Laporan Analisis: Krisis Kedaulatan Digital Indonesia di Balik Insiden Pusat Data Nasional

Ringkasan Eksekutif: Insiden PDN sebagai Gejala Kerentanan Sistemik

Serangan siber pada Pusat Data Nasional Sementara (PDNS) Indonesia pada Juni 2024 merupakan titik balik yang krusial, namun bukan merupakan peristiwa yang terisolasi. Laporan ini menyintesis temuan yang menunjukkan bahwa insiden tersebut adalah konsekuensi yang dapat diprediksi dari kegagalan sistemik yang mengakar dalam tata kelola digital Indonesia. Serangan yang dilakukan oleh kelompok ransomware Brain Cipher/Lockbit 3.0 ini melumpuhkan ratusan layanan publik, mulai dari imigrasi hingga pendidikan, dan mengekspos kerentanan mendalam pada infrastruktur teknis, manajemen sumber daya manusia (SDM), dan kebijakan strategis.

Meskipun pemerintah telah merespons dengan kebijakan baru dan narasi publik tentang akuntabilitas, terdapat kesenjangan kritis antara peraturan yang ada dan implementasinya yang efektif. Undang-Undang Perlindungan Data Pribadi (UU PDP), meskipun merupakan langkah legislatif yang signifikan, terhambat oleh mekanisme penegakan hukum yang lemah, kurangnya independensi kelembagaan, dan janji yang belum terpenuhi untuk membentuk badan pengawas khusus. Kegagalan Indonesia bukanlah karena ketiadaan kerangka hukum, melainkan ketidakmampuan untuk menerjemahkan undang-undang di atas kertas menjadi perlindungan yang efektif dan terlembaga dalam praktik. Laporan ini mengemukakan perlunya pergeseran paradigma fundamental dari manajemen krisis yang reaktif menjadi pendekatan yang proaktif dan terintegrasi dari seluruh elemen pemerintahan untuk membangun ketahanan digital dan kedaulatan data.

1. Pendahuluan: Serangan Pusat Data Nasional sebagai

Titik Krusial

1.1. Latar Belakang dan Signifikansi

Pusat Data Nasional (PDN) memegang peran sentral dalam ekosistem digital strategis Indonesia. Sebagai tulang punggung untuk mengonsolidasikan data dan layanan pemerintah, integritasnya sangat penting untuk kedaulatan digital nasional. Peran ini menjadikan PDN target utama bagi para pelaku kejahatan siber, di mana setiap gangguan dapat memiliki dampak yang luas dan merusak kepercayaan publik serta reputasi negara.

1.2. Insiden Juni 2024: Tinjauan Awal

Pada tanggal 20 Juni 2024, PDNS 2 diserang oleh siber, yang menyebabkan gangguan langsung dan meluas pada layanan publik yang vital.[1] Layanan imigrasi dan permohonan visa menjadi terhambat, menciptakan antrean panjang di bandara dan kantor imigrasi.[3] Insiden ini menjadi studi kasus utama dalam laporan ini untuk menganalisis kerentanan yang mendasari dan implikasi yang lebih luas bagi keamanan siber Indonesia.

1.3. Ruang Lingkup dan Tujuan Laporan

Laporan ini menyediakan analisis komprehensif dan multidimensi terhadap insiden PDN. Laporan ini akan menguji penyebab teknis dan manusia, konsekuensinya yang meluas, konteksnya dalam sejarah peretasan sektor publik, dan yang paling penting, implikasinya terhadap kerangka hukum dan regulasi Indonesia untuk perlindungan data.

2. Anatomi Peretasan: Kronologi dan Akar Masalah Insiden PDN

Bagian ini secara cermat merekonstruksi peristiwa serangan PDN, melampaui narasi publik untuk mengungkap kegagalan teknis dan manusia yang mendasarinya.

2.1. Kronologi Serangan: Dari Infiltrasi hingga Manajemen Krisis

Insiden ini dimulai pada 17 Juni 2024, ketika fitur keamanan Windows Defender dinonaktifkan secara sengaja, yang menciptakan celah kerentanan kritis.[1] Pada tanggal 20 Juni 2024, pukul 00.54 WIB, aktivitas berbahaya dimulai, termasuk instalasi file berbahaya, penghapusan

filesystem penting, dan penonaktifan layanan yang sedang berjalan. Aktivitas ini memuncak dengan *crash*-nya Windows Defender pada pukul 00.55 WIB, yang menandai awal dari serangan.[1] Serangan ini menggunakan varian ransomware yang disebut Brain Cipher, yang merupakan pengembangan terbaru dari kelompok ransomware Lockbit 3.0.[4] Serangan tersebut berdampak pada 210 instansi pemerintah pusat dan daerah.[6]

Pemerintah, melalui Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN), mengonfirmasi serangan pada 24 Juni.[1] Para pelaku meminta tebusan sebesar 8 juta dolar AS atau sekitar Rp131,2 miliar.[6] Namun, dalam perkembangan yang tidak terduga, kelompok peretas Brain Cipher mengeluarkan pernyataan publik pada 3 Juli, di mana mereka meminta maaf kepada masyarakat Indonesia dan menyediakan kunci dekripsi secara gratis.[8] Mereka mengklaim bahwa serangan tersebut adalah "pentest" dengan pembayaran pasca-peretasan dan bahwa mereka menyediakan kunci tersebut tanpa intervensi dari layanan khusus atau lembaga hukum.[12]

2.2. Akar Masalah: Kegagalan Faktor Teknis dan Manusia

Investigasi menunjukkan bahwa penyebab utama insiden ini adalah kombinasi dari kegagalan teknis dan kelalaian manusia.

- **Kegagalan Berpusat pada Manusia:**
  - **Kelalaian Kata Sandi:** Penyebab utama serangan adalah kelalaian pengguna dalam menggunakan kata sandi, yang menciptakan kerentanan serius.[11] Menurut seorang pakar keamanan siber, penggunaan kata sandi yang lemah oleh pengelola PDN menunjukkan "kurangnya profesionalisme".[13]
  - **Literasi dan Kesadaran Digital yang Rendah:** Para ahli dari CISSReC dan UGM

secara konsisten menyoroti rendahnya kesadaran dan ketersediaan SDM yang berkualitas sebagai akar penyebab kerentanan dalam sistem pemerintah.[5] Kelemahan pada unsur manusia ini dapat membuat sistem keamanan yang paling canggih sekalipun menjadi tidak efektif.

- **Kelemahan Operasional dan Sistemik:**
  - **Ketiadaan Kebijakan Cadangan Data (Backup) yang Wajib:** Salah satu temuan yang paling krusial adalah bahwa hanya 2% data di PDNS-2 yang dicadangkan.[13] Hal ini disebabkan oleh kebijakan cadangan data yang bersifat "opsional" dan kurangnya anggaran di berbagai instansi pemerintah.[13] Sebagai respons, pemerintah telah berjanji untuk membuat kebijakan cadangan data menjadi wajib.[11]
  - **Arsitektur IT yang Rentan:** Penggunaan sistem operasi (OS) yang populer dan "rentan" seperti Windows juga menuai kritik, dengan beberapa ahli menyarankan Linux sebagai alternatif yang lebih aman.[9] Pernyataan kelompok peretas bahwa data tersebut "mudah dibongkar dan dienkripsi" semakin memperkuat temuan kerentanan sistemik ini.[17]

2.3. Analisis yang Lebih Mendalam

Serangan PDN bukanlah serangan acak dari peretas yang sangat terampil yang mengeksploitasi kerentanan yang tidak diketahui. Sebaliknya, serangan ini adalah kasus klasik dari serangkaian peristiwa kausal. Rendahnya literasi digital dan kesadaran keamanan siber di kalangan staf pemerintah [5] menyebabkan kelalaian kata sandi [11], yang pada gilirannya memberikan titik masuk bagi ransomware.[1] Ketiadaan sistem cadangan data yang wajib [13] kemudian memperparah dampaknya, memastikan bahwa kerugian data hampir total dan pemulihannya membutuhkan waktu yang lama. Rangkaian peristiwa ini menunjukkan bahwa kerentanan yang paling signifikan bukanlah pada teknologi, melainkan berakar pada kegagalan manusia dan institusi.

Pernyataan publik pemerintah, yang sangat berfokus pada "kelalaian satu pengguna" dan janji untuk mengambil tindakan hukum [11], berfungsi untuk mengalihkan pertanggungjawaban dari kegagalan sistemik dan institusional yang memungkinkan satu titik kegagalan melumpuhkan sistem nasional. Sistem yang benar-benar tangguh seharusnya memiliki keamanan berlapis dan menerapkan kebijakan

zero trust [18] yang dapat memitigasi dampak dari kesalahan satu orang. Dengan menunjuk satu individu, pemerintah menghindari refleksi diri yang lebih dalam dan tidak nyaman tentang kesiapan, alokasi sumber daya, dan tata kelolanya sendiri.

Keputusan kelompok Brain Cipher untuk meminta maaf dan menyediakan kunci dekripsi

secara gratis sangat tidak biasa dalam dunia ransomware. Tindakan ini tidak seharusnya dipandang sebagai tindakan altruisme. Sebaliknya, hal ini dapat menjadi langkah strategis untuk mempermalukan pemerintah Indonesia di panggung global, menunjukkan postur keamanannya yang lemah. Pernyataan para peretas, "Kami berharap serangan kami membuat Anda jelas tentang betapa pentingnya mendanai industri dan merekrut spesialis yang berkualitas" [12], menempatkan serangan tersebut sebagai pelajaran hukuman daripada sekadar usaha finansial murni. Hal ini juga menciptakan preseden berbahaya, karena dapat mendorong kelompok lain untuk menyerang target pemerintah demi keuntungan ideologis atau reputasi, bukan hanya finansial. Fakta bahwa PDN dianggap "mudah untuk dibongkar" [17] memperkuat motivasi ini, menunjukkan bahwa serangan tersebut oportunistik dan berupaya rendah.

Tabel 1: Kronologi dan Kegagalan Teknis Insiden PDN

Tanggal & Waktu	Peristiwa Kunci dan Temuan	Penyebab/Keterangan	Sumber Referensi
17 Juni 2024, 23.15 WIB	Windows Defender dinonaktifkan	Upaya penonaktifan fitur keamanan yang memungkinkan aktivitas berbahaya berjalan	[1]
20 Juni 2024, 00.54 WIB	Aktivitas berbahaya dimulai	Instalasi file berbahaya, penghapusan *filesystem* penting, penonaktifan layanan	[1]
20 Juni 2024, 00.55 WIB	Windows Defender *crash* dan tidak dapat beroperasi	Titik puncak serangan, menandakan keberhasilan ransomware	[1]
20 Juni 2024	Gangguan pada layanan publik, termasuk imigrasi,	Dampak langsung dari serangan ransomware Brain	[2]

	PPDB, dan lainnya	Cipher yang mengunci data	
24 Juni 2024	Konfirmasi resmi oleh BSSN	Insiden diungkapkan sebagai serangan siber jenis ransomware Brain Cipher/Lockbit 3.0	[1]
27 Juni 2024	Rapat DPR: Terungkap 98% data tidak dicadangkan	Kurangnya kepatuhan terhadap Peraturan BSSN Nomor 4 Tahun 2021 yang mewajibkan cadangan data	[13]
1 Juli 2024	Menkopolhukam mengumumkan penyebabnya adalah kelalaian kata sandi	Hasil forensik menunjukkan kelalaian satu pengguna sebagai titik masuk serangan	[11]
3 Juli 2024	Kelompok peretas memberikan kunci dekripsi secara gratis	Tindakan tidak biasa yang diklaim sebagai 'pentest' untuk memberi pelajaran kepada pemerintah	[11]

3. Rangkaian Konsekuensi: Gangguan, Ketidakpercayaan, dan Dampak Ekonomi

Bagian ini merinci dampak luas dari insiden PDN, mulai dari kekacauan langsung hingga erosi

jangka panjang terhadap kepercayaan publik dan ekonomi.

3.1. Gangguan Layanan Publik yang Kritis

Serangan tersebut menyebabkan lumpuhnya ratusan layanan publik yang vital.[6] Layanan utama yang terpengaruh termasuk imigrasi dan pemrosesan paspor di bandara-bandara besar [2], proses Penerimaan Peserta Didik Baru (PPDB) di beberapa daerah [2], serta 47 domain layanan di bawah Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi.[19] Pemerintah telah berupaya memulihkan layanan ini dengan memindahkannya ke

cold site cadangan di Batam.[13]

3.2. Erosi Kepercayaan Publik

Insiden ini secara mendalam mengguncang kepercayaan masyarakat terhadap kemampuan pemerintah untuk melindungi data sensitif.[4] Masyarakat merasa bahwa data mereka telah jatuh ke tangan peretas.[21] Perasaan ini bukan hal baru; peretasan sebelumnya, seperti kebocoran data BPJS Kesehatan pada tahun 2021 yang berdampak pada 279 juta warga [22], telah menciptakan skeptisisme yang meluas.[25] Insiden PDN semakin memperburuk ketidakpercayaan ini, yang berpotensi menyebabkan resistensi publik terhadap inisiatif pemerintah digital di masa depan.[25]

3.3. Dampak Ekonomi dan Reputasi

Serangan ini menimbulkan beban finansial yang signifikan, termasuk biaya pemulihan data dan sistem, kerugian akibat gangguan operasional, dan potensi pembayaran tebusan yang tidak jadi dilakukan.[4] Pada tingkat makro, insiden ini merusak reputasi Indonesia di kancah internasional. Hal ini dapat membuat negara menjadi "kurang menarik bagi investor asing" [8], terutama mereka yang bergerak di industri teknologi, yang membutuhkan keamanan data yang kuat untuk beroperasi. Peristiwa ini dapat merusak investasi besar, seperti rencana investasi Microsoft sebesar 2,3 miliar dolar Kanada untuk mengembangkan infrastruktur

cloud dan kecerdasan buatan.[8]

3.4. Analisis Lebih Mendalam

PDN dirancang untuk memusatkan data pemerintah demi efisiensi yang lebih besar dan kebijakan "satu data". Namun, insiden ini mengungkap kerapuhan yang melekat pada model ini. Meskipun sentralisasi menawarkan efisiensi, hal ini juga menciptakan satu target tunggal yang sangat bernilai bagi para penjahat siber. Serangan yang berhasil pada pusat data ini memiliki dampak berantai yang sangat besar di seluruh ekosistem layanan publik.[2] Kondisi ini menyoroti kegagalan strategis yang krusial karena tidak menerapkan protokol cadangan dan pemulihan data yang berlapis dan terdesentralisasi sejak awal.

Kepercayaan publik adalah mata uang fundamental dari sebuah ekonomi digital. Ketika warga kehilangan kepercayaan bahwa pemerintah dapat melindungi data mereka, mereka menjadi ragu untuk berpartisipasi dalam layanan digital, seperti aplikasi kesehatan atau sistem rekam medis elektronik.[25] Defisit kepercayaan ini dapat menghambat keberhasilan inisiatif digitalisasi pemerintah dan pada akhirnya memperlambat pembangunan ekonomi dan sosial negara.

4. Konteks Historis: Memahami Pola Peretasan Sektor Publik

Insiden PDN bukanlah anomali, melainkan sebuah titik data dalam tren yang mengkhawatirkan. Bagian ini menghubungkan serangan PDN dengan sejarah peretasan data di sektor publik dan swasta untuk menunjukkan pola kerentanan sistemik yang jelas.

4.1. Kronologi Peretasan (2020-2024)

Peretasan data telah menjadi masalah yang berulang di Indonesia, yang memengaruhi entitas swasta maupun pemerintah.

- **Tokopedia (2020):** Kebocoran 91 juta data pengguna.[7]
- **BPJS Kesehatan (2021):** Kebocoran 279 juta data warga, termasuk informasi medis sensitif.[22] Kerugiannya diperkirakan mencapai Rp600 triliun.[24]

- **BSI (2023):** Serangan ransomware oleh kelompok Lockbit 3.0, menyebabkan total penutupan layanan perbankan dan pencurian data nasabah.[6]
- **Instansi Pemerintah Lainnya (2024):** INAFIS dan Badan Intelijen Strategis Tentara Nasional Indonesia diretas secara berurutan pada Juni 2024.[8] Peretas Bjorka juga mengklaim telah membobol Direktorat Jenderal Pajak.[7]

4.2. Pola Berulang dan Kerentanan Bersama

Banyak dari serangan tersebut, termasuk BSI dan PDN, menggunakan ransomware, dengan tujuan tidak hanya mengenkripsi data tetapi juga mengeksfiltrasi data untuk dijual di *dark web*.[4] Faktor manusia terbukti menjadi titik lemah yang berulang, seperti terlihat pada peretasan situs web BKN oleh seorang guru honorer yang mencuri dan menjual data [7], dan insiden BSI, di mana laptop seorang karyawan terinfeksi malware.[7]

Sifat berulang dari insiden-insiden ini menunjukkan pendekatan yang reaktif, bukan proaktif, terhadap keamanan siber. Ketiadaan badan pusat yang independen untuk menegakkan standar dan melakukan audit di seluruh instansi memperburuk masalah ini.

4.3. Analisis Lebih Mendalam

Meskipun serangan-serangan awal menargetkan entitas sektor swasta seperti Tokopedia, serangan yang lebih baru dan berdampak besar telah bergeser ke infrastruktur pemerintah yang kritis (PDN, BKN, INAFIS) dan entitas milik negara (BSI). Peningkatan target ini menunjukkan bahwa lanskap ancaman semakin matang dan memiliki motivasi yang lebih politis atau strategis. Para penjahat siber kini secara langsung menantang kemampuan negara untuk melindungi data yang paling penting dan mempertahankan kendali atas layanan publik. Hal ini merupakan serangan langsung terhadap kedaulatan digital, bukan hanya kejahatan finansial.

Sejarah panjang peretasan data juga menunjukkan bahwa lanskap hukum yang terfragmentasi sebelum UU PDP sama sekali tidak memadai untuk mencegah penjahat siber atau menyediakan kerangka kerja yang jelas untuk akuntabilitas.[26] Kurangnya undang-undang yang terpadu dan komprehensif membuat sulit untuk menetapkan tanggung jawab yang jelas dan menegakkan standar, yang memungkinkan kerentanan terus berlanjut tanpa pengawasan.

Tabel 2: Insiden Kebocoran Data Utama di Indonesia (2020-2024)

Entitas yang Terkena Dampak	Tanggal/Tahun	Jenis Serangan	Kelompok Peretas (jika diketahui)	Jumlah Data yang Terkena Dampak	Implikasi
Tokopedia	2020	Data Exfiltration	Tidak diketahui	91 juta data pengguna	Data dijual di *dark web*
BPJS Kesehatan	2021	Data Exfiltration	Tidak diketahui	279 juta data warga	Data medis sensitif bocor, kerugian diperkirakan Rp600 triliun
Bank Syariah Indonesia (BSI)	Mei 2023	Ransomware	Lockbit 3.0	Data nasabah dan karyawan	Layanan perbankan lumpuh, data dijual di *dark web*
Direktorat Jenderal Pajak	2024	Data Exfiltration	Bjorka	6 juta NPWP	Data sensitif dijual, klaim DJP tidak terverifikasi
Badan Kepegawaian Negara (BKN)	2024	SQL Injection	Kontrak Guru (internal)	6,3 GB data pegawai negeri	Data dijual untuk keuntungan ekonomi
Pusat Data Nasional Sementara (PDNS)	Juni 2024	Ransomware	Brain Cipher/Lockbit 3.0	210 instansi pemerintah, sebagian besar data hilang	Layanan publik lumpuh, kerugian finansial, reputasi negara

5. Kekacauan Hukum dan Regulasi: Tinjauan Kritis Kerangka Perlindungan Data Indonesia

Bagian ini secara langsung menjawab pertanyaan inti pengguna dengan menganalisis kerangka hukum perlindungan data Indonesia. Argumentasinya adalah bahwa meskipun undang-undang sudah ada, "kesenjangan implementasi" yang kritis membuatnya tidak efektif.

5.1. Undang-Undang Perlindungan Data Pribadi (UU PDP): Langkah Maju yang Penting?

Undang-Undang Nomor 27 Tahun 2022 disahkan pada 17 Oktober 2022 dan mulai berlaku penuh pada 17 Oktober 2024.[29] Tujuan undang-undang ini adalah untuk menciptakan kerangka hukum yang kuat guna melindungi data pribadi, memberikan individu kendali atas informasi mereka, dan menetapkan tanggung jawab yang jelas bagi pengendali data.[29] Undang-undang ini melarang pengumpulan, pengungkapan, penggunaan, dan pemalsuan data yang tidak sah.[29] UU PDP juga menetapkan sanksi administratif (hingga 2% dari pendapatan tahunan) dan sanksi pidana, termasuk hukuman penjara dan denda yang besar untuk pelanggaran serius.[22]

5.2. Kesenjangan Implementasi: Janji Lembaga PDP yang Belum Terwujud

Salah satu ketentuan utama dari UU PDP adalah pembentukan Lembaga Pengawas Perlindungan Data Pribadi (PDP) yang independen.[29] Lembaga ini seharusnya menjadi "regulator, fasilitator penyelesaian sengketa, dan penegak".[29] Namun, meskipun target pembentukannya pada kuartal ketiga tahun 2024 [36] dan tenggat waktu penegakan penuh pada Oktober 2024 [30], lembaga tersebut masih belum terbentuk hingga Maret 2025.[38] Sementara itu, fungsinya dikelola sementara oleh Kementerian Komunikasi dan Informatika (Kominfo).[37]

5.3. Analisis Komparatif: UU PDP vs. Standar Global (GDPR)

UU PDP memiliki prinsip-prinsip dasar yang sama dengan *General Data Protection Regulation* (GDPR) Uni Eropa, seperti persetujuan dan hak-hak subjek data.[30] Namun, kelemahan signifikan masih ada. UU PDP "kurang berkembang dalam hal detail prosedural, kesiapan institusional, dan penegakan hukum".[39] Undang-undang ini memiliki denda yang lebih rendah [22], pendekatan yang kurang ketat terhadap akuntabilitas [39], dan tidak memiliki jangkauan ekstrateritorial yang luas dan orientasi "

privacy by design" seperti GDPR.[39] Kelemahan hukum yang signifikan adalah tidak adanya prinsip persetujuan untuk transfer data ke yurisdiksi asing.[40]

5.4. Hak Korban dan Ketiadaan Proses Hukum

UU PDP memberikan hak untuk menuntut ganti rugi atas kerugian akibat kebocoran data.[41] Namun, meskipun ketentuan ini ada, Peraturan Pemerintah (PP) yang diperlukan untuk merinci proses ganti rugi belum dikeluarkan, yang menciptakan "kekosongan hukum" di mana korban memiliki hak di atas kertas tetapi tidak memiliki prosedur yang jelas untuk menggunakannya.[41] Hal ini menyulitkan korban untuk mencari restitusi atau kompensasi atas kerugian yang mereka alami.

5.5. Analisis Lebih Mendalam

Pertanyaan pengguna tentang "hukum yang tidak jelas" sebagian tidak tepat. Indonesia kini memiliki undang-undang perlindungan data yang spesifik dan menyeluruh.[29] Kegagalan yang sesungguhnya adalah kegagalan institusional. Undang-undang hanya sekuat mekanisme penegakannya. Kegagalan untuk membentuk Lembaga PDP independen seperti yang diatur oleh undang-undang [38] berarti bahwa kementerian yang bertanggung jawab atas PDN, Kominfo, juga merupakan regulator dan penegak hukum sementara.[37] Hal ini menciptakan konflik kepentingan yang fundamental dan berbahaya, di mana penjaga data yang diretas juga bertanggung jawab untuk menyelidiki dan memberikan sanksi atas peretasan tersebut. Cacat

struktural ini membahayakan seluruh kerangka akuntabilitas.

Tabel 3: Analisis Komparatif UU PDP Indonesia vs. GDPR Uni Eropa

Aspek	UU Perlindungan Data Pribadi (UU PDP) Indonesia	General Data Protection Regulation (GDPR) Uni Eropa
Kerangka Hukum	UU No. 27 Tahun 2022	Peraturan (EU) 2016/679
Tujuan Filsafat	Berpusat pada negara, perlindungan individu, dan kepentingan publik	Berpusat pada bisnis, menyeimbangkan pertumbuhan ekonomi digital dan inovasi
Kewenangan Lembaga Pengawas	Belum terbentuk, sementara dikelola oleh Kominfo	Lembaga perlindungan data nasional yang independen sudah terbentuk dan berfungsi
Sanksi Administratif	Maksimal 2% dari pendapatan tahunan	Maksimal €20 juta atau 4% dari pendapatan global tahunan (mana yang lebih tinggi)
Prinsip Utama	Persetujuan adalah basis hukum utama dan satu-satunya dalam sebagian besar kasus	Persetujuan, transparansi, tujuan yang jelas, minimisasi data, dan akuntabilitas
Jangkauan Ekstrateritorial	Diatur dalam UU, tetapi penerapan terhadap transfer data lintas batas masih lemah	Berlaku untuk pemrosesan data penduduk UE di mana pun perusahaan berada
Hak Subjek Data	Hak untuk mengakses, mengoreksi, menghapus, dan menarik persetujuan	Hak yang sama ditambah hak atas portabilitas data dan hak untuk menolak pembuatan profil otomatis

Akuntabilitas	Disebutkan secara umum tanpa mewajibkan struktur tata kelola komprehensif	Diperlakukan secara ketat, mewajibkan organisasi untuk menunjukkan kepatuhan

6. Jalan Menuju Ketahanan: Rekomendasi Komprehensif untuk Masa Depan Digital yang Aman

Bagian terakhir ini memberikan rekomendasi yang dapat ditindaklanjuti, beralih dari insiden spesifik ke reformasi kebijakan yang luas dan jangka panjang.

6.1. Tindakan Teknis dan Operasional yang Mendesak

Pemerintah harus segera memberlakukan Peraturan Menteri (Permen) yang baru [16] yang membuat cadangan data menjadi wajib bagi semua instansi pemerintah.[11] Hal ini harus disertai dengan penerapan sistem klasifikasi data bertingkat (strategis, terbatas, terbuka) untuk menerapkan protokol keamanan dan cadangan yang berbeda untuk setiap tingkatan.[13] Selain itu, pergeseran dari pendekatan reaktif ke model keamanan

zero trust yang proaktif sangat krusial.[18] Ini termasuk penerapan otentikasi multi-faktor, penggunaan sistem operasi yang lebih aman [14], dan investasi pada teknologi deteksi ancaman tingkat lanjut.

6.2. Reformasi Kebijakan dan Tata Kelola

Langkah paling penting untuk membangun kembali kepercayaan publik adalah segera membentuk Lembaga PDP yang independen.[22] Lembaga ini harus diberdayakan untuk bertindak secara otonom dalam menegakkan undang-undang dan memastikan akuntabilitas. Pemerintah juga harus meminta pertanggungjawaban pejabat senior atas kegagalan sistemik, bukan hanya menyalahkan karyawan individu atas kesalahan manusia.[8] Penunjukan pemimpin yang profesional dengan keahlian teknis pada peran teknologi kunci di pemerintahan juga

penting.[14] Selain itu, pemerintah harus mewajibkan pelatihan literasi siber dan kebersihan digital yang berkelanjutan bagi seluruh pegawai pemerintah.[5]

6.3. Transformasi Hukum dan Budaya

Pemerintah harus memprioritaskan penyusunan dan penerbitan Peraturan Pemerintah (PP) yang merinci prosedur kompensasi bagi korban, seperti yang diamanatkan oleh UU PDP.[41] Peraturan ini akan mengisi "kekosongan hukum" yang ada dan memberikan jalan yang jelas bagi para korban untuk mencari keadilan. Terakhir, sangat penting untuk menumbuhkan budaya kesadaran keamanan siber nasional, dengan menekankan bahwa perlindungan data adalah tanggung jawab bersama antara pemerintah, entitas swasta, dan individu warga negara.[9]

7. Kesimpulan: Dari Langkah Reaktif ke Kedaulatan Proaktif

Insiden PDN adalah pelajaran yang nyata dan menyakitkan. Hal ini jelas mencerminkan bahwa infrastruktur dan tata kelola digital Indonesia belum siap menghadapi tantangan era digital. "Kegagalan" yang diidentifikasi oleh pengguna bukanlah kurangnya usaha, melainkan kesenjangan kritis antara ambisi (undang-undang data yang baru, kebijakan satu data) dan kerja mendasar untuk membangun institusi dan penegakan hukum. Untuk benar-benar mencapai kedaulatan digital, Indonesia harus melampaui sikap reaktif, mengatasi kerentanan sistemiknya di tingkat tata kelola, dan memprioritaskan reformasi institusional dan hukum yang diperlukan untuk membangun kembali kepercayaan publik.

Karya yang dikutip

1. BSSN Identifikasi Pusat Data Nasional Sementara Diserang ..., diakses Agustus 16, 2025, https://kominfo.lhokseumawekota.go.id/berita/read/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware-20240705172015016 5
2. Menyoal Gangguan PDN yang Sampai Pengaruhi Layanan Publik - Investor Daily, diakses Agustus 16, 2025, https://investor.id/business/364895/menyoal-gangguan-pdn-yang-sampai-pengaruhi-layanan-publik
3. PDN Kena Serangan Ransomware, Ini Dampak yang Mulai Masyarakat Rasakan -

Info Komputer, diakses Agustus 16, 2025, https://infokomputer.grid.id/read/124111990/pdn-kena-serangan-ransomware-ini-dampak-yang-mulai-masyarakat-rasakan
4. Ransomware pada Data PDN: Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber - Kampus Akademik, diakses Agustus 16, 2025, https://ejurnal.kampusakademik.co.id/index.php/jssr/article/download/2966/2725/12198
5. Insiden Peretasan PDNS 2, Pakar Sorot Kualitas SDM Indonesia, diakses Agustus 16, 2025, https://www.cnnindonesia.com/teknologi/20240626110919-192-1114286/insiden-peretasan-pdns-2-pakar-sorot-kualitas-sdm-indonesia
6. Mengenal Ransomware Lockbit 3.0 yang menyerang Pusat Data Nasional Sementara (PDNS) - BPIP-CSIRT, diakses Agustus 16, 2025, https://csirt.bpip.go.id/posts/mengenal-ransomware-lockbit-3-0-yang-menyerang-pusat-data-nasional-sementara-pdns
7. 15 Kasus Cyber Crime di Indonesia Tahun 2024 - Edavos, diakses Agustus 16, 2025, https://edavos.com/kasus-cyber-crime/
8. Indonesian Government Under Fire Following String of Cyber Breaches, diakses Agustus 16, 2025, https://www.asiapacific.ca/publication/indonesian-government-under-fire-after-cyber-breaches
9. Kominfo Klaim Hacker PDNS Belum Ancam Bocorkan Data Warga - CNN Indonesia, diakses Agustus 16, 2025, https://www.cnnindonesia.com/teknologi/20240626165502-192-1114496/kominfo-klaim-hacker-pdns-belum-ancam-bocorkan-data-warga
10. Kominfo Tanggapi Serangan Ransomware Terhadap ... - RRI.co.id, diakses Agustus 16, 2025, https://www.rri.co.id/nasional/786996/kominfo-tanggapi-serangan-ransomware-terhadap-pdns-dua
11. Hacker group gives decryption key to Indonesian Government to restore national data centre, diakses Agustus 16, 2025, https://govinsider.asia/intl-id/article/hacker-group-gives-decryption-key-to-indonesian-government-to-restore-national-data-centre
12. Hackers Who Brought Down an Entire Country's Infrastructure with Ransomware Say Sorry and Release Keys for Free - Bitdefender, diakses Agustus 16, 2025, https://www.bitdefender.com/en-us/blog/hotforsecurity/hackers-who-brought-down-an-entire-countrys-infrastructure-with-ransomware-say-sorry-and-release-keys-for-free
13. Terungkap, pusat data nasional diserang gara-gara kelalaian ..., diakses Agustus 16, 2025, https://govinsider.asia/indo-en/article/terungkap-pusat-data-nasional-diserang-gara-gara-kelalaian-password
14. 4 Penyebab PDNS Bisa Diserang Hacker, Pakar UM Surabaya: Kurangnya Literasi Digital, diakses Agustus 16, 2025,

https://www.detik.com/edu/edutainment/d-7417243/4-penyebab-pdns-bisa-diserang-hacker-pakar-um-surabaya-kurangnya-literasi-digital
15. Kominfo Ungkap Alasan Pusat Data Nasional Hanya Back up 2% - Katadata, diakses Agustus 16, 2025, https://katadata.co.id/berita/nasional/667f8ed354568/kominfo-ungkap-alasan-pusat-data-nasional-hanya-back-up-2
16. Permen Baru Soal Wajib Backup Data Akan Ditandatangani Menkominfo Besok - RRI, diakses Agustus 16, 2025, https://www.rri.co.id/nasional/792453/permen-baru-soal-wajib-backup-data-akan-ditandatangani-menkominfo-besok
17. Hacker group gives decryption key to Indonesian Government to restore national data centre, diakses Agustus 16, 2025, https://govinsider.asia/intl-en/article/hacker-group-gives-decryption-key-to-indonesian-government-to-restore-national-data-centre
18. PDN Diserang Siber, Pakar UGM Ungkap Langkah Menjaga ..., diakses Agustus 16, 2025, https://ugm.ac.id/id/berita/pdn-diserang-siber-pakar-ugm-ungkap-langkah-menjaga-keamanan-server/
19. Ini Sejumlah Layanan Publik yang Terganggu akibat Serangan Ransomware di PDN ·, diakses Agustus 16, 2025, https://lampost.co/teknologi/ini-sejumlah-layanan-publik-yang-terganggu-akibat-serangan-ransomware-di-pdn/
20. Kementerian Pendayagunaan Aparatur Negara dan Reformasi ..., diakses Agustus 16, 2025, https://www.menpan.go.id/site/berita-terkini/berita-daerah/menko-polhukam-pastikan-layanan-pdns-2-kembali-normal-bulan-ini
21. Cyber Attack Fallout from PDN: Questioning Government Cybersecurity Priorities - Center for Digital Society, diakses Agustus 16, 2025, https://digitalsociety.id/2024/07/09/cyber-attack-fallout-from-pdn-questioning-government-cybersecurity-priorities/18039/
22. The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era, diakses Agustus 16, 2025, https://journal.stekom.ac.id/index.php/Hakim/article/download/2291/1733/7337
23. Jaminan Informasi dan Keamanan yang Lebih Baik: Studi Kasus BPJS Kesehatan, diakses Agustus 16, 2025, https://journal.fkom.uniku.ac.id/ilkom/article/download/202/62/833
24. Ahli Sebut Kerugian Kebocoran Data Penduduk-BPJS Rp600 T - CNN Indonesia, diakses Agustus 16, 2025, https://www.cnnindonesia.com/teknologi/20210623115637-199-658214/ahli-sebut-kerugian-kebocoran-data-penduduk-bpjs-rp600-t
25. Analisis Dampak Kebocoran Data Kesehatan terhadap Kepercayaan Publik dan Efektivitas Layanan Kesehatan Digital - ResearchGate, diakses Agustus 16, 2025, https://www.researchgate.net/publication/391238276_Analisis_Dampak_Kebocoran_Data_Kesehatan_terhadap_Kepercayaan_Publik_dan_Efektivitas_Layanan_Kesehatan_Digital

26. Personal Data Protection Act and Challenges to Its Implementation, diakses Agustus 16, 2025, https://fia.ui.ac.id/en/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/
27. Komparasi Pengaturan Perlindungan Data Pribadi di Indonesia dan Uni Eropa - Jurnal Hukum Lex Generalis, diakses Agustus 16, 2025, https://ojs.rewangrencang.com/index.php/JHLG/article/download/173/82/779
28. Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia - ResearchGate, diakses Agustus 16, 2025, https://www.researchgate.net/publication/367870969_Personal_Data_Protection_Authority_Comparative_Study_between_Indonesia_United_Kingdom_and_Malaysia
29. Introduction of the Official Personal Data Protection Act (UU PDP ..., diakses Agustus 16, 2025, https://www.bdo.co.id/en-gb/insights/introduction-of-the-official-personal-data-protection-act-(uu-pdp)
30. A Guide to Indonesia Data Privacy Law for Business - Abhitech, diakses Agustus 16, 2025, https://www.abhitech.co.id/blog/employer-of-record/data-privacy-law/
31. Data protection laws in Indonesia - Data Protection Laws of the World, diakses Agustus 16, 2025, https://www.dlapiperdataprotection.com/index.html?t=law&c=ID
32. Navigating the Personal Data Protection Act (UU PDP) - BDO, diakses Agustus 16, 2025, https://www.bdo.co.id/en-gb/insights/navigating-the-personal-data-protection-act-(uu-pdp)
33. EFEKTIVITAS PENERAPAN UU PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI E-COMMERCE: TINJAUAN TERHADAP KEAMANAN KONSUMEN, diakses Agustus 16, 2025, https://jurnalistiqomah.org/index.php/syariah/article/view/3818/2443
34. UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI LAW OF THE REPUBLIC OF INDONESIA NUMBER 27 - ABNR, diakses Agustus 16, 2025, https://www.abnrlaw.com/lib/files/IND-ENG-UU%2027-2022%20Pelindungan%20Data%20Pribadi%20(ABNR).pdf
35. Pertanggungjawaban Hukum Terhadap Kebocoran ... - Lintar - Untar, diakses Agustus 16, 2025, https://lintar.untar.ac.id/repository/penelitian/buktipenelitian_10218003_4A20022 4093322.pdf
36. Pembentukan lembaga pengawas PDP ditargetkan selesai kuartal III 2024 - ANTARA News, diakses Agustus 16, 2025, https://www.antaranews.com/berita/4172616/pembentukan-lembaga-pengawas-pdp-ditargetkan-selesai-kuartal-iii-2024
37. Misterius, Begini Nasib Lembaga Pengawasan Perlindungan Data Pribadi, diakses Agustus 16, 2025, https://www.cnbcindonesia.com/tech/20241114193435-37-588354/misterius-begini-nasib-lembaga-pengawasan-perlindungan-data-pribadi

38. Data Sering Bocor Tak Ada Lembaga Pengawas, Begini Nasib Warga RI - CNBC Indonesia, diakses Agustus 16, 2025, https://www.cnbcindonesia.com/tech/20250317132512-37-619216/data-sering-bocor-tak-ada-lembaga-pengawas-begini-nasib-warga-ri
39. The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR, diakses Agustus 16, 2025, https://ijble.com/index.php/journal/article/download/1178/1043/4474
40. (PDF) Comparative analysis of personal data protection in Indonesia ..., diakses Agustus 16, 2025, https://www.researchgate.net/publication/393525211_Comparative_analysis_of_personal_data_protection_in_Indonesia_and_Singapore_for_a_sustainable_digital_future
41. KEKOSONGAN NORMA HUKUM DALAM ... - OJS Unud, diakses Agustus 16, 2025, https://ojs.unud.ac.id/index.php/kerthasemaya/article/download/99322/54339