada identifikasi risiko sejak dini dan mitigasi kerentanan secara proaktif sebelum dieksploitasi oleh aktor-aktor berbahaya.

Selanjutnya, penuis mengemukakan bahwa pemerintah seyogianya mengevaluasi pembentukan suatu mekanisme pengungkapan kerentanan *(vulnerability disclosure program)* dan memperluas kolaborasi yang transparan dengan komunitas pakar keamanan siber serta peretas etis di yurisdiksi Indonesia. Partisipasi entitas independen dalam identifikasi dan notifikasi kelemahan keamanan secara akuntabel dapat menjadi strategi preventif yang berdaya guna dalam rangka

Vol 6 No 2 (2026) 334–346 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v6i2.13136

memperkukuh resiliensi siber di tingkat nasional. Dengan demikian, jaminan proteksi sistem elektronik tidak hanya bertumpu pada kapabilitas internal institusi pemerintah, melainkan juga disokong oleh suatu ekosistem keamanan siber nasional yang bersifat sinergis dan berkelanjutan.

DAFTAR PUSTAKA

Anderson, Ross. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd Editio). Wiley Publishing, Inc.

Asshiddiqie, J. (2011). *Konstitusi dan Konstitusionalisme Indonesia* (1st ed.). Sinar Grafika.

Dewi, S., Hukum, F., & Padjadjaran, U. (2016). *Konsep perlindungan hukum atas privasi dan data pribadi dikaitkan dengan penggunaan cloud computing di Indonesia*. *5*(1), 22–30.

Kriswandaru, A. S., Pratiwi, B., Studi, P., Hukum, I., Studi, P., Hukum, I., Kewirausahaan, P. S., Info, A., Data, P., Hukum, K., Data, P., & Hukum, P. (2024). *Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus*. *2*(4), 740–755. https://doi.org/10.51903/hakim.v2i04.2157

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Jurnal Hukum Dan Pembangunan*, *50*(4), 497–518.

Pascoe, C. (2024). *Public Draft: The NIST Cybersecurity Framework 2.0 National Institute of Standards and Technology*.

Putri, D. A., Rizqy, M., & Putra, S. (2025). *Tanggung Jawab Prosesor Data terhadap Kebocoran Data Pusat Data Nasional Tahun 2024*. *8*(1), 29–34. https://doi.org/10.35965/ijlf.v8i1.7902

Satjipto Rahardjo. (2006). *Ilmu Hukum* (Cetakan Ke). Citra Aditya Bakti.

Soekanto, Soerjono., Sri Mamudji. (2015). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (17th ed.). Rajawali Pers.

Solms, R. Von., & Niekerk, J. Van. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* (2nd Editio). Wiley Publishing, Inc.

Susanto, H., Almunawar, M. N., & Kang, C. C. (2012). *Toward Cloud Computing Evolution : Efficiency vs Trendy vs Security*.

Yuniarti, Siti. (2023). Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia. *Jurnal Legislasi Indonesia*, 81–102.