Equality: Law And Social
Volume 1, Nomor 4, 2026
E-ISSN: 3123-1926
Akses Terbuka: https://ejournal.risetanakbangsa.id/jhs

Analisis Yuridis Kebocoran Data pada Pusat Data Nasional Sementara (PDNS) dalam Perspektif Undang-Undang Perlindungan Data Pribadi

Amalia siti Nurrohmah[1], Hilman Nur[2]
[1,2] Universitas Suryakancana, Indonesia
Korespondensi: sitinurrohmahamalia@gmail.com

Informasi Artikel

Riwayat artikel:
Diterima April 26th, 2026
Direvisi Mei 02th, 2026
Diterima Mei 04th, 2026

Kata kunci:
Perlindungan data pribadi, kebocoran data, Pusat Data Nasional Sementara (PDNS), pertanggungjawaban hukum, privasi digital.

ABSTRAK

Penelitian ini dilatarbelakangi oleh meningkatnya risiko kebocoran data pribadi di era digital, khususnya pada kasus kebocoran data Pusat Data Nasional Sementara (PDNS) tahun 2024 yang berdampak pada terganggunya layanan publik dan menurunnya kepercayaan masyarakat. Penelitian ini bertujuan untuk menganalisis pengaturan hukum perlindungan data pribadi di Indonesia, mengkaji pertanggungjawaban hukum pemerintah sebagai pengendali data, serta menilai implikasinya terhadap perlindungan hak masyarakat. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual berbasis data sekunder. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki dasar hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, masih terdapat kesenjangan antara norma dan implementasi, khususnya terkait mekanisme pengawasan, sanksi, dan ganti rugi bagi korban kebocoran data. Kasus PDNS mengindikasikan adanya kelemahan sistem keamanan serta belum optimalnya akuntabilitas pemerintah dalam pengelolaan data pribadi. Penelitian ini menemukan adanya kekosongan pengaturan yang komprehensif mengenai pertanggungjawaban negara dalam insiden kebocoran data. Oleh karena itu, diperlukan penguatan sistem keamanan, kejelasan mekanisme pertanggungjawaban, serta pembentukan sistem pengawasan yang efektif guna menjamin perlindungan data pribadi dan memulihkan kepercayaan publik.

PENDAHULUAN

Di era digital yang semakin terkoneksi dan bergantung pada teknologi informasi, data pribadi menjadi salah satu aset paling berharga sekaligus paling rentan terhadap berbagai bentuk eksploitasi. Pengumpulan, penyimpanan, dan pemrosesan data pribadi oleh institusi publik maupun swasta menimbulkan kebutuhan mendesak akan kerangka hukum yang kokoh untuk melindungi hak-hak individu atas privasi dan kendali atas informasi pribadi mereka (Karnedi & Alam, 2025)**.**

Perkembangan teknologi informasi dan komunikasi yang cukup pesat membawa transformasi dalam berbagai aspek kehidupan masyarakat. Salah satu dampak yang paling signifikan adalah meningkatnya aktivitas dalam sektor publik maupun privat yang berbasis atau bergantung pada sistem digital (Ongkowiguno & Marsal, 2025). Seperti dalam pengelolaan data nasional. Digitalisasi layanan publik membuat pemerintah menggabungkan berbagai sistem informasi ke dalam satu pusat data agar pelayanan menjadi lebih cepat, efisien, dan berkualitas untuk masyarakat.

Di sisi lain, upaya global dalam meningkatkan perlindungan data pribadi tercermin dari implementasi General Data Protection Regulation (GDPR) oleh Uni Eropa, yang tidak hanya mengatur tata kelola data pribadi secara ketat tetapi juga menjamin hak-hak individu seperti hak untuk dihapus (right to be forgotten) dan hak portabilitas data (data portability). Di Indonesia, pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan langkah progresif yang mencerminkan kesadaran pemerintah akan pentingnya perlindungan data dalam menghadapi tantangan ekosistem digital. Namun, implementasi dan pengawasan terhadap UU ini masih menghadapi sejumlah kendala (Karnedi & Alam, 2025).

Salah satu contohnya adalah Pusat Data Nasional Sementara (PDNS). Perkembangan teknologi ini dapat meningkatkan risiko kebocoran data pribadi yang semakin meningkat, sehingga berdampak pada hak masyarakat. Risiko tersebut terwujud secara nyata pada 20 Juni 2024 ketika Indonesia mengalami insiden keamanan siber terbesar dalam sejarah pemerintahan digitalnya. PDNS diserang

ransomware Brain Cipher yang melumpuhkan layanan pada 282 instansi pemerintah, termasuk sektor strategis seperti imigrasi, bea cukai, kesehatan, dan Pendidikan (Puannandini et al., 2026).

Kebocoran data di Pusat Data Nasional Sementara (PDNS) mengungkap kelemahan keamanan data nasional dan menimbulkan keprihatinan tentang perlindungan hukum di Indonesia. Kebocoran ini melibatkan jutaan data pribadi yang dapat digunakan untuk tujuan kriminal, menunjukkan perlunya peningkatan sistem hukum perlindungan data (Gabriel, 2024). Serangan ini tidak hanya menyebabkan lumpuhnya layanan publik di berbagai sektor, tetapi juga mengungkapkan kelemahan struktural dalam manajemen keamanan informasi pemerintah, seperti lemahnya kontrol akses, ketiadaan sistem pencadangan (backup), dan minimnya kesiapan dalam menangani insiden siber secara terkoordinasi. Padahal, keberhasilan sistem digital pemerintahan tidak hanya ditentukan oleh ketersediaan infrastruktur teknologi, tetapi juga oleh kualitas manajerial dalam mengelola risiko dan menjamin kontinuitas layanan publik di tengah krisis (Tommy et al., 2025).

Kasus kebocoran data terjadi pada Pusat Data Nasional Sementara (PDNS), yang merupakan sistem transisi sebelum implementasi penuh Pusat Data Nasional (PDN). Menurut Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang SPBE, PDN dirancang untuk meningkatkan kualitas penyelenggaraan layanan SPBE dengan menyediakan infrastruktur yang andal dan terstandarisasi. PDN juga berperan dalam memastikan keamanan dan ketersediaan data pemerintah, yang merupakan aspek krusial dalam penyelenggaraan pemerintahan digital. Dengan adanya PDN, diharapkan terjadi peningkatan efisiensi operasional dan pengurangan duplikasi data antar instansi, sehingga mendukung terciptanya tata kelola pemerintahan yang bersih, transparan, dan akuntabel. Lebih lanjut, PDN mendukung transformasi digital nasional dengan menyediakan infrastruktur yang memungkinkan integrasi data dan layanan secara menyeluruh. Hal ini sejalan dengan upaya pemerintah dalam mewujudkan pelayanan publik yang berkualitas dan terpercaya melalui pemanfaatan teknologi informasi dan komunikasi (Tommy et al., 2025).

Kebocoran data pribadi membuat masyarakat merasa tidak aman dan kehilangan kepercayaan kepada pemerintah. Secara hukum, negara wajib melindungi data pribadi karena itu merupakan bagian dari hak asasi manusia. Namun, dalam kenyataannya masih belum jelas bagaimana bentuk tanggung jawab negara dan bagaimana cara memberikan ganti rugi terhadap korban kebocoran data.

Dari perspektif hukum tata negara dan hukum administrasi, pemerintah memiliki kewajiban untuk memberikan perlindungan terhadap hak-hak warga negara, termasuk hak atas privasi dan data pribadi. Kegagalan dalam melindungi data dapat dikategorikan sebagai bentuk kelalaian negara (state liability) yang berpotensi menimbulkan tanggung jawab hukum. Oleh karena itu, penting untuk mengkaji lebih dalam mengenai bentuk pertanggungjawaban pemerintah serta mekanisme pemulihan bagi masyarakat yang dirugikan akibat kebocoran data.

Berdasarkan uraian tersebut, perlu dilakukan analisis hukum yang mendalam terhadap kebocoran data pada PDNS untuk mengetahui bagaimana tanggung jawab pemerintah dan implikasinya terhadap perlindungan data pribadi di era digital. Dengan demikian penelitian ini berupaya menjawab pertanyaan: (1) bagaimana pengaturan hukum perlindungan data pribadi terhadap kebocoran data pada PDNS di era digital; dan (2) bagaimana pertanggungjawaban hukum pemerintah atas kebocoran data PDNS dan implikasinya bagi perlindungan hak data pribadi masyarakat.

Sejalan dengan rumusan masalah tersebut penelitian ini bertujuan untuk: (1) untuk menganalisis aturan hukum tentang perlindungan data pribadi terkait kebocoran data PDNS di era digital, termasuk melihat kelebihan dan kekurangan Undang-Undang Perlindungan Data Pribadi serta aturan pendukung lainnya; dan (2) untuk mengetahui bagaimana bentuk tanggung jawab hukum pemerintah atas kasus PDNS, serta dampaknya terhadap perlindungan hak data pribadi masyarakat, termasuk memberikan saran perbaikan kebijakan ke depan. Dengan demikian, penelitian ini diharapkan dapat memberikan solusi agar kasus serupa tidak terulang dan dapat mengembalikan kepercayaan masyarakat terhadap sistem pemerintahan digital.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum yuridis normatif (doktrinal), yaitu penelitian yang berfokus pada pengkajian norma hukum dalam peraturan perundang-undangan, asas hukum, serta doktrin yang berkembang dalam ilmu hukum. Metode ini digunakan untuk menganalisis isu kebocoran data pada Pusat Data Nasional Sementara dalam perspektif perlindungan data pribadi.

Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi terkait, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan mengenai sistem elektronik dan penyelenggaraan pemerintahan berbasis elektronik. Pendekatan konseptual digunakan untuk menganalisis konsep perlindungan data pribadi, asas perlindungan hukum, dan teori pertanggungjawaban negara. Sementara itu, pendekatan kasus digunakan untuk mengkaji insiden kebocoran data PDNS sebagai peristiwa hukum konkret.

Sumber bahan hukum dalam penelitian ini terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan, sedangkan bahan hukum sekunder berupa literatur hukum, jurnal ilmiah, dan pendapat para ahli. Adapun bahan hukum tersier meliputi kamus hukum dan ensiklopedia yang mendukung pemahaman konsep.

Analisis bahan hukum dilakukan secara kualitatif dengan menggunakan metode interpretasi hukum, yaitu interpretasi gramatikal, sistematis, dan teleologis, serta didukung oleh argumentasi hukum untuk menemukan kesesuaian antara norma dan praktik. Penelitian ini bersifat preskriptif, yaitu memberikan rekomendasi terhadap penguatan regulasi dan mekanisme pertanggungjawaban hukum dalam perlindungan data pribadi.

HASIL DAN PEMBAHASAN

Pengaturan Hukum Perlindungan Data Pribadi terhadap Kebocoran Data pada PDNS di Era Digital

Menurut Alan Westin, perlindungan data pribadi merupakan bagian dari hak privasi, yaitu hak individu untuk menentukan kapan dan sejauh mana informasi tentang dirinya disampaikan kepada pihak lain. Sementara itu, menurut Peter P. Swire, perlindungan data pribadi merupakan suatu sistem hukum dan kebijakan yang mengatur bagaimana organisasi mengelola data individu guna mencegah penyalahgunaan serta memberikan hak kepada individu atas datanya. Pandangan ini juga sejalan dengan penelitian dalam jurnal hukum di Indonesia yang menyatakan bahwa perlindungan data pribadi mencak up pengaturan terhadap pengumpulan, pengelolaan, dan penggunaan data individu melalui kerangka hukum yang jelas guna menjamin hak privasi dan mencegah penyalahgunaan data.

Pengaturan hukum mengenai perlindungan data pribadi di Indonesia menunjukkan perkembangan yang signifikan sejak disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi. Hal ini bertujuan untuk melindungi hak privasi, mencegah penyalahgunaan data, dan memastikan keamanan data pribadi dalam pemrosesan oleh instansi pemerintah maupun korporasi.

Sebelum adanya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, aturan tentang perlindungan data pribadi di Indonesia masih tersebar di berbagai peraturan dan belum diatur dalam satu undang-undang khusus. Misalnya, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bahwa penggunaan data pribadi di media elektronik harus mendapat persetujuan dari pemiliknya. Lalu, Peraturan Pemerintah Nomor 71 Tahun 2019 menegaskan bahwa penyelenggara sistem elektronik wajib menjaga keamanan data yang mereka kelola.

Selain itu, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 memberikan pedoman teknis tentang bagaimana data pribadi dikumpulkan, disimpan, dan digunakan. Ada juga Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan yang melindungi kerahasiaan data penduduk, serta Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik yang membatasi penyebaran informasi yang mengandung data pribadi.

Namun, aturan-aturan tersebut belum memberikan perlindungan yang menyeluruh karena masih tersebar dan belum tersusun dalam satu sistem hukum yang jelas, Karena itu, hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi hal yang sangat penting dalam hukum Indonesia. Dengan adanya undang-undang ini, aturan yang sebelumnya tersebar menjadi lebih teratur dan perlindungan terhadap data pribadi menjadi lebih kuat sebagai bagian dari hak privasi dan hak asasi manusia.

Implementasi UU tersebut dalam kasus-kasus pembocoran data pribadi melibatkan beberapa aspek penting, antara lain:

1. Kewajiban Penangguang Jawab Data

UU tersebut akan menetapkan kewajiban bagi penanggung jawab data, seperti perusahaan atau organisasi yang mengumpulkan dan mengelola data pribadi. Mereka harus menjaga kerahasiaan dan keamanan data pribadi yang mereka miliki. Implementasi UU dapat meminta penanggung jawab data untuk mengadopsi langkah-langkah teknis dan organisasi yang memadai untuk melindungi data pribadi dari akses yang tidak sah atau penggunaan yang tidak sah.

2. Kewajiban Pemberitahuan
   Jika terjadi kebocoran data UU tersebut dapat mengharuskan penanggung jawab data untuk memberikan pemberitahuan kepada individu yang terkena dampak jika terjadi pelanggaran keamanan data yang dapat mengakibatkan kerugian atau risiko bagi mereka. Pemberitahuan tersebut harus dilakukan dengan segera setelah pelanggaran data terdeteksi, sehingga individu dapat mengambil langkah-langkah yang diperlukan untuk melindungi diri mereka sendiri, seperti mengganti kata sandi atau memantau aktivitas keuangan mereka.
3. Sanksi dan Tanggung Jawab
   Implementasi UU akan menetapkan sanksi dan tanggung jawab bagi pelanggar data pribadi. Sanksi ini dapat berupa denda yang signifikan atau tuntutan hukum terhadap penanggung jawab data yang melanggar ketentuan perlindungan data. UU tersebut juga dapat menetapkan tanggung jawab kompensasi bagi individu yang menderita kerugian akibat dari pelanggaran data pribadi, termasuk pemulihan kerugian finansial atau pemulihan reputasi (Saly et al., 2023).

Pada tahun 2024 terdapat kasus kebocoran data Pusat Data Nasional Sementara (PDNS). Dalam konteks ini, pengelolaan data melalui Pusat Data Nasional Sementara (PDNS) menjadi salah satu fokus utama, mengingat perannya sebagai pusat integrasi data pemerintah yang berskala besar dan strategis. Pemerintah sebagai pengendali data memiliki tanggung jawab untuk memastikan bahwa data yang dikelola tidak disalahgunakan, tidak diakses oleh pihak yang tidak berwenang, serta terlindungi dari ancaman kebocoran.

Kebocoran data yang terjadi pada PDNS menjadi bukti nyata adanya kesenjangan antara regulasi dan praktik. Insiden tersebut menunjukkan bahwa sistem keamanan data yang dimiliki pemerintah masih rentan terhadap serangan siber. Dalam perspektif hukum, kebocoran data ini tidak hanya mencerminkan kegagalan teknis, tetapi juga dapat dikategorikan sebagai bentuk kelalaian dalam menjalankan kewajiban hukum sebagai pengendali data.

Dalam aspek pertanggung jawaban hukum, pada prinsipnya pemerintah dapat dimintai pertanggung jawab atas terjadinya kasus kebocoran data PDNS. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) Adalah langkah besar bagi Indonesia dalam menghadapi tantangan perlindungan data di era digital. Sebelum ada UU ini, aturan soal data pribadi tersebar di berbagai sektor dan belum terkoordinasi dengan baik. Jadi, kehadiran UU PDP membawa harapan baru, masyarakat ingin ada perlindungan hukum yang lebih jelas dan kuat atas data pribadinya (Rinjani & Firmansyah, 2025).

Di sisi lain, perkembangan era digital membuat perlindungan data pribadi menjadi semakin sulit. Teknologi yang terus berkembang menyebabkan jumlah data yang dikelola menjadi semakin banyak. Namun, di saat yang sama, ancaman terhadap keamanan data juga semakin canggih, seperti serangan siber dan peretasan. Penggunaan sistem seperti PDNS memang membantu pengelolaan data menjadi lebih cepat dan efisien. Akan tetapi, dengan terjadinya kebocoran data PDNS, berdampak besar besar dan merugikan masyarakat. Kebocoran ini secara langsung melanggar hak privasi warga negara yang dijamin oleh Pasal 28G UUD 1945 dan UU No. 27 Tahun 2022.

Hak atas privasi, terkadang dikenal sebagai hak untuk tidak diganggu, diciptakan oleh Warren dan Brandheis dan diterbitkan dalam sebuah manuskrip berjudul "The Right to Privacy" di jurnal ilmiah Harvard University Law School. Menurut Warren dan Brandheis dalam jurnal tersebut, tumbuh dan berkembangnya teknologi telah menimbulkan kesadaran masyarakat yang menimbulkan kesadaran bahwa setiap orang berhak untuk menikmati hidup (Suari & Sarjana, 2024).

Hak privasi terhadap data pribadi mencakup hak setiap individu untuk mengetahui apa yang terjadi dengan data pribadi mereka, siapa yang mengaksesnya, untuk tujuan apa data tersebut digunakan, dan bagaimana data tersebut diolah dan disimpan. Lebih dari itu, prinsip ini juga melibatkan hak untuk memberikan izin atau persetujuan atas penggunaan data pribadi tersebut, serta hak untuk meminta penghapusan data (right to be forgotten) atau koreksi jika data tersebut tidak akurat (Suari & Sarjana, 2024).

Kepercayaan terhadap sistem digital sangat tergantung pada sejauh mana keamanan data dijaga. Kepercayaan yang tinggi akan mendorong partisipasi masyarakat dalam ekosistem digital, yang pada gilirannya akan mempercepat adopsi teknologi dan memperkuat komunitas digital. Ini bukan hanya soal menjaga informasi pribadi, tetapi juga tentang
mempertahankan kendali atas kehidupan digital mereka, sehingga mereka dapat berinteraksi secara aman dan bebas dalam platform media sosial (Putri et al., 2025).
Dengan demikian, perlindungan data pribadi di Indonesia masih berada pada tahap transisi, yaitu dari penguatan regulasi menuju efektivitas implementasi. Oleh karena itu, diperlukan sinergi antara penguatan sistem keamanan, kejelasan mekanisme penegakan hukum, serta peningkatan kapasitas kelembagaan agar tujuan perlindungan data pribadi dapat tercapai secara optimal di tengah tantangan era digital.

PertanggungJawaban Hukum Pemerintah atas Kebocoran Data PDNS dan Implikasinya bagi Perlindungan Hak Data Pribadi Masyarakat

Setiap warga negara memiliki hak konstitusional yang dijamin oleh undang undang. Salah satu hak konstitusional yang diatur dalam UUD RI 1945 adalah hak atas perlindungan diri pribadi, sebagaimana dijelaskan dalam Pasal 28 G Ayat (1). Hak pribadi melibatkan perlindungan terhadap data pribadi dan identitas seseorang, termasuk informasi sensitif seperti Kartu Tanda Penduduk (KTP), Surat Izin Mengemudi (SIM), Paspor, dan lain sebagainya. Perlindungan data pribadi semakin penting dalam era digital untuk menjaga kebebasan individu dan mencegah penyalahgunaan informasi (Mamonto, 2022).

Data pribadi, dalam Undang-Undang Nomor 24 Tahun 2013 tentang perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, adalah data diri seseorang yang harus disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaan identifikasi, nyata yang melekat dan dapat diidentifikasi baik secara langsung maupun tidak langsung yang sesuai dengan ketentuan peraturan perundang-undangan (Asthi et al., 2025).

Di Indonesia, perlindungan data pribadi dalam konteks digital diatur dalam Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang juga memperjelas bahwa perlindungan data pribadi merupakan komponen dari hak asasi manusia dan menetapkan kewajiban bagi pengelola data untuk menjaga keamanan dan kerahasiaan data yang mereka kelola (Asthi et al., 2025). Meskipun aturan tentang perlindungan data pribadi sudah diatur dalam UU PDP, Indonesia masih sering mengalami kasus kebocoran data. Salah satu yang paling besar terjadi pada tahun 2024, yaitu kebocoran data di Pusat Data Nasional Sementara (PDNS) yang merupakan sistem transisi sebelum implementasi penuh Pusat Data Nasional (PDN).

Kebocoran data pribadi di Indonesia merupakan masalah serius yang berdampak pada berbagai aspek kehidupan masyarakat. Meningkatnya penggunaan teknologi informasi membuat data pribadi seperti NIK, nama, email, dan nomor handphone rentan disalahgunakan karena memiliki nilai jual tinggi. Selain itu, kebocoran data juga mengganggu layanan publik yang penting, seperti sistem perpajakan, layanan keimigrasian, dan layanan Pendidikan (Asthi et al., 2025).

Serangan siber yang menargetkan Pusat Data Nasional Sementara (PDNS) menimbulkan gangguan serius di berbagai sektor. Akibatnya, proses pelayanan menjadi terhambat dan masyarakat kesulitan mengakses layanan penting, seperti pengurusan pajak, paspor, serta program pendidikan seperti KIP Kuliah. Selain menyebabkan keterlambatan dalam proses administrasi, insiden kebocoran data pada PDNS tahun 2024 juga berdampak pada terganggunya akses masyarakat terhadap berbagai layanan penting yang seharusnya dapat mereka peroleh sebagai haknya.

Pemerintah sebagai penyelenggara negara memiliki kewenangan sekaligus tanggung jawab dalam mengelola, menyimpan, dan melindungi data masyarakat yang dihimpun melalui berbagai layanan publik. Namun, seiring dengan meningkatnya ketergantungan pada sistem digital, risiko kebocoran data juga semakin besar dan dapat menimbulkan berbagai dampak hukum serta kerugian bagi masyarakat. Konstruksi tanggung jawab hukum negara atas kebocoran data publik bersifat kompleks karena bersinggungan dengan berbagai cabang hukum tanpa pengaturan komprehensif dan terintegrasi.

Konstruksi tanggung jawab hukum negara atas kebocoran data publik bersifat kompleks karena bersinggungan dengan berbagai cabang hukum tanpa pengaturan komprehensif dan terintegrasi. Perspektif Hukum Administrasi Negara: Tanggung jawab dianalisis dari pendekatan liability based on fault (fautes de service) dan strict liability. UU Administrasi Pemerintahan Pasal 21-22 mengatur

tanggung jawab pejabat pemerintahan untuk ganti rugi, namun tidak secara eksplisit mencakup kebocoran data akibat kelalaian pengelolaan infrastruktur digital atau kegagalan melindungi data dari serangan siber (Puannandini et al., 2026).

Perspektif Hukum Perdata: Tanggung jawab dikonstruksikan melalui doktrin perbuatan melawan hukum (PMH) Pasal 1365 KUH Perdata. Kegagalan negara melindungi data personal dapat dikategorikan sebagai PMH karena melanggar kewajiban hukum dan prinsip kehati-hatian. Namun penerapan menghadapi problematika: perdebatan apakah negara dapat menjadi subjek PMH, ketidakjelasan siapa yang dapat digugat, dan kesulitan pembuktian unsur kesalahan dan kausalitas dalam kasus serangan siber (Puannandini et al., 2026).

Perspektif UU PDP: Pasal 16 mewajibkan pengendali data menerapkan langkah teknis dan organisatoris memadai, Pasal 34 mengatur hak subjek data mengajukan gugatan Ganti rugi, dan Pasal 58 mengatur sanksi administratif hingga denda 2% pendapatan tahunan. Namun tidak mengatur secara eksplisit tanggung jawab negara memberikan kompensasi atau mekanisme kompensasi kolektif untuk kebocoran massal. Perspektif Hukum Pidana: UU PDP Pasal 67-71 mengatur sanksi pidana untuk pelanggaran, namun pertanggungjawaban pidana bersifat personal dan tidak dapat dikenakan kepada negara sebagai entitas. Jalur pidana tidak dapat menjadi satu-satunya mekanisme memenuhi hak korban atas kompensasi (Puannandini et al., 2026).

Implementasi hak subjek data dalam UU PDP di Indonesia masih menghadapi berbagai tantangan. Salah satu tantangan utama adalah belum meratanya pemahaman masyarakat terkait hak-hak yang mereka miliki atas data pribadi mereka. Banyak individu yang tidak mengetahui bahwa mereka memiliki hak untuk mengakses, mengoreksi, menghapus, serta menolak pemrosesan data pribadi mereka sebagaimana diatur dalam UU PDP. Kurangnya sosialisasi yang efektif dari pemerintah menjadi faktor utama yang menghambat pemahaman masyarakat terhadap hak-hak tersebut (Dinata, 2026).

Selain itu, dari perspektif organisasi, banyak institusi yang masih belum memiliki mekanisme yang jelas untuk mengakomodasi permintaan subjek data. Dalam beberapa kasus, individu yang ingin menggunakan haknya terhadap data pribadi menghadapi hambatan birokrasi yang kompleks, yang menyebabkan ketidakjelasandalam proses pengajuan keberatan atau penghapusan data. Hal ini menunjukkan perlunya regulasi yang lebih spesifik terkait prosedur pelaksanaan hak subjek data (Dinata, 2026).

Implikasi dari berbagai permasalahan tersebut terhadap perlindungan hak data pribadi masyarakat cukup besar. Rendahnya pemahaman masyarakat mengenai hak subjek data menyebabkan individu tidak dapat secara optimal mengontrol penggunaan data pribadinya, sehingga meningkatkan risiko penyalahgunaan oleh pihak yang tidak bertanggung jawab. Di sisi lain, belum siapnya institusi dalam menyediakan mekanisme yang jelas, transparan, dan responsif terhadap permintaan subjek data menunjukkan bahwa perlindungan data pribadi masih bersifat normatif dan belum efektif dalam praktik. Kondisi ini diperparah dengan belum adanya pengaturan yang komprehensif mengenai tanggung jawab negara dan mekanisme kompensasi dalam kasus kebocoran data berskala besar, seperti yang terjadi pada PDNS,

Akibatnya, hak-hak masyarakat yang telah dijamin dalam peraturan perundang-undangan, khususnya UU PDP, belum sepenuhnya dapat diwujudkan secara nyata. Selain menimbulkan kerugian material dan immaterial, kebocoran data juga berdampak pada menurunnya kepercayaan publik terhadap pemerintah dalam mengelola sistem digital dan data pribadi. Oleh karena itu, diperlukan upaya yang lebih konkret dari pemerintah, baik melalui penguatan regulasi teknis, peningkatan keamanan siber, pembentukan lembaga pengawas yang independen, maupun peningkatan edukasi dan sosialisasi kepada masyarakat. Dengan langkah tersebut, diharapkan perlindungan hak data pribadi dapat berjalan secara efektif dan mampu memberikan jaminan keamanan serta kepastian hukum bagi seluruh masyarakat.

KESIMPULAN

Perlindungan data pribadi di Indonesia secara normatif telah memiliki dasar hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, namun penelitian ini menemukan adanya kesenjangan antara pengaturan dan implementasi. Kasus kebocoran data pada Pusat Data Nasional Sementara (PDNS) tahun 2024 menunjukkan lemahnya sistem keamanan dan tata kelola data pemerintah. Lebih lanjut, terdapat kekosongan pengaturan yang komprehensif mengenai mekanisme pertanggungjawaban negara serta pemberian ganti rugi kepada korban kebocoran data,

sehingga menimbulkan ketidakpastian hukum dan melemahkan perlindungan hak privasi masyarakat. Kondisi ini menunjukkan bahwa perlindungan data pribadi di Indonesia masih berada pada tahap transisi dan belum sepenuhnya efektif dalam menjamin keamanan data dan kepercayaan publik.

REFERENSI

Asthi, M., Ari, S., Hakim, A., & Baihaqy, A. (2025). *Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN)*. *4*(156), 31–37. https://www.ejournal-kumhamdiy.com/wicarana/article/view/167/43

Dinata, B. M. (2026). *Implementasi Hak Subjek Data dalam Undang-Undang Perlindungan Data Pribadi: Tantangan dan Efektivitas*. *08*(1), 446–453. https://journalversa.com/s/index.php/jhm/article/view/5080/5838

Gabriel, A. (2024). Perlindungan Hukum Atas Data Pribadi Dalam Kasus Kebocoran Data Pusat Data Nasional Sementara (Pdns) Dalam Perspektif Hukum Pidana. *Seminar Nasional Hukum Dan Pancasila*, *3*, 18–26. https://conference.untag-sby.ac.id/index.php/snhp/article/view/4239/2706

Karnedi, G., & Alam, G. R. (2025). *El-Mujtama : Jurnal Pengabdian Masyarakat El-Mujtama : Jurnal Pengabdian Masyarakat*. *5*(3), 610–622. https://doi.org/10.47467/elmujtama.v5i3.8549

Mamonto, D. F. (2022). *Analisis Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022*. https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/56215

Ongkowiguno, C. M., & Marsal, I. (2025). Politik Hukum Perlindungan Data Pribadi dalam Layanan Publik Digital di Indonesia. *Judge: Jurnal Hukum*, *6*(04), 1321–1326. https://journal.cattleyadf.org/index.php/Judge/article/view/1851/1013

Puannandini, D. A., Faridl, F., Auliya, S., & Buwana, N. (2026). *Tanggung Jawab Hukum Negara atas Kebocoran Data Publik di Era Interkoneksi Digital Nasional : Analisis Kasus Serangan Siber PDNS Kementerian Komunikasi dan Digital*. *10*, 3627–3635. https://jptam.org/index.php/jptam/article/view/36643/23305

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). *Keamanan Online dalam Media Sosial : Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Jurnal Pengabdian Nasional (JPN) Indonesia*. *6*(1), 38–52. https://journal.stmiki.ac.id/index.php/jpni/article/view/1097/834

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 75. https://doi.org/10.38043/jah.v8i1.6793

Saly, J. N., Artamevia, H., Kheista, K., Juni, B., Gulo, S., Rhemrev, E. A., & Christie, M. (2023). *Analisis Perlindungan Data Pribadi terkait UU No. 27 Tahun 2022*. *1*(3), 147–148. https://journal.untar.ac.id/index.php/JSSH/article/view/28615/17126

Suari, K. R. A., & Sarjana, I. M. (2024). *Menjaga Privasi di Era Digital:Perlindungan DataPribadi di Indonesia*. *1*. https://journal.undiknas.ac.id/index.php/JAH/article/view/4484/1337

Tommy, S., Irwan, M., & Nasution, P. (2025). *EVALUASI MANAJEMEN RISIKO KEAMANAN SIBER PADA INFRASTRUKTUR DIGITAL PEMERINTAH : STUDI KASUS PUSAT DATA NASIONAL (PDN) Prodi Manajemen , Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Sumatera Utara I . Pendahuluan Dalam era transformasi dig*. *04*(01), 1–26. https://jurnalgrahakirana.ac.id/index.php/JMEB/article/view/104/73#