Desentralisasi : Jurnal Hukum, Kebijakan Publik, dan Pemerintahan
Volume. 2 Nomor. 3 Agustus 2025
e-ISSN: 3063-2803; p-ISSN: 3063-279X, Hal. 247-262
DOI: https://doi.org/10.62383/desentralisasi.v2i3.940
Available online at: https://ejournal.appihi.or.id/index.php/Desentralisasi

Perlindungan Hukum terhadap Subjek Data Kebocoran Data oleh Badan Publik Menurut UU Nomor 27 Tahun 2022

Nabiha Khansa Rusyda[1*], Kukuh Tejomurti[2]
[1-2] Universitas Sebelas Maret, Indonesia
Email : nabihakhansarusyda@student.uns.ac.id [1], kukuhmurtifhuns@staff.uns.ac.id [2]

Alamat: Jalan Ir. Sutami 36 Kentingan, Jebres, Surakarta, Jawa Tengah, Indonesia 57126
Korespondensi penulis: nabihakhansarusyda@student.uns.ac.id *

***Abstract**. This study aims to analyze the legal protection of personal data subjects in the case of the 2024 data breach at the Temporary National Data Center (PDNS) managed by the Ministry of Communication and Informatics (Kominfo), based on Law Number 27 of 2022 on Personal Data Protection. The research employs a normative juridical method with a case study approach and statutory analysis. Legal materials are obtained from primary and secondary sources using literature research techniques. The findings reveal that Kominfo, as a public body and personal data controller, has not fully fulfilled its obligations to protect personal data as mandated by the law, as reflected in weak security systems, lack of transparency, and slow response to the breach incident. This study highlights the urgent need for the establishment of implementing regulations and an independent supervisory institution to ensure the effective protection of personal data for the public in Indonesia.*

***Keywords**: Legal Protection, Public Body, Data Breach, Kominfo, Personal Data Protection Law*.

Abstrak. Penelitian ini mempunyai tujuan untuk menganalisis perlindungan hukum terhadap subjek data pribadi dalam kasus kebocoran data Pusat Data Nasional Sementara (PDNS) oleh Kementerian Komunikasi dan Informatika (Kominfo) tahun 2024 berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Penelitian ini memakai metode yuridis normatif dengan pendekatan studi kasus dan analisis peraturan perundang-undangan. Bahan hukum yang diperoleh dari bahan hukum primer dan sekunder dengan teknik pengumpulan studi kepustakaan (*literature research*). Hasil penelitian menunjukkan bahwa Kominfo sebagai badan publik dan pengendali data pribadi belum sepenuhnya memenuhi kewajiban perlindungan data sebagaimana diatur dalam UU PDP, yang tercermin dari lemahnya sistem keamanan, kurangnya transparansi, serta lambatnya penanganan insiden kebocoran. Penelitian ini menegaskan pentingnya pembentukan peraturan pelaksana pemerintah dan lembaga pengawas independen guna menjamin efektivitas perlindungan data pribadi masyarakat di Indonesia.

Kata kunci: Perlindungan Hukum, Badan Publik, Kebocoran Data, Kominfo, UU PDP.

1. LATAR BELAKANG

Di era digital yang senantiasa dengan cepat, data pribadi sudah dijadikan aset yang teramat berharga. Informasi pribadi misalnya nama, alamat, nomor telepon, dan preferensi pribadi kita kini dikumpulkan, dimanfaatkan, bahkan diperdagangkan oleh beragam entitas, mulai dari perusahaan teknologi besar, lembaga keuangan sampaiaplikasi yang ada di ponsel. Meskipun kemudahan mengakses data pribadi membawa banyak keuntungan, perihal ini turut memunculkan risiko tinggi terhadap pengamanan serta privasi setiap orang. Jika data pribadi bocor, dampaknya bisa sangat serius, seperti pencurian identitas, penipuan keuangan, bahkan ancaman atas keamanan negara. Sebab itu, melindungi data pribadi kini menjadi pembicaraan yang krusial di era digital. Perlindungan hukum atas data pribadi juga sangat dibutuhkan agar

Received: Mei 14, 2025; Revised: Mei 29, 2025; Accepted: Juni 25, 2025; Online Available: Juli 02 2025

ada kejelasan keterhubungan hukum antar yang mengendalikan data pribadi serta subjek data. Selain itu, aturan ini dapat mendorong pengendali data pribadi untuk lebih berhati-hati dalam menjaga data yang mereka miliki. (Bayu Satrio & Wih Widiatno, 2020).

Setiap warga negara di Indonesia punya beragam hal dasar yang terjamin oleh undang-undang. Negara juga punya tanggung jawab guna melindungi seluruh warganya, seperti yang tertulis di Pembukaan UUD 1945. Satu dari banyak hak penting yang tertera dalam UUD 1945 ialah hak atas perlindungan diri, yang tercantum dalam Pasal 28 G Ayat (1). Hak ini mencakup perlindungan data serta identitas pribadi individu, misalnya Kartu Tanda Penduduk (KTP), Surat Izin Mengemudi (SIM), paspor, serta data sensitif lainnya (Mamonto, 2022). Di era digital seperti sekarang, menjaga data pribadi jadi makin penting agar kebebasan individu tetap terjaga dan data tidak disalahgunakan. Perlindungan data pribadi di dunia digital makin mendesak bersamaan dengan naiknya tingkat penggunaan internet serta teknologi. Sayangnya, cukup banyak individu yang kurang menyadari atas krusialnya menjaga data pribadinya, sehingga data tersebut mudah diselewengkan oleh beragam pihak yang tidak bertanggung jawab. Data yang tersimpan di internet bisa dengan midahnya diakses dan digunakan untuk hal-hal yang merugikan. Sebab itu, perlindungan hukum yang ketat sangat dibutuhkan agar data pribadi konsumen tetap aman dan tidak disalahgunakan.

Undang-Undang Nomor 27 Tahun 2022 mengatur mengenai Perlindungan Data Pribadi (setelahnya disebut UU PDP) yang mempunyai tujuan memberi perlindungan hukum yang lebih kuat bagi individu berkenaan pengumpulan, penggunaan, serta penyebaran data pribadi mereka. Undang-undang ini turut menyoroti mekanisme pengawasan serta penegakan hukum lewat terbentuknya lembaga pengawas independen. UU PDP di Indonesia dirancang guna memberi perlindungan hukum bagi subjek data pribadi. UU ini mengatur berbagai hal terkait pengumpulan, pengolahan, dan pemanfaatan data pribadi oleh pengendali data. Selain itu, UU PDP memutuskan sanksi tegas bagi pengendali data yang tidak menaati hak privasi subjek data sebagai bentuk penegakan hukum. UU ini juga memberi hak kepada subjek data guna mengontrol informasi pribadi tiap individu, sehingga mereka memiliki otoritas penuh atas data tersebut.

Menilik data dari Databoks, pada kuartal III tahun 2022, Indonesia menempati posisi ketiga sebagai negara dengan akumulasi kasus kebocoran data paling banyak di dunia. Pada periode tersebut, termuat sejumlah 12.742.031 data akun di Indonesia telah alami kebocoran. Jumlah ini sangat besar dan menjadi perhatian serius bagi negara. Dalam artikel ini akan membahas mengenai permasalahan kebocoran data Pusat Data Nasional Sementara (selanjutnya disebut PDNS) yang berada dibawah Kominfo dalam hal ini badan publik sebagai

pengendali data pribadi. Pemerintah kurang memperhatikan permasalahan kebocoran data pribadi di Indonesia yang dibuktikan dengan terulangnya kembali insiden peratasan terhadap situs pemerintah PDNS pada tanggal 20 Juni 2024.

Direktur Jenderal Aplikasi Informatika Kominfo, Samuel Abrijani Pangerapan, menginformasikan bahwa serangan siber yang terjadi telah berdampak pada data dari 210 instansi pemerintahan pusat dan daerah (Ardipandanto, 2024), termasuk layanan keimigrasian di seluruh bandara internasional Indonesia. Akibatnya, layanan pembuatan paspor mengalami gangguan, contohnya di Kantor Imigrasi Kelas I Khusus non-TPI Jakarta Barat, di mana waktu membuat paspor yang biasanya 3-4 hari menjadi 7-8 hari. Namun, sejak pagi 24 Juni 2024, sistem layanan publik Direktorat Jenderal Imigrasi mulai membaik, seperti layanan visa on arrival. Selain itu, data milik Badan Intelijen Strategis (BAIS) TNI dan Indonesia *Automatic Fingerprint Identification System* (Inafis) POLRI turut terdampak serangan tersebut. Serangan ini berupa *ransomware* yang dikenal sebagai *Brain Chipper*, varian terbaru dari *Lockbit* 3.0, yang menyebabkan gangguan besar pada PDNS di Surabaya. Sebanyak 282 instansi pemerintah terdampak, dengan 239 instansi mengalami gangguan layanan publik tanpa *backup* data, sementara 43 instansi lainnya mengalami gangguan namun memiliki backup sehingga bisa segera pulih. Pemerintah menilai masalah utama adalah tata kelola dan kurangnya pencadangan data secara rutin sesuai dengan peraturan keamanan pusat data nasional. Akun penyerang yang menamai dirinya MoonzHaxor dikatakan sudah memuat unggahan kiriman penjualan data Inafis POLRI di harga 1000 sampai 7000 dollar AS. Gangguan turut dirasakan Sistem Informasi Manajemen Sistem Penyediaan Air Minum (SIMSPAM) dan Sistem Informasi Infrastruktur Sanitasi Kementerian Pekerjaan Umum dan Perumahan Rakyat, juga Sistem Informasi Pengelolaan Keuangan Daerah Kementerian Dalam Negeri (Sukman, 2024).

Pusat Data Nasional (PDN) adalah inisiatif yang dikerjakan oleh Kementerian Komunikasi dan Informatika (Kominfo) Indonesia guna mengintegrasikan serta mengelola data dari berbagai instansi pemerintah secara terpusat. Tujuan utama dari pembangunan PDN adalah untuk meningkatkan efisiensi, keamanan, dan interoperabilitas data pemerintah, serta mendukung implementasi kebijakan berbasis data. Langkah ini sejalan dengan transformasi digital yang sedang digalakkan oleh pemerintah Indonesia untuk memajukan pelayanan publik dan pengambilan keputusan berbasis data. Pada Juli 2024, terjadi kebocoran data pada PDNS dan data tersebut diposting dan dijual di situs "*Breach Forums*" oleh akun bernama "aptikakominfo". Informasi yang bocor mencakup Nama, Nomor Induk Kependudukan (NIK), Rekening Bank, NPWP, dan Nomor Rekening, serta data pribadi lainnya. Data ini dijual dengan harga USD 121,000, menimbulkan kekhawatiran serius terkait privasi dan keamanan

bagi para individu yang informasinya terungkap. Insiden ini menyoroti kebutuhan mendesak akan peningkatan keamanan siber dan perlindungan data di Indonesia. Kebocoran ini melibatkan jutaan data pribadi yang bisa dipakai guna tujuan kriminal, menunjukkan perlunya peningkatan sistem hukum perlindungan data. Didasarkan Pasal 12 ayat (1) UU PDP, setiap subjek data pribadi punya hak guna melaksanakan penggugatan serta mendapat ganti rugi apabila terjadi perihal yang melanggar selama data pribadi yang subjek miliki diproses. Berdasarkan isu-isu tersebut penulis merasa hal ini menarik diteliti berkenaan keterhubungan hukum serta tanggung jawab badan publik sebagai pengendali data pribadi atas bocornya data pribadi yang terjadi.

2. KAJIAN TEORITIS

A. Teori Perlindungan Hukum

Untuk mencapai keseimbangan atau keadilan dalam hukum, perlindungan hukum berarti hukum diharuskan menyambung serta menyelaraskan semua kepentingan masyarakat, juga memberi batasan atas kepentingan beberapa pihak lain. Persetujuan ataupun kesepakatan keseluruhan elemen masyarakat guna mengatur keseluruhan kaitan serta perilaku antar anggota masyarakat sertaantar masyarakat dengan pemerintah menyebabkan terjadinya perlindungan hukum (Raharjo, 2000). R. La Porta dalam Jurnal of Financial Economics menyampaikan bahwasanya, perlindungan hukum mempunyai dua sifat utama, yakni sifat pencegahan serta sifat hukuman. Wujud perlindungan yang paling konkret terlihat melalui institusi penegak hukum misalnya kepolisian, kejaksaan, pengadilan, erta lembaga sejenis lainnya. Institusi-institusi ini berperan penting dalam mencegah pelanggaran hukum sekaligus memberikan sanksi bagi pelaku pelanggaran.

Phillipus M. Hadjon membagi 2 (dua) jenis perlindungan hukum, meliputi:

1. Perlindungan Hukum Preventif

   Perlindungan yang diberi oleh pemerintah disertai tujuan pencegahan sebelum munculnya pelanggaran.

2. Perlindungan Hukum Represif

   Perlindungan hukum yang represif punya tujuan yakni penyelesaian atas sengketa. Penanganan perlindungan hukum oleh Pengadilan Umum serta Pengadilan Administrasi di Indonesia tergolong kategori perlindungan hukum ini.

Undang-Undang Perlindungan Data Pribadi memberi hak kepada individu guna mengakses, memperbaiki, serta menghapus data pribadi mereka selaras dengan Pasal 8 UU PDP. Jikalau ada pelanggaran yang dilaksanakan oleh pengendali data pribadi baik secara

administratif ataupun pidana dapat dikenai sanksi berupa denda, penjara, atau penghentian pemrosesan data. Hal ini bertujuan untuk mendorong kepatuhan terhadap regulasi dan melindungi hak-hak individu di Indonesia.

B. Teori Data Pribadi

Data merupakan informasi yang tercatat dalam satu wujud yang bisa terproses lewat peralatan-peralatan yang berfungsi lewat cara yang otomatis menanggapi beragam instruksi yang diberi bagi tujuan tersebut.Data yang isinya informasi yang tersimpan pada sebuah komputer ataupun pada media penyimpanan komputer seperti disk-diskmagnetis. Suatu database merupakan kumpulan data komputer, sebagai contoh, suatu daftar nama dan alamat klien atau suatu daftar pegawai dan rincian-rincian mengenai diri mereka,yang disimpan pada sebuah file komputer. Suatu database biasanya dioperasikan lewat penggunaan sebuah program komputer untuk akses serta menggerakan data yang dimuat didalamnya. Secara umum, data adalah kumpulan fakta atau rincian berkenaan satu kejadian yang masih mentah serta belum dilaksanakan pengolahan. Data merupakan hasil yang didapat langsung dari lapangan tanpa disertai proses mengolah sebelumnya. Data ini berisi informasi yang berkaitan dengan kehidupan seseorang dan bisa dikenali dari informasi lain yang dipunya oleh pemakai data. Informasi ini juga mencakup pendapat atas individu tersebut, namun tidak termasuk keseluruhan indikasi tas keinginan pemakai data terkait individu itu. Subjek dari data ini adalah individu yang masih hidup, yang dikenal sebagai data pribadi. Data pribadi sendiri ialah informasi tentang seseorang yang tersimpan, terkelola, serta terlindungi kerahasiaannya.

Definisi data pribadi dikutip dari Kamus Besar Bahasa Indonesia ialah informasi yang mencakup karakteristik yang konkret dan akurat, yang bisa digunakan sebagai fondasi untuk menganalisis suatu hal tertentu. Istilah "pribadi" merujuk pada individu dalam konteks yang lebih sempit, yaitu sebagai individu atau diri sendiri. Dengan adanya UU PDP diharapkan kedepannya data pribadi setiap individu dapat dilindungi secara lebih efisien dan mencegah timbulnya kasus seperti kebocoran data pribadi terutama di era yang serba digital saat ini. Berdasar Pasal 1 Ayat (1) UU PDP , "data pribadi" mengacu pada data individu yang sudah teridentifikasi ataupun bisa diidentifikasi lewat cara terpisah ataupun dipadukan bersama informasi lainnya melalui sistem elektronik atau no-nelektronik. Dengan demikian, perlindungan data pribadi mencakup keseluruhan usaha guna melindungi data pribadi sepanjang proses pemrosesan hingga hak konstitusional Subjek Data Pribadi (yang memiliki data pribadi) dilindungi.

C. Teori Badan Publik

Badan publik adalah sebuah lembaga yang menjalankan fungsi pemerintahan atau memberikan pelayanan kepada masyarakat, dan dananya berasal dari anggaran negara, baik dari pemerintah pusat maupun daerah. Dalam hukum Indonesia, definisi badan publik dijelaskan dalam Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP). Pasal 1 Ayat (3) UU KIP menyatakan bahwasanya badan publik meliputi lembaga eksekutif, legislatif, yudikatif, serta lembaga lain yang tugas utamanya berhubungan dengan penyelenggaraan negara. Dana untuk badan-badan ini sebagian ataupun keseluruhannya bersumber dari Anggaran Pendapatan dan Belanja Negara (APBN) ataupun Anggaran Pendapatan dan Belanja Daerah (APBD). Di samping itu, organisasi non-pemerintah yang dananya sebagian ataupun seluruhnya bersumber dari anggaran tersebut, sumbangan masyarakat, ataupun bantuan dari luar negeri turut tergolong dalam kategori badan publik."Badan publik di Indonesia didasarkan Undang-Undang No.14 Tahun 2008, terbagi menjadi beberapa kategori yaitu :

1. Badan Publik Negara, seperti kementerian, lembaga tinggi negara, dan pemerintah daerah.
2. Badan Publik Non-Negara, misalnya organisasi masyarakat, lembaga swadaya masyarakat (LSM), serta yayasan yang menerima dana dari APBN/APBD atau masyarakat.

Pembagian ini memperluas cakupan transparansi dan akuntabilitas tidak hanya pada institusi pemerintahan formal tetapi juga entitas non-pemerintah yang mendapat dukungan dana publik.

Pasal 1 ayat (4) Undang-Undang Nomor 27 Tahun 2022 berkenaan Perlindungan Data Pribadi menetapkan bahwasanya, badan publik termasuk dalam kategori pengendali data pribadi, dan mereka bertanggung jawab untuk menentukan tujuan dan mengawasi pemrosesan data. Institusi pemerintah seperti lembaga eksekutif, legislatif, yudikatif, dan lainnya yang memproses data pribadi untuk kepentingan umum atau tujuan negara termasuk dalam kategori badan publik yang mengendalikan data. Salah satu contohnya adalah kasus PDNS 2024 di mana Kominfo bertanggung jawab atas kebocoran data yang disebabkan oleh kelalaian dalam pengelolaan sistem.

Beberapa kewajiban badan publik sebagai pengendali data pribadi selaras dengan UU PDP yaitu :

1. Wajib mempunyai dasar hukum pemrosesan data sesuai dengan Pasal 20 UU PDP yaitu persetujuan subjek data atas pemenuhan kewajiban hukum (misalnya pelayanan KTP, BPJS)
2. Wajib menjaga keamanan data pribadi subjek data sesuai dengan pasal 35 UU PDP yaitu Badan publik wajib menerapkan langkah teknis (enkripsi, autentikasi) dan administratif (SOP, audit) untuk melindungi data.
3. Wajib Transparansi dan Akurasi sesuai dengan Pasal 27-29 bahwa pemrosesan data harus terbatas, spesifik, dan transparan serta wajib memastikan data akurat sebelum diproses.

Dalam UU PDP juga dimuat mengenai badan publik sebagai pengendali data pribadi, memiliki pengecualian dan batasan atau dengan kata lain badan publik dapat mengabaikan kewajiban dalam kondisi khusus yaitu apabila ada kondisi kepentingan negara seperti keamanan nasional, pertahanan dan penyidikan hukum atau pengawasan sektor strategis seperti sistem keuangan atau moneter.

3. METODE PENELITIAN

Jenis penelitian yang dipakai ketika penelitian ini yakni penelitian hukum normatif. Dalam penyusunan skripsi ini menggunakan penelitian bersifat preskriptif. Penelitian bersifat preskriptif dalam ilmu hukum berarti bahwa objek kajiannya adalah kesesuaian atau koherensi antar norma hukum serta prinsip hukum, juga antar aturan hukum serta norma hukum itu sendiri. Selain itu, penelitian ini juga mengkaji kesesuaian antara perilaku atau tindakan seseorang dengan norma hukum yang berjalan. Dalam konteks jurnal ini, penulis menelaah kesesuaian aturan hukum perlindungan data pribadi dalam UU PDP dengan praktik pengelolaan data pribadi oleh Kominfo selakubadan publik, khususnya terkait kasus kebocoran data PDNS tahun 2024 dan memberikan saran atau rekomendasi berkenaanapa yang selayaknya dilaksanakan dalam mengatasi permasalahan hukum yang muncul. Pendekatan yang dipakai dalam penelitian ini ialah pendekatan undang-undang tepatnya UU No.27 Tahun 2022 berkenaan Perlindungan Data Pribadi.

4. HASIL DAN PEMBAHASAN

PDNS ialah infrastruktur sementara yang dibangun guna penyimpanan serta pengelolaan data dari beagam instansi pemerintah sebelum Pusat Data Nasional (PDN) utama berjalan seutuhnya. Melansir data kominfo, PDNS tersebar di tiga wilayah. Proyek ini dioperasikan oleh dua operator telekomunikasi meliputi PT Telkom (TLKM) serta Indosat (ISAT). Detailnya, Indosat lewat PT Lintasarta menjalankan satu PDNS di Serpong. Sementara itu, PT Telkom (TLM) menjalankan pusat data di Surabaya dan serta cold site di Batam (Ira, 2024). Tujuan utama PDNS ialah untuk menaikkan tingkat efisiensi serta integrasi data antar instansi pemerintah, memberi dukungan atas tata kelola data yang lebih baik, juga mempersingkat transformasi digital di sektor publik. Pada 20 Juni 2024, server PDNS menemui gangguan sebab serangan *ransomware*, yang mengakibatkan terganggunya berbagai layanan publik, termasuk layanan keimigrasian. Permasalahan ini awalnya dilapor oleh penyedia layanan PDNS 2, sehingga lekas membutuhkan koordinasi antara Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), dan penyedia layanan terkait guna menangani masalah tersebut. Berikut kronologi kebocoran data secara rinci (Anastasya, 2024) :

Tabel 1. Kronologi Kebocoran Data PDNS Tahun 2024

Tanggal & Waktu	Aktivitas
17 Juni 2024, 23:15 WIB	Usaha pertama dengan menangguhkan fitur keamanan *Windows Defender* yang bisa membuat komputer lebih rentan atas serangan *malware* seperti *ransomware*
18 Juni 2024, 03:21 WIB	Serangan *ransomware* tahap pertama terlihat lewat bertambahnya akun pengguna baru pada sistem.
19 Juni 2024, 22:18 WIB	Serangan memasuki proses infiltrasi di mana penyerang mendapatkan akses awal dengan mencuri kredensial dan memanfaatkan celah keamanan
20 Juni 2024, 00:54 WIB	Fitur *directory backup* ditangguhkan oleh pengguna baru yang sudah bisa memasuki sistem
20 Juni 2024, 00:57 WIB	*Ransomware* setelahnya dioperasikan pada perangkat backup di PDN, melaksanakan enkripsi data substansial yang disimpan
20 Juni 2024	Pelaku meminta uang penebusan sejumlah USD 8 juta sebagai syarat pemulihan akses data yang sudah dikunci
23 Juni 2024	Serangan ini bermula dengan memperlihatkan dampak pada gangguan layanan publik, termasuk layanan imigrasi serta kesehatan
27 Juni 2024	Sejumlah lembaga yang terkena dampak sudah bisa mengembalikan layanan mereka secara berangsur

Serangan *ransomware* yang menimpa PDNS berdampak besar pada sekitar 282 instansi pemerintah, namun hanya 44 instansi yang berhasil terselamatkan. Gangguan ini menyebabkan layanan publik penting misalnya kesehatan, imigrasi, dan pendidikan terganggu. Misalnya, akses data pasien di rumah sakit tertunda sehingga perawatan menjadi terlambat. Layanan imigrasi seperti *autogate*, visa, izin tinggal, M-Paspor, sertacekal online juga mengalami gangguan. Sebagai solusi sementara, operasional layanan imigrasi berpindah ke *Amazon Web Service* (AWS). Di sektor pendidikan, sejumlah 800 ribu data pendaftar Kartu Indonesia Pintar (KIP) terdampak, sehingga pengumuman penerima KIP-K yang harusnya terlaksana pada 1 Juli 2024 harus ditangguhkan. Serangan ini juga menimbulkan kerugian finansial diperkirakan menyentuh angka miliaran rupiah, meliputi biaya pemulihan sistem, hilangnya pendapatan sebab layanan terganggu, juga potensi denda sebab melanggar perlindungan data. Selain itu, data pribadi warga negara, termasuk informasi kesehatan dserta keuangan, berisiko bocor, yang menurunkan kepercayaan publik terhadap pemerintah. Insiden ini menunjukkan lemahnya pengamanan data pemerintah dan menjadi peringatan penting untuk meningkatkan keamanan siber di sektor publik.

A. Kedudukan dan Kewajiban Badan Publik sebagai Pengendali Data Pribadi

Pemerintah Indonesia mengeluarkan UU PDP untuk menjamin perlindungan data pribadi warga negara. Regulasi ini menyatukan berbagai aturan perlindungan data yang sebelumnya tersebar menjadi satu payung hukum, sehingga diharapkan pelaksanaan perlindungan data pribadi menjadi lebih efektif dan efisien. Dalam UU PDP, data pribadi dibagi atas dua kategori utama: data pribadi spesifik, yang meliputi informasi sensitif misalnya data kesehatan, biometrik, genetika, catatan kriminal, data anak-anak, serta data keuangan; juga data pribadi umum, yang meliputi informasi misalnya nama lengkap, jenis kelamin, kewarganegaraan, agama, dan status perkawinan. Pembagian ini membantu dalam menentukan tingkat perlindungan yang sesuai bagi setiap jenis data. Dalam undang-undang ini, subjek data pribadi memiliki hak guna mengetahui tujuan pemrosesan data pribadi, mempunyai hak untuk perbaikan atas kesalahan yang hadir pada diri mereka sendiri, dan hak untuk mendapat ganti rugi atas pelanggaran pemrosesan data pribadi. Pihak yang menangani data pribadi terdiri dari dua kategori: pengendali data pribadi (yang menentukan tujuan serta mengelola data) serta prosesor data pribadi (yang memproses data untuk pengendali yang ditunjuk). Pihak dalam kategori ini termasuk orang, badan publik, serta organisasi internasional. Tidak hanya diperlukan persetujuan jelas dari pihak yang menangani data pribadi, pemrosesan data juga dapat dilakukan mengikuti wewenang yang diberikan oleh perundang-undangan sebagai rangka pelayanan publik. Dengan kata lain badan publik (yang utamanya bertanggung jawab

atas pengelolaan negara) memiliki otoritas untuk melakukan pemrosesan data sesuai dengan wewenang yang diberikan oleh perundang-undangan.

Unsur pengendali data pribadi dalam UU PDP dapat ditemukan dalam Pasal 1 ayat (4) yang menyebutkan bahwa "Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri atau bersama-sama dalam menentukan tujuan dan melakukan pengendalian terhadap pemrosesan Data Pribadi". Pertama, terkait unsur "setiap orang". Selanjutnya, jika merujuk kembali pada unsur (kriteria) pengendali data pribadi lainnya dalam Pasal 1 Ayat (4) UU PDP disebutkan bahwasanya pengendali data pribadi "bertindak sendiri atau bersama-sama dalam menetapkan tujuan dan melakukan pengendalian terhadap pemrosesan Data Pribadi". Perihal ini menunjukkan bahwa pengendali data pribadi saat penentuan tujuan pemrosesan serta pelaksanaan pengendalian atas pemrosesan bisa terlaksana secara individual ataupun bersamaan (terdiri atas dua orang ataupun lebih pengendali data pribadi serta seterusnya).

Dalam buku yang berjudul *Cyber Law*: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional, pengendali data pribadi diartikan selaku entitas yang melaksanakan pengelolaan data pribadi. Pengelolaan yang dimaksud juga diartikan sebagai suatu kegiatan atau serangkaian kegiatan, baik melalui pemanfaatan teknologi pengolahan data lewat cara otomatis ataupun manual, yang dilakukan lewat cara terstruktur maupun memanfaatkan sistem penyimpanan data, yang selanjutnya dilakukan terhadap data pribadi, termasuk (tetapi tidak terbatas pada) pengolahan, pengumpulan, penggunaan, pengungkapan, penyebaran, serta pengamanan data pribadi (Rosadi, 2022). Definisi pengendali data pribadi sebagaimana dirumuskan dalam Naskah Akademik RUU PDP sama dengan definisi yang terdapat dalam naskah-naskah sebelumnya, meskipun frasa "pengelola data pribadi" masih digunakan dalam naskah tersebut. Menurut Naskah Akademik RUU PDP, "orang atau badan hukum, badan usaha, lembaga penyelenggara negara, badan publik, atau organisasi kemasyarakatan lainnya" dianggap sebagai pengelola data pribadi. (Halaman 134, Naskah Akademik RUU PDP). Pengendali data pribadi pada hakikatnya juga melakukan pengawasan terhadap data pribadi, yang didefinisikan sebagai "kegiatan atau serangkaian kegiatan yang dilakukan terhadap data pribadi, baik dengan menggunakan alat bantu pengolahan data secara otomatis maupun manual, secara terstruktur, maupun dengan menggunakan sistem penyimpanan data, termasuk tetapi tidak terbatas pada pengumpulan, penggunaan, pengungkapan, penyebarluasan, dan pengamanan data pribadi" dalam Naskah Akademik RUU PDP. (Halaman 136, Naskah Akademik RUU PDP).

Kebocoran data yang terjadi saat itu sudah menandakan adanya kekacauan dalam pengelolaan *cyber security system* yang dimiliki oleh Indonesia. Sebuah server yang penting seharusnya dilengkapi dengan kepemilikan sandi yang kuat untuk mengamankan data di dalamnya. Namun, pengelola PDN terlihat tidak profesional karena pembuatan serta penggunaan sandi secara sembarangan yakni berupa "Admin#1234". Dalam kasus ini, Kominfo selaku pengendali data pribadi berkewajiban agar menentukan alasan pemrosesan data, tujuan pemrosesan, juga metode yang dipakai guna mencapai tujuan tersebut. Pengendali data pribadi wajibmempertimbangkan risiko ketika mereka memproses data, hal ini terutama berlaku ketika mereka menangani data dalam volume besar. Untuk menjaga keamanan, pengendali harus membuat serta mengaplikasikan prosedur teknis guna memberi perlindungan atas data yang diawasi. Data pribadi yang dikelola oleh pengendali harus dilindungi dari pemrosesan yang tidak sah. Kominfo juga harus mencegah orang yang tidak seharusnya mengaksesnya untuk melakukan tindakan ilegal. Penerapan regulasi yang ketat sesuai dengan UU PDP Pasal 46 apabila terjadi kegagalan dalam Perlindungan Data Pribadi maka pengendali data pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada subjek data pribadi dan lembaga. Kominfo sebagai badan publik yang merupakan pengendali data pribadi atas kasus ini wajib menyampaikan informasi kepada masyarakat yang didalamnya harus mencakup data pribadi yang diungkap, kapan, serta bagaimana data pribadi yang diungkap, juga usaha penanganan disertai pemulihan atas kebocoran data pribadi PDNS Tahun 2024 yang berada dibawah Kominfo.

B. Perlindungan Hukum bagi Subjek Data dalam Kasus Kebocoran Data oleh Badan Publik

Hak Subjek Data dalam UU PDP berasal dari hak atas privasi (*right to privacy)* yang konsep awalnya dicetuskan oleh S.Warren dan L. Brandheis pada 1980 (Anjas, 2020). Privasi ialah hak tiap individu agar merasakan hidup serta dibiarkan sendiri dalam artian tidak terganggu kehidupan pribadinya, baik oleh orang lain maupun oleh negara. Hak privasi membutuhkan pengakuan hukum seiring berkembangnya zaman diperlukan juga perkembangan hukum aturan tentang hak privasi ini (Sekaring, 2021). Hubungan antara privasi serta perlindungan data pribadi ialah hak bagi individu, kelompok, maupun institusi guna menentukan kapan, bagaimana, serta sampai sejauh apa mereka mau membagikan informasi mengenai diri mereka kepada orang lain, ataupun bahkan memutuskan apakah mereka nantinya memberikan informasi tersebut pada pihak lain sama sekali. Dengan kata lain, privasi memberikan kendali penuh atas informasi pribadi yang dimiliki. (Sinta, 2018).

Hak subjek data dalam UU PDP meliputi berbagai hak penting yang bertujuan memberi perlindungan serta kontrol atas data pribadi yang mereka punyai. Berbagai hak tersebut meliputi: hak agar mendapat informasi yang jelas berkenaan identitas pengendali data, dasar kepentingan hukum, tujuan permintaan serta penggunaan data pribadi, juga akuntabilitas pihak yang mengelola data (Pasal 5 UU PDP). Subjek data juga mempunyai hak untuk melengkapi, memperbarui, ataupun memperbaiki data pribadi yang tidak akurat (Pasal 6 UU PDP), serta mendapat akses juga salinan data pribadi mereka secara gratis mengikuti ketentuan (Pasal 7 UU PDP). Selain itu, mereka dapat mengakhiri pemrosesan, menghapus, serta memusnahkan data pribadi yang dimiliki oleh pengendali data (Pasal 8 UU PDP), menarik kembali persetujuan pemrosesan data, mengajukan keberatan terhadap pengambilan keputusan otomatis, serta menunda ataupun membatasi pemrosesan data secara proporsional. Subjek data juga punya hak untuk menggugat serta menerima ganti rugi atas pelanggaran pemrosesan data pribadi (Pasal 12 UU PDP). Untuk mengajukan berbagai hak tersebut, subjek data dapat mengajukan permohonan langsung kepada pengendali data pribadi yang bersangkutan dengan menyertakan identitas diri yang jelas. Pengendali data wajib menanggapi permohonan tersebut dalam jangka waktu yang diatur oleh UU PDP. Selain itu, UU ini mengatur kewajiban pengendali dan prosesor data pribadi dalam menjaga keamanan dan kerahasiaan data, serta menyediakan mekanisme penyelesaian sengketa baik sanksi administratif maupun pidana apabila terjadi pelanggaran, sehingga memberikan jaminan perlindungan hukum yang efektif bagi subjek data (Pasal 57 dan Pasal 67 UU PDP). Mekanisme ini menjamin bahwa hak subjek data dapat ditegakkan secara efektif sesuai ketentuan hukum yang berlaku.

Philip M. Hadjon menyampaikan bahwasanya perlindungan hukum berarti menjaga harkat dan martabat juga mengakui hak asasi manusia yang dipunya oleh subjek hukum. Perlindungan ini diberi berdasar atas ketentuan hukum yang diberlakukan, baik sebagai bentuk kekuasaan yang sah maupun sebagai kumpulan aturan atau pun norma yang fungsinya guna melindungi sesuatu dari gangguan atau ancaman lainnya (Philipus, 2007). Dalam teori perlindungan hukum menurut Phillipus M. Hadjon, dibedakan 2 (dua) jenis perlindungan hukum, yakni :

a. Perlindungan Hukum Preventif

Perlindungan preventif ialah tindakan guna mencegah terjadinya pelanggaran hukum yang akan menimbulkan sengketa. Analisis perlindungan hukum preventif yang seharusnya dilaksanakan dalam kasus ini:

1) Penerapan Sistem Keamanan yang Andal dan Bertanggung Jawab

Dalam Pasal 39 ayat (2) UU PDP, pengendali data pribadi wajib melaksanakan pencegahan data pribadi diakses secara tidak sah lewat penggunaan sistem keamanan yang andal, aman, serta bertanggung jawab. Upaya preventif ini mencakup penggunaan enkripsi, firewall, sistem deteksi intrusi, dan pembaruan perangkat lunak secara berkala untuk mencegah kebocoran data. Dalam kasus ini, server PDNS diketahui tidak memenuhi persyaratan ISO 22301 (Salsabilla, 2025).

2) Pembentukan Peraturan Pemerintah Pelaksana UU

Dalam 10 Pasal UU PDP disebutkan bahwasanya ketentuan lebih lanjut akan diatur dalam Peraturan Pemerintah. Dengan adanya peraturan tersebut, UU akan lebih mudah dipahami implementasinya dikarenakan dalam UU umumnya masih bersifat umum dan belum dapat diterapkan secara teknis serta tidak adanya pedoman operasional yang jelas bagi para pelaksana di lapangan. Hal ini dapat menimbulkan ketidakpastian hukum, tumpang tindih kebijakan, serta lemahnya pengawasan dan penegakan sanksi terhadap pelanggaran, seperti dalam kasus perlindungan data pribadi di Indonesia.

3) Pembentukan Lembaga Perlindungan Data Pribadi

Dalam Bab IX Kelembagaan UU PDP disebutkan bahwa perlu dibentuknya suatu lembaga untuk melaksanakan pengawasan terhadap perlindungan data pribadi dan untuk keperluan penegakan hukum terhadap pelanggaran UU PDP. Lembaga ini mempunyai lima belas kewenangan dalam penyelenggaraan perlindungan data pribadi yang secara garis besar meliputi perumusan serta penetapan kebijakan dan strategi perlindungan data pribadi, pengawasan penyelenggaraan perlindungan data pribadi, penegakan hukum administratif, serta fasilitasi penyelesaian sengketa di luar pengadilan (Kukuh, 2025). Jangkauan perlindungan data pribadi dalam hukum pelindungan data mencakup beberapa aspek utama, yaitu definisi serta jenis data pribadi, beragam prinsip pelindungan data, kewajiban pengendali serta prosesor data, beragam hak pemilik data, serta pengawasan dan penegakan hukum yang didukung oleh keberadaan lembaga independen (Djafar, 2019).

b. Perlindungan Hukum Represif

Perlindungan represif mempunyai tujuan guna menyelesaikan sengketa. Analisis perlindungan hukum represif yang seharusnya dilaksanakan dalam kasus ini :

1) Transparansi atas kasus yang terjadi

Badan publik wajib segera memberitahukan kepada subjek data dan masyarakat jika terjadi kebocoran data, sesuai dengan ketentuan UU PDP Pasal 46 Ayat (1) yang berbunyi "Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada: subjek data pribadi dan lembaga."

2) Penegakan Sanksi

Pengendali data pribadi yang melakukan kegagalan dalam melindungi data subjek data pribadi sesuai dengan Bab VIII Sanksi Administratif dan Bab XIV Ketentuan Pidana, wajib dijatuhi sanksi sesuai dengan ketentuan UU PDP.

Dalam UU PDP, belum diatur secara eksplisit mengenai ketentuan yang memberikan hak untuk menggugat subjek data pribadi apabila terjadi kelalaian pemrosesan data oleh pengendali data pribadi, undang-undang belum secara eksplisit menetapkan bahwasanya pengendali data pribadi bertanggung jawab atas pembuktian atau tanggung jawab mutlak, sehingga jika terjadi insiden siber, pengendali data pribadi dapat dinyatakan bertanggung jawab secara keseluruhan, tidak hanya untuk pemulihan data tetapi juga untuk hal-hal berikut. Terkait kasus kebocoran data PDNS Kominfo pada tahun 2024, subjek data secara langsung yaitu masyarakat memiliki hak untuk menggugat pengendali data pribadi yaitu Kominfo. Namun, pada praktiknya belum ada aturan secara jelas bagaimana proses penuntutan atas kasus yang terjadi.

5. KESIMPULAN DAN SARAN

Didasarkan hasil penelitian, bisa didapat simpulan bahwasanya badan publik memiliki kedudukan yang penting sebagai pengendali data pribadi, yang menuntut tanggung jawab penuh dalam menjamin keamanan, kerahasiaan, dan integritas data pribadi yang dikelolanya mengikuti ketentuan perundang-undangan. Namun, dalam kasus kebocoran data oleh badan publik seperti yang terjadi pada Kominfo, ditemukan bahwa kewajiban perlindungan data pribadi tidak terlaksana secara sempurna, baik dari sisi sistem pengamanan, transparansi, maupun penanganan insiden. Perlindungan hukum bagi subjek data dalam kasus tersebut secara normatif telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, namun implementasinya di lapangan senantiasa menemui beragam hambatan, seperti keterlambatan penanganan, kurangnya pengawasan, dan belum adanya peraturan pelaksana yang memadai. Sebab itu, penulis merekomendasikan agar pemerintah segera menerbitkan peraturan pelaksana yang jelas, memperkuat pengawasan, serta

membentuk lembaga pengawas independen untuk memastikan efektivitas perlindungan data pribadi.

DAFTAR REFERENSI

Anjas Putra Pramudito. (2022). Kedudukan dan perlindungan hak atas privasi di Indonesia. Jurist Diction, (4).

Ardianto, D. (2020). Kebocoran data di Indonesia dan implikasinya terhadap privasi warga negara. Jurnal Hukum dan Teknologi, 12(3), 145–162.

Bayu Satrio, M., & Widiatno, M. W. (2020). Perlindungan hukum terhadap data pribadi dalam media elektronik (analisis kasus kebocoran data pengguna Facebook di Indonesia). Journal Civitas Academica of Law Esa Unggul University, 1(1).

Djafar, W. (2019). Hukum perlindungan data pribadi di Indonesia: Lanskap, urgensi dan kebutuhan pembaruan. Dalam Seminar Hukum dalam Era Analisis Big Data, Program Pascasarjana Fakultas Hukum UGM (Vol. 26).

Ira. (2024). Kilas balik pusat data nasional: Dibangun dengan utang, kini diserang. Katadata.co.id. https://katadata.co.id/berita/nasional/667e4993acbe1/kilas-balik-pusat-data-nasional-dibangun-dengan-utang-kini-diserang (Diakses: 27 Juni 2024, pukul 00.20)

Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. Jurnal Al Wasath, 2(1).

Mamonto, D. F. (2022). Analisis perlindungan hukum terhadap penyalahgunaan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022. E-Journal UNSTRAT.

Mardiasmo. (2019). Perpajakan (Edisi Terbaru 2018). Penerbit Andi.

Naskah Akademik Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP).Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Philipus, M. H. (2007). Perlindungan hukum bagi rakyat di Indonesia (Edisi Khusus, Cetakan Pertama). Peradaban.

Rosadi, S. D. (2022). Cyber law: Aspek data privasi menurut hukum internasional, regional dan nasional. Refika Aditama.

Rosadio, S. D. (2018). Perlindungan privasi dan data pribadi dalam era ekonomi digital di Indonesia. Fakultas Hukum Universitas Padjadjaran.

Salsabilla. (2025). Mengenal proyek pusat data nasional. Tempo.co. https://www.tempo.co/hukum/mengenal-proyek-pusat-data-nasional-1544987 (Diakses: 13 Maret 2025, pukul 13.01)

Simorangkir, A., Sihombing, H., Sihite, P. I., & Parhusip, J. (2024). Ransomware pada data PDN: Implikasi etis dan tanggung jawab profesional dalam pengelolaan keamanan siber. Jurnal Sains Student Research.

Sukman, R. D. (2024). Kebocoran data nasional sebanyak 210 instansi kena bobol. Binus University: School of Information System. https://sis.binus.ac.id/2024/11/12/kebocoran-data-nasional-sebanyak-210-instansi-kena-bobol/ (Diakses: 14 Maret 2025)

Tejomurti, K. (2025). Menanti otoritas perlindungan data pribadi.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G Ayat (1) tentang hak perlindungan pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.