

IBLAM LAW REVIEW

P-ISSN

2775-4146

E-ISSN

2775-3174

Volume 6, Nomor 1, 2026

Authors

¹ Laksana Budiwiyo Lie

² Agnes Fitriyantica

Affiliation

IBLAM School of Law

Email

laksana@ieee.org¹

agnesfitriyantica@iblam.ac.id²

Date Published

19 January 2026

DOI

<https://doi.org/10.52249/ilr.v6i1.657>

Mewujudkan Ketahanan dan Kepatuhan Data di Era Digital: Harmonisasi Strategi Backup 3-2-1 dengan Regulasi Keamanan Siber dan Pelindungan Data Pribadi di Indonesia

Abstract

Indonesia's accelerating digital transformation requires strong data resilience as a core element of cybersecurity and personal data protection. This study aims to achieve data resilience and compliance through the harmonization of the backup 3-2-1 strategy with the regulatory framework for personal data protection in Indonesia. This research employs a normative juridical method using statute and conceptual approaches, supported by international standards such as NIST SP 800-34 and ISO/IEC 27040:2024. The findings indicate that the obligations of data controllers under Articles 35 and 39 of the PDP Law are consistent with resilience principles, yet the law lacks prescriptive technical guidelines on backup mechanisms, frequency, and recovery testing. This absence contributes to a gap between formal compliance and actual operational readiness. The study also highlights the crucial role of coordinated oversight among Komdigi, BSSN, and OJK in establishing a coherent national data resilience ecosystem. This research concludes that integrating legal requirements with technical controls through Cyber Resilience Governance framework is essential to reinforce data sovereignty and ensure effective implementation of the PDP Law. Key policy recommendations include issuing a technical regulation on national backup standards, strengthening the authority of the Data Protection Agency, and enhancing technical capabilities across public and private institutions

Keywords: data resilience, PDP Law, 3-2-1 backup strategy

Abstrak

Transformasi digital yang semakin pesat menuntut penerapan ketahanan data sebagai komponen penting dalam keamanan siber dan pelindungan data pribadi. Penelitian ini bertujuan untuk mewujudkan ketahanan dan kepatuhan data melalui harmonisasi strategi backup 3-2-1 dengan kerangka regulasi pelindungan data pribadi di Indonesia. Metode yang digunakan adalah yuridis normatif dengan pendekatan statute dan conceptual approach, serta mengacu pada standar teknis seperti NIST SP 800-34 dan ISO/IEC 27040:2024. Hasil penelitian menunjukkan bahwa kewajiban pengendali data dalam Pasal 35 dan 39 UU PDP sejalan dengan prinsip ketahanan data, tetapi belum dilengkapi pedoman teknis minimum terkait mekanisme pencadangan, frekuensi backup, dan pengujian pemulihan. Ketiadaan standar teknis ini menimbulkan kesenjangan antara kepatuhan normatif dan kesiapan operasional. Temuan lain menegaskan pentingnya sinergi Komdigi, BSSN, dan OJK dalam membentuk ekosistem ketahanan data nasional yang harmonis. Penelitian ini menyimpulkan bahwa integrasi hukum dan teknologi melalui pendekatan Cyber Resilience Governance diperlukan untuk memperkuat kedaulatan data sekaligus memastikan efektivitas implementasi UU PDP. Rekomendasi kebijakan mencakup penyusunan peraturan pelaksana mengenai standar backup nasional, penguatan peran Badan Pelindungan Data Pribadi, serta peningkatan kapasitas teknis institusi publik dan privat.

Kata kunci: ketahanan data, UU PDP, strategi backup 3-2-1

PENDAHULUAN

Perkembangan teknologi digital telah mengubah paradigma dalam tata kelola data secara global. Di Indonesia, digitalisasi menjadi prioritas nasional sebagaimana tercantum dalam *Indonesia Digital Roadmap 2021–2024* yang dikeluarkan oleh Kementerian Komunikasi dan Informatika, dimana sejak Oktober 2024 kementerian tersebut telah berganti nama menjadi Kementerian Komunikasi dan Digital (Komdigi). Dokumen tersebut menegaskan bahwa data merupakan sumber daya strategis baru yang perlu dikelola secara aman, berkelanjutan, dan sesuai dengan prinsip kedaulatan negara. Dalam konteks ini, keamanan dan ketahanan data (*data resilience*) menjadi bagian integral dari perlindungan data pribadi dan keberlanjutan infrastruktur digital.

Dalam konteks pembentukan kebijakan hukum nasional di era digital, harmonisasi regulasi menjadi prasyarat penting agar norma hukum mampu merespons dinamika teknologi yang berkembang cepat, khususnya dalam pengelolaan data sebagai aset strategis negara (Fitriyantica, 2019).

Laju digitalisasi yang tinggi di Indonesia membawa tantangan serius terhadap aspek keamanan informasi. Laporan Badan Siber dan Sandi Negara (2024) mencatat bahwa pada tahun 2023 telah terjadi 403,9 juta anomali trafik dengan dominasi *malware* (44,47%), serta kebocoran 1,67 juta data yang mayoritas menasar sektor administrasi publik. Eskalasi risiko ini mendorong peningkatan anggaran operasional sebesar 12,6% menjadi Rp624,37 miliar guna memperkuat kapabilitas mitigasi dan ketahanan siber nasional. Kasus kebocoran data seperti yang menimpa instansi pemerintah dan perusahaan swasta memperlihatkan lemahnya sistem pengelolaan data, khususnya pada aspek pencadangan dan pemulihan (*backup and recovery*). Hal ini menegaskan bahwa keberadaan kebijakan hukum tanpa kesiapan teknis dapat menyebabkan ketimpangan antara regulasi dan praktik perlindungan data.

Pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang tercantum dalam Lembaran Negara Republik Indonesia Tahun 2022 Nomor 204, merupakan langkah monumental dalam membangun kerangka hukum pelindungan data di Indonesia. UU ini mengatur prinsip, hak subjek data, serta kewajiban pengendali dan prosesor data untuk menjamin keamanan serta kerahasiaan data pribadi. Salah satu ketentuan penting adalah Pasal 35, yang menyatakan bahwa pengendali data wajib menerapkan langkah-langkah teknis dan organisasi guna melindungi data pribadi dari gangguan, kebocoran, dan kerusakan. Namun, undang-undang ini belum memberikan panduan teknis mengenai bagaimana prinsip ketahanan data tersebut seharusnya diimplementasikan dalam sistem informasi modern (Hanafi & Lubis, 2023).

Dalam praktik internasional, konsep *data resilience* erat kaitannya dengan strategi pencadangan data yang dikenal sebagai strategi *backup 3-2-1*. Strategi ini menyarankan agar organisasi memiliki tiga salinan data, disimpan di dua jenis media yang berbeda, dan satu salinan tersimpan di lokasi yang terpisah. Strategi ini juga menjadi acuan dalam standar NIST SP 800-34 tentang *Contingency Planning Guide for Federal Information Systems* dan ISO/IEC 27040:2024 yang terletak pada penguatan ketahanan operasional dan perlindungan data kritis saat menghadapi gangguan sistem atau serangan siber. Kedua standar ini memastikan bahwa proses pemulihan bencana (*disaster recovery*) didukung oleh sistem

penyimpanan yang tervalidasi keamanannya, mencakup aspek enkripsi, integritas data, serta sanitasi media guna menjamin ketersediaan informasi yang krusial bagi kelangsungan organisasi. Dalam konteks Indonesia, strategi *backup* 3-2-1 dapat dipandang sebagai implementasi teknis atas mandat hukum dalam UU PDP untuk memastikan keberlanjutan dan keamanan data pribadi.

Ketahanan data pada sistem berbasis *cloud* memerlukan pendekatan terintegrasi antara manajemen risiko, strategi *backup*, dan pemulihan bencana, terutama dalam menghadapi *ransomware* dan kerentanan sistem distribusi data (Abdi et al., 2024). Menurut Abdi et al., pendekatan *disk-based* dan *cloud-based* dalam lingkungan pemerintahan terbukti memberikan *trade-off* antara efisiensi biaya, RTO, dan RPO.

Selain UU PDP, terdapat sejumlah regulasi sektoral yang memperkuat kewajiban perlindungan dan ketahanan data. Misalnya, Peraturan OJK Nomor 38/POJK.03/2016 tentang *Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum* mewajibkan setiap bank memiliki mekanisme cadangan data dan rencana pemulihan bencana (*disaster recovery plan*) sebagai bagian dari manajemen risiko. Regulasi teknis lainnya, seperti Peraturan BSSN Nomor 8 Tahun 2020 tentang **Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik**, mempertegas pentingnya pengujian sistem informasi terhadap ancaman siber dan memastikan kesiapan pemulihan data (Badan Siber dan Sandi Negara, 2020).

Namun demikian, masih terdapat kesenjangan antara norma hukum dan penerapan teknis di lapangan. Banyak organisasi yang menganggap perlindungan data sebatas *network security*, tanpa menyiapkan strategi pemulihan data yang efektif (Ardika, 2025). Dalam pandangan hukum, hal ini menimbulkan pertanyaan mengenai sejauh mana tanggung jawab hukum pengendali data dapat diukur jika terjadi kehilangan data akibat kelalaian dalam menerapkan prinsip *data resilience*. Kekosongan panduan teknis ini dapat menimbulkan *compliance gap* antara kewajiban hukum dan praktik implementasi (Bennett & Raab, 2017).

Kedaulatan data (*data sovereignty*) kemudian muncul sebagai isu strategis dalam konteks nasional (Yun, 2025). Prinsip ini menekankan bahwa data warga negara harus dikelola di bawah yurisdiksi hukum Indonesia, baik secara lokasi fisik maupun kontrol akses. Pemerintah melalui Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) serta kebijakan *Government Cloud* berupaya memastikan data nasional tidak tergantung pada infrastruktur asing. Konsep ini menunjukkan bahwa penguatan *data resilience* tidak hanya mendukung kepatuhan terhadap UU PDP, tetapi juga memperkuat posisi Indonesia dalam mempertahankan kedaulatan digitalnya di tengah globalisasi ekonomi data (Joenaedi & Tarina, 2024).

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan *statute approach* dan *conceptual approach*, yaitu menelaah ketentuan peraturan perundang-undangan, teori hukum siber, serta standar teknis internasional yang relevan.

Data sekunder diperoleh dari peraturan, literatur hukum, dan jurnal ilmiah bereputasi. Hasil penelitian ini diharapkan memberikan kontribusi pada pembentukan kebijakan publik yang memperkuat sinergi antara hukum dan teknologi dalam mencapai kedaulatan data nasional.

HASIL DAN PEMBAHASAN

Analisis Yuridis terhadap Ketentuan UU PDP dan Relevansinya dengan Prinsip Ketahanan Data

1. Prinsip Ketahanan Data dalam Perspektif Hukum

Konsep ketahanan data (*data resilience*) mencerminkan kemampuan suatu sistem untuk menjaga ketersediaan, integritas, dan pemulihan data dari gangguan, serangan, atau bencana (Prabowo & Ramadhani, 2021). Prinsip ini berperan penting dalam konteks hukum perlindungan data karena kegagalan menjaga ketersediaan data dapat berimplikasi pada tanggung jawab hukum pengendali data sebagaimana diatur dalam Pasal 35 UU PDP.

Joenaedi & Tarina (2024) menegaskan bahwa ketahanan data bukan sekadar urusan teknis, melainkan bagian dari legal compliance yang wajib diterapkan oleh setiap pengendali data. UU PDP mengatur bahwa langkah-langkah teknis dan organisasi harus diterapkan untuk mencegah kerusakan atau kebocoran data pribadi (Pasal 39). Ketentuan ini sejalan dengan prinsip *security of processing* dalam General Data Protection Regulation (GDPR) Uni Eropa, Pasal 32, mengatur Keamanan Pemrosesan Data, dimana mewajibkan pengendali dan prosesor data menerapkan langkah teknis dan organisasi yang tepat (seperti enkripsi, pseudonimisasi, dan pengujian rutin) untuk melindungi data pribadi, memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan sistem, serta mampu memulihkan data saat terjadi insiden, dengan mempertimbangkan risiko dan biaya implementasi.

Oleh karena itu, *data resilience* memiliki kedudukan hukum yang strategis: ia menjadi penghubung antara prinsip tanggung jawab hukum (*accountability principle*) dan prinsip kehati-hatian (*due diligence*). Dalam praktik, perusahaan dapat dianggap lalai (*liability by omission*) apabila tidak menerapkan mekanisme cadangan dan pemulihan data yang memadai (Filler et al., 2022).

2. Kewajiban Pengendali Data dan Implementasi Teknis

Strategi backup 3-2-1 adalah metode pencadangan data yang mensyaratkan keberadaan tiga salinan data, disimpan pada dua jenis media yang berbeda, dengan satu salinan berada di lokasi terpisah. Strategi backup 3-2-1 menjadi standar operasional untuk memastikan ketersediaan, integritas, dan kemampuan pemulihan data pada kondisi insiden siber atau bencana.

UU PDP mewajibkan pengendali data menjamin keamanan dan ketersediaan data pribadi melalui kebijakan dan mekanisme perlindungan teknis yang sesuai dengan perkembangan teknologi informasi. Dalam konteks implementasi, hal ini berkaitan erat dengan strategi pencadangan data (*data backup*) dan rencana pemulihan bencana

(disaster recovery plan), sebagaimana diwajibkan pula oleh POJK No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, untuk sektor perbankan (Otoritas Jasa Keuangan, 2016).

Secara global, praktik terbaik yang banyak diadopsi adalah strategi backup 3-2-1, yakni memiliki tiga salinan data, disimpan di dua media berbeda, dan satu salinan di lokasi terpisah. Pendekatan berlapis ini secara signifikan meningkatkan ketahanan data (data resilience) dan kepercayaan para pemangku kepentingan terhadap kemampuan organisasi dalam melindungi aset informasi yang paling berharga. Terlebih lagi, kepatuhan terhadap standar internasional ini membantu organisasi memenuhi ekspektasi pengawasan regulator dan menghindari sanksi berat akibat kehilangan atau kerusakan data pribadi yang diatur oleh UU PDP. Prinsip ini dijadikan standar oleh NIST SP 800-34 dan ISO/IEC 27040:2024. Konsep ini juga selaras dengan tujuan hukum UU PDP, yaitu menjamin availability, integrity, dan recoverability dari data pribadi. Tabel berikut menunjukkan perbandingan strategi backup 3-2-1 dengan ketentuan hukum yang relevan dalam UU PDP:

Tabel 1. Korelasi Strategi Backup 3-2-1 dengan Ketentuan UU PDP

Elemen 3-2-1 backup	Makna Teknis	Keterkaitan dengan Ketentuan UU PDP
3 Copies (3 Salinan Data)	Mencegah kehilangan data akibat kerusakan sistem utama	Pasal 35 & 39: Kewajiban melindungi data pribadi dari kerusakan atau kehilangan
2 Different Media (2 Media Berbeda)	Diversifikasi media penyimpanan (misal HDD + cloud) untuk menghindari kegagalan tunggal	Pasal 35: Pengendali wajib menjamin keamanan data pribadi dalam setiap tahap pemrosesan
1 Offsite Copy (1 Cadangan di Lokasi Terpisah)	Memastikan data tetap aman bila terjadi bencana lokal	Pasal 39: Pengendali wajib mencegah akses ilegal atau gangguan fisik

Sumber: NIST SP 800-34; ISO/IEC 27040:2024; UU No. 27 Tahun 2022 (diolah penulis, 2025).

OJK menegaskan strategi serupa melalui SE OJK No. 29/SEOJK.03/2022 tentang Ketahanan Dan Keamanan Siber Bagi Bank Umum, yang mewajibkan uji pemulihan data secara berkala untuk menjamin kontinuitas operasional sektor keuangan (Otoritas Jasa Keuangan, 2022). Kominfo juga mewajibkan disaster recovery center (DRC) dalam wilayah hukum Indonesia melalui SE Kominfo No. 20 Tahun 2016 tentang Penyelenggara Sistem Elektronik, yang menyatakan bahwa penyelenggara sistem elektronik untuk pelayanan publik yang digunakan untuk perlindungan data pribadi harus menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia (Kementerian Komunikasi dan Informatika, 2016). Hal ini memperkuat prinsip data sovereignty di mana negara memiliki yurisdiksi penuh terhadap data warga negara yang dikelola oleh penyelenggara sistem elektronik domestik.

Meskipun demikian, penulis melihat belum adanya pedoman teknis yang jelas dalam UU PDP mengenai mekanisme minimal backup atau frekuensi pencadangan. Akibatnya, banyak entitas publik dan swasta yang hanya memenuhi kepatuhan administratif tanpa ketahanan operasional yang nyata (*formal compliance without resilience*).

3. Analisis Kesenjangan Hukum-Teknologi

Kesenjangan antara norma hukum dan praktik teknis menjadi persoalan utama dalam penerapan UU PDP. UU PDP bersifat prinsipil dan tidak menetapkan standar teknis eksplisit, sehingga pengendali data memiliki kebebasan interpretasi terhadap tingkat keamanan yang “memadai” (Bennett & Raab, 2017). Dalam praktik, banyak organisasi yang tidak memiliki *recovery time objective* (RTO) dan *recovery point objective* (RPO) yang jelas, padahal dua indikator ini penting dalam mengukur ketahanan data (Prabowo & Ramadhani, 2021).

Sebagian besar korporasi di Indonesia hanya fokus pada pencegahan kebocoran (*data breach prevention*) tanpa strategi pemulihan (*post-incident recovery*) yang matang. Padahal, dalam sistem hukum siber yang baik, pemulihan data merupakan bagian dari tanggung jawab hukum pengendali data.

Penulis mengusulkan integrasi hukum dan teknologi dalam bentuk *Cyber Resilience Governance*, yaitu model pengawasan terpadu antara regulator, auditor, dan penyelenggara sistem elektronik. Dalam konteks Indonesia, model ini dapat menjadi cikal bakal pengembangan pedoman pelaksana UU PDP yang lebih teknis dan operasional.

Dengan demikian, analisis yuridis menunjukkan bahwa perlindungan data pribadi tidak dapat dipisahkan dari penerapan prinsip ketahanan data. Strategi backup 3-2-1 menjadi instrumen yang relevan untuk menjembatani kesenjangan hukum-teknologi dan memperkuat kedaulatan data nasional.

Strategi Integrasi Hukum dan Teknologi untuk Mewujudkan Kedaulatan Data Melalui Kepatuhan dan Ketahanan

1. Perbandingan Regulasi Global tentang Ketahanan dan Pelindungan Data

Untuk memahami posisi Indonesia secara global, berikut disajikan perbandingan antara GDPR Uni Eropa, Personal Data Protection Act (PDPA) Singapura, dan UU PDP Indonesia dalam aspek ketahanan dan kepatuhan terhadap perlindungan data pribadi.

Tabel 2. Perbandingan Regulasi Pelindungan Data dan Prinsip Ketahanan di Berbagai Yurisdiksi

Aspek	GDPR Uni Eropa	PDPA Singapura	UU PDP Indonesia
Dasar Hukum	Regulation (EU) 2016/679 (GDPR)	Personal Data Protection Act 2012	UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi
Prinsip Ketahanan Data	“Security of Processing” (Art. 32) – mencakup <i>availability</i> dan <i>restore access</i>	Pasal 24 PDPA: langkah-langkah keamanan teknis untuk mencegah kehilangan data	Pasal 35 & 39 UU PDP: pengendali wajib melindungi data dari kerusakan, kehilangan, dan akses ilegal

Aspek	GDPR Uni Eropa	PDPA Singapura	UU PDP Indonesia
Kewajiban Pemulihan Data	Wajib memiliki <i>backup and restore plan</i>	Didorong melalui panduan PDPC (non-mandatory)	Tidak dijelaskan secara teknis, diserahkan kepada kebijakan internal
Lembaga Pengawas	European Data Protection Board (EDPB)	Personal Data Protection Commission (PDPC)	Kementerian Kominfo / Badan Pelindungan Data Pribadi (BPDP)
Sanksi atas Kelalaian	Hingga €20 juta atau 4% dari omzet tahunan	Hingga SGD 1 juta atau 10% dari omzet tahunan (revisi PDPA tahun 2020)	Maksimal 2% dari pendapatan tahunan korporasi (Pasal 57)
Integrasi Teknis	Mengacu pada ISO/IEC 27001 & ENISA Resilience Framework	Berdasarkan PDPC Technical Guidelines	Mengacu pada standar global, belum ada ketentuan wajib

Sumber: EU GDPR (2016); PDPA Singapore (2012); UU PDP Indonesia (2022); ISO/IEC 27040:2024; diolah penulis (2025).

Tabel di atas menunjukkan bahwa dibandingkan dengan GDPR dan PDPA Singapura, UU PDP Indonesia masih bersifat normatif dan belum preskriptif secara teknis. Oleh karena itu, perlu peraturan turunan yang mengatur resilience mechanism secara eksplisit, seperti frekuensi backup, lokasi penyimpanan, dan prosedur pemulihan data pasca-insiden.

2. Sinergi antara Kepatuhan Hukum dan Ketahanan Teknologi

Penerapan perlindungan data pribadi tidak dapat dilepaskan dari sinergi antara kepatuhan hukum (legal compliance) dan ketahanan teknologi (technical resilience). UU PDP menegaskan kewajiban pengendali data untuk menerapkan langkah-langkah teknis dan organisasi dalam melindungi data pribadi dari gangguan, kebocoran, dan kerusakan. Namun, tanpa infrastruktur teknologi yang memadai, prinsip hukum tersebut sulit diwujudkan secara efektif.

Kedaulatan data (data sovereignty) menuntut adanya kontrol penuh negara atas siklus hidup data mulai dari pengumpulan, penyimpanan, pemrosesan, hingga transfer lintas batas. Hal ini mencakup dua aspek utama: (a) kontrol yuridis, yakni penegakan hukum di dalam yurisdiksi nasional, dan (b) kontrol teknis, yaitu kemampuan aktual untuk mengamankan dan memulihkan data dalam sistem digital domestik (Organisation for Economic Co-operation and Development, 2021).

Menurut Bennett & Raab (2017), efektivitas perlindungan data tergantung pada compliance ecosystem yang mengintegrasikan hukum, kebijakan, dan teknologi. Pendekatan serupa diterapkan di Uni Eropa melalui General Data Protection Regulation (GDPR) Pasal 32, yang mewajibkan organisasi memiliki mekanisme pemulihan data yang efektif. Model ini dikenal sebagai “resilience by design”, yakni prinsip di mana perlindungan hukum dirancang bersamaan dengan ketahanan teknis (Voigt & von dem Bussche, 2021).

3. Sinergi Peran Regulator Nasional

Upaya membangun kedaulatan data memerlukan koordinasi yang kuat antar lembaga regulator nasional. Tiga lembaga utama berperan strategis:

- a. Kementerian Komdigi, sebagai otoritas kebijakan dan pengawasan perlindungan data pribadi.
- b. BSSN, sebagai lembaga yang menetapkan standar keamanan informasi dan melaksanakan audit siber nasional.
- c. OJK, yang memastikan penerapan IT risk management di sektor jasa keuangan.

Sinergi kelembagaan ini harus diperkuat dengan sistem pelaporan dan audit berbasis data resilience maturity model, di mana entitas publik maupun privat dievaluasi berdasarkan kemampuan mereka menjaga dan memulihkan data. OECD (2021) menekankan bahwa keberhasilan kebijakan perlindungan data nasional sangat bergantung pada institutional coherence antar lembaga penegak hukum dan regulator teknis.

Selain itu, pembentukan Badan Pelindungan Data Pribadi (BPDP) sebagaimana diatur dalam Pasal 58 UU PDP akan menjadi langkah penting dalam mewujudkan tata kelola data nasional yang terintegrasi, dengan fungsi ganda sebagai pengawas dan pengembang standar kepatuhan teknis.

4. Tantangan Implementasi dan Rekomendasi Kebijakan

Meskipun kerangka hukum Indonesia sudah komprehensif, implementasi di lapangan masih menghadapi sejumlah tantangan:

- a. Belum adanya standar minimum ketahanan data nasional.
UU PDP belum mengatur secara eksplisit strategi backup 3-2-1 maupun frekuensi backup. Diperlukan Peraturan Pemerintah yang menetapkan *technical compliance benchmark*.
- b. Kapasitas teknis yang belum merata di sektor publik.
- c. Banyak instansi pemerintah belum memiliki disaster recovery plan yang teruji. Program sertifikasi dari BSSN dapat membantu meningkatkan kesiapan (Badan Siber dan Sandi Negara, 2020).
- d. Kurangnya koordinasi antar lembaga.
Kemdigi, OJK, dan BSSN masih berjalan sektoral. Diperlukan *Data Resilience Task Force* di bawah BPDP untuk harmonisasi.
- e. Risiko data lintas batas (*cross-border*).
Pengawasan transfer data ke luar negeri perlu diperkuat melalui data *localization policy* dan regional resilience zone sebagaimana diusulkan dalam RUU KKS.

Dengan memperkuat aspek-aspek di atas, hukum dan teknologi dapat berfungsi secara sinergis dalam membangun kedaulatan digital Indonesia. Prinsip ketahanan data bukan hanya kewajiban hukum, tetapi juga strategic enabler bagi keamanan nasional dan kepercayaan publik terhadap transformasi digital pemerintah dan industri.

KESIMPULAN

Berdasarkan analisis yuridis, ketentuan dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) memberikan landasan normatif yang memperkuat upaya peningkatan ketahanan data di Indonesia melalui kewajiban teknis dan organisasi bagi pengendali data. Namun, norma-norma tersebut masih bersifat prinsipil, sehingga memerlukan peraturan pelaksana yang lebih preskriptif agar ketentuan hukum dapat diterjemahkan menjadi standar teknis operasional yang terukur dan dapat diaudit. Untuk mewujudkan ketahanan dan kepatuhan data, harmonisasi Strategi Backup 3-2-1 dengan regulasi nasional dan praktik operasional harus segera diimplementasikan. Hal ini mensyaratkan penyusunan standar teknis, penguatan koordinasi antarregulator, serta mekanisme audit dan uji pemulihan berkala sehingga Strategi Backup 3-2-1 dapat menjembatani kesenjangan antara kepatuhan hukum dan kesiapan teknis organisasi. Oleh karena itu, pemerintah perlu segera menerbitkan peraturan pelaksana UU PDP yang mengatur standar teknis minimum ketahanan data, termasuk kewajiban Strategi Backup 3-2-1, frekuensi pencadangan, lokasi penyimpanan, format enkripsi, dan parameter RTO/RPO sebagai tolok ukur kepatuhan operasional. Selain itu, organisasi publik maupun privat harus mengadopsi Strategi Backup 3-2-1 sebagai standar operasional minimum, meningkatkan kapasitas SDM teknis, serta rutin melaksanakan audit dan uji pemulihan. Diperlukan pula forum koordinasi lintas-regulator untuk harmonisasi kebijakan dan penegakan kepatuhan.

DAFTAR PUSTAKA

- Abdi, A., Bennouri, H., & Keane, A. (2024). Cyber resilience, risk management, and security challenges in enterprise-scale cloud systems: Comprehensive review. 2024 13th Mediterranean Conference on Embedded Computing (MECO), 1–8. <https://arrow.tudublin.ie/cgi/viewcontent.cgi?article=1015&context=itbinfocon>
- Ardika, I. W. C. (2025). Tinjauan hukum terhadap perlindungan data pribadi di era digital: Kasus kebocoran data pengguna layanan e-commerce. *Indonesian Journal of Law and Justice*, 2(3), 11. <https://doi.org/10.47134/ijlj.v2i3.3601>
- Badan Siber dan Sandi Negara. (2020). Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik. BSSN.
- Badan Siber dan Sandi Negara. (2024). Laporan tahunan keamanan siber Indonesia 2023. BSSN.
- Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*. Routledge.
- Filler, D. M., Haendler, D. M., & Fischer, J. L. (2022). Negligence at the breach: Information fiduciaries and the duty to care for data. *Connecticut Law Review*, 54(3), 512. https://opencommons.uconn.edu/law_review/512
- Fitriyantica, A. (2019). Harmonisasi peraturan perundang-undangan Indonesia melalui konsep omnibus law. *Gema Keadilan*, 6(3), 300–316. <https://doi.org/10.14710/gk.2019.6751>
- Hanafi, I., & Lubis, A. F. (2023). Protection of privacy and intellectual property rights in digital data management in Indonesia. *The Easta Journal of Law and Human Rights*, 2(1), 33–40. <https://doi.org/10.58812/eslhr.v2i01.151>
- Joenaedi, F. A., & Tarina, D. D. Y. (2024). Cyber insurance as a risk mitigation tool and company compliance instrument with Indonesia's Personal Data Protection Law. *Unram Law Review*, 8(2). <https://doi.org/10.29303/ulrev.v8i2.380>

- Kementerian Komunikasi dan Informatika. (2016). Surat Edaran Menteri Kominfo Nomor 20 Tahun 2016 tentang Penyelenggara Sistem Elektronik.
- Organisation for Economic Co-operation and Development. (2021). Data governance and cross-border data flows: A policy framework for OECD countries. OECD Publishing.
- Otoritas Jasa Keuangan. (2016). Peraturan OJK Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.
- Otoritas Jasa Keuangan. (2022). Surat Edaran OJK Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum.
- Prabowo, W. A., & Ramadhani, R. D. (2021). Perancangan contingency planning disaster recovery unit teknologi informasi menggunakan NIST SP800-34. *Techno.Com*, 20(1), 38-49.
- Voigt, P., & von dem Bussche, A. (2021). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.
- Yun, H. (2025). China's data sovereignty and security: Implications for global digital borders and governance. *Chinese Political Science Review*, 10, 178-203. <https://doi.org/10.1007/s41111-024-00269-9>