LAN RI
MAKARTI BHAKTI NAGARI
Pusat Pembelajaran & Strategi Kebijakan Pelayanan Publik

Privasi dalam Bahaya, Alarm Tata Kelola Data Nasional

DITUJUKAN KEPADA: KEMENTERIAN KOMUNIKASI DAN DIGITAL, BADAN SIBER DAN SANDI NEGARA, DINAS KOMUNIKASI DAN INFORMASI PROVINSI/KABUPATEN/KOTA

Tim Penulis:
Kristita Liwu Hati A, Joana Kriskinantyas Rahayu, & Kemal Hidayah
(Analis Kebijakan – PUSJAR SKPP LAN)

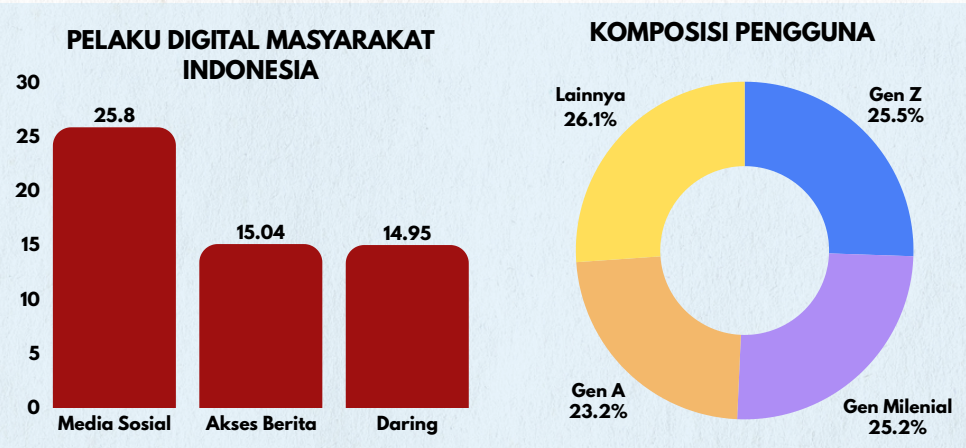
POLICY BRIEF – EDISI MARET 2026

EXECUTIVE SUMMARY

Policy brief ini membahas meningkatnya risiko kebocoran data pribadi dan kejahatan siber di Indonesia yang berpotensi merugikan masyarakat, melemahkan kepercayaan publik, serta mengancam keamanan ekosistem digital nasional. Pesatnya pertumbuhan pengguna internet dan layanan digital belum sepenuhnya diimbangi dengan tata kelola perlindungan data yang kuat, standar keamanan yang seragam, serta mekanisme pengawasan yang efektif. Oleh karena itu, *Policy brief* ini menawarkan beberapa alternatif solusi untuk memperkuat sistem perlindungan data pribadi di Indonesia, antara lain melalui pengujian keamanan sistem digital sebelum dioperasikan, pembentukan skema kompensasi bagi korban kebocoran data, reformasi tata kelola pengawasan perlindungan data, serta penguatan ekosistem pelaporan dan transparansi insiden siber. Melalui langkah-langkah tersebut, diharapkan ekosistem digital Indonesia dapat berkembang secara lebih aman, akuntabel, dan mampu melindungi kepentingan masyarakat di era transformasi digital.

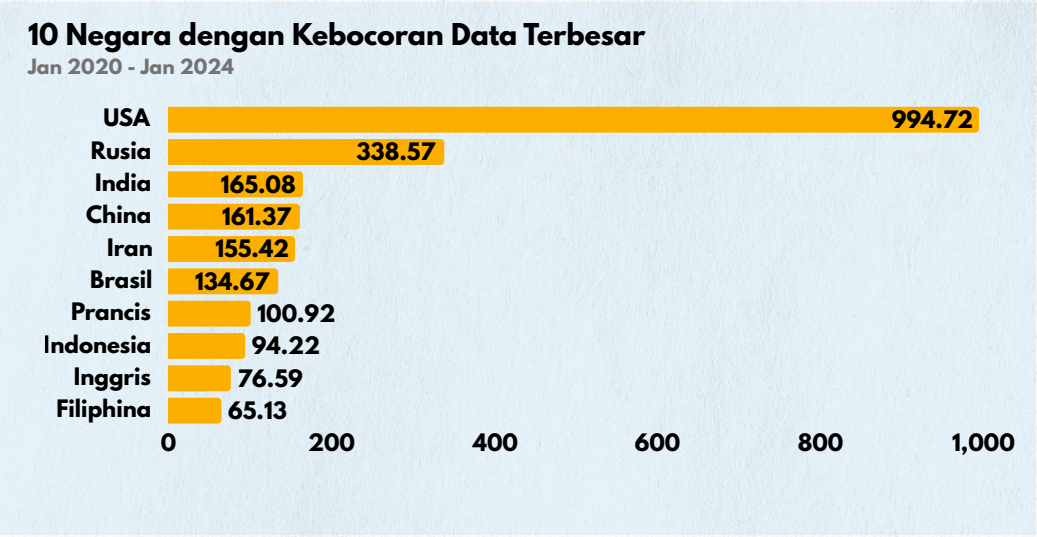
PENDAHULUAN

Kepercayaan publik terhadap negara semakin ditentukan oleh kemampuan pemerintah melindungi data pribadi warganya, namun serangkaian insiden kebocoran menunjukkan bahwa fondasi perlindungan tersebut masih rapuh. Gelombang kebocoran data mulai menjadi perhatian publik sejak 2019-2020, ketika sejumlah platform digital besar mengalami pembobolan jutaan akun pengguna (Kompas, 2025).



Sumber: (APJII, 2025)

Platform seperti Instagram, TikTok, YouTube, dan Facebook menjadi ruang interaksi utama warga di ekosistem digital. Dominasi kelompok usia produktif dan usia sekolah ini menegaskan bahwa ekosistem digital Indonesia bertumpu pada generasi yang sangat aktif dalam media sosial, transaksi digital, dan konsumsi konten daring sekaligus memiliki tingkat eksposur tinggi terhadap risiko penyalahgunaan data (APJII, 2025).



Di balik meningkatnya jumlah pengguna internet di Indonesia, tren kejahatan siber juga menunjukkan peningkatan yang signifikan baik dari sisi frekuensi maupun skala dampaknya. Ekspansi aktivitas digital mulai dari media sosial, transaksi keuangan, hingga layanan publik berbasis elektronik membuka ruang yang semakin luas bagi eksploitasi data pribadi.

Sumber: Surfshark (2024)

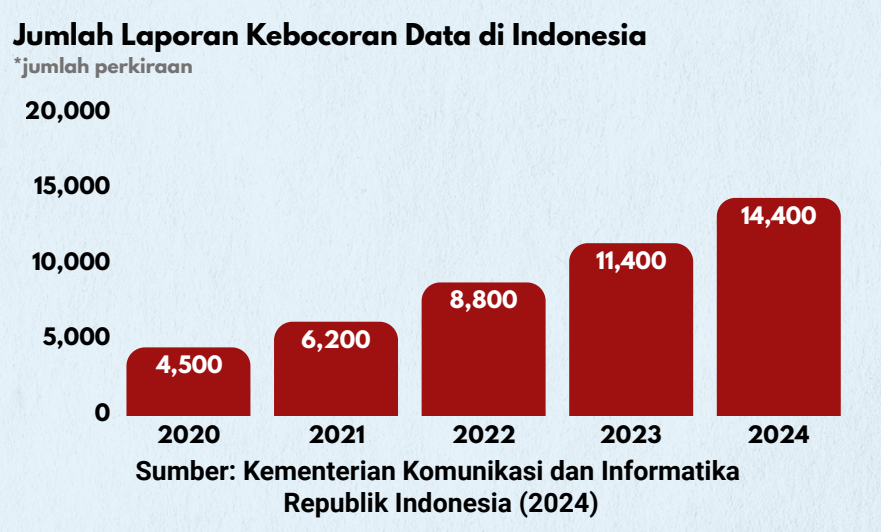
Di kawasan Asia, Singapura melalui *Cybersecurity Act* dan *Smart Nation Initiative* mewajibkan lembaga publik serta sektor kritikal menerapkan *secure coding* dan *resilience testing* untuk memastikan sistem tetap berjalan meski terjadi serangan. Australia mengembangkan *Essential Eight Maturity Model* yang menekankan toleransi terhadap kesalahan manusia melalui *patching* otomatis, *multi-factor authentication,* dan backup sistem sejak tahap desain. Tanpa penguatan tata kelola, peningkatan kapasitas keamanan siber, serta penegakan regulasi yang konsisten, pertumbuhan digital justru berpotensi memperbesar kerentanan masyarakat terhadap penyalahgunaan data dan kejahatan berbasis digital. Oleh karena itu, persoalan kebocoran data pribadi perlu didiskusikan secara lebih komprehensif.

DESKRIPSI MASALAH

Dalam beberapa tahun terakhir, Indonesia menghadapi berbagai kasus kebocoran data pribadi yang berdampak signifikan terhadap masyarakat. Sejumlah insiden menunjukkan bahwa sistem pengelolaan dan perlindungan data, baik dari sektor pemerintah maupun swasta, masih menghadapi tantangan serius.

1 Lonjakan Kejahatan Siber, Penipuan Digital, dan Kerentanan Human Error.

Transformasi digital yang masif di Indonesia turut diiringi oleh peningkatan signifikan kejahatan siber. Kepolisian Negara Republik Indonesia mencatat telah menangani lebih dari 32.000 laporan kejahatan siber hingga Januari 2025. Kasus tersebut didominasi oleh penipuan online (14.495 kasus), disusul ancaman kekerasan digital serta pencemaran nama baik (Humas.Polri, 2026). Temuan serupa juga disampaikan oleh Badan Siber dan Sandi Negara (BSSN).



Sumber: Kementerian Komunikasi dan Informatika Republik Indonesia (2024)

Sepanjang periode pelaporan terakhir, tercatat lebih dari 26 juta kasus *phising*, peningkatan lebih dari 30 kali lipat pada kasus *web defacement*, serta lonjakan drastis insiden kebocoran data dari 1,67 juta menjadi 56 juta kasus hanya dalam satu tahun. Lonjakan ini mengindikasikan eskalasi ancaman yang tidak hanya meningkat dari sisi kuantitas, tetapi juga kompleksitas serangan (Firdaus Baderi, 2025).

Di tingkat kesiapan organisasi, laporan *Fortinet* 2025 *State of Cloud Security Report* menunjukkan bahwa 76% organisasi di Indonesia masih mengalami kekurangan keahlian dalam keamanan *cloud*. Kondisi ini memperlihatkan adanya kesenjangan kapasitas sumber daya manusia di bidang keamanan siber, terutama dalam menghadapi migrasi sistem ke infrastruktur berbasis *cloud* yang semakin luas digunakan oleh sektor publik maupun swasta. Selain itu, Bank Indonesia mencatat lebih dari 370 juta serangan siber yang menargetkan infrastruktur digital nasional sepanjang tahun sebelumnya. Serangan tersebut tidak hanya menyasar individu, tetapi juga sistem pembayaran, layanan keuangan, dan infrastruktur strategis negara (dig.watch, 2024).

2 Meningkatnya Kerugian Ekonomi bagi Masyarakat dan Negara

Dari sisi kerugian ekonomi, dampak kebocoran data semakin signifikan. Data statistik menunjukkan bahwa kerugian finansial akibat penipuan digital di Indonesia mencapai sekitar Rp18 triliun pada tahun 2024, dan masih berlanjut hingga mencapai Rp4,6 triliun sampai Agustus 2025 berdasarkan catatan Badan Siber dan Sandi Negara. Sementara itu, data dari Otoritas Jasa Keuangan (OJK) dan *Indonesia Anti Scam Center* (IASC) mencatat total kerugian akibat penipuan online telah mencapai lebih dari Rp2,6 triliun hingga Mei 2025, angka ini menggambarkan tingginya intensitas ancaman terhadap sistem keuangan dan layanan digital nasional.

Kerugian akibat kebocoran data pribadi tidak hanya menyangkut aspek privasi, tetapi juga berdampak luas terhadap perekonomian. Berdasarkan laporan Indonesia *Cyber Security Independent Resilience Team* (CSIRT.ID), estimasi kerugian material akibat kebocoran data yang mencakup sekitar 279 juta penduduk Indonesia mencapai kurang lebih Rp600 triliun. Perhitungan tersebut mencakup berbagai dampak turunan, seperti penyalahgunaan nomor kontak pribadi, pembajakan akun media sosial, hingga maraknya panggilan dan pesan penipuan dari nomor tidak dikenal (CNN Indonesia, 2021).

3 Lemahnya Tata Kelola dan Standar Keamanan yang Belum Seragam

Berdasarkan data dari Index, pertahanan siber Indonesia juga masih sangat lemah, berada di kisaran 3,46 poin, jauh dari indeks rata-rata global di angka 6,19 poin. Sementara data dari *National Security Index*, nilai keamanan siber Indonesia hanya sebesar 64% dan menempati urutan ke-47 secara global. Hal ini terjadi karena banyak organisasi di Indonesia belum mengadopsi standar keamanan global, seperti ISO 27001, yang dirancang untuk melindungi sistem informasi dari ancaman siber (CNN Indonesia, 2024).

Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) telah diberlakukan melalui UU No. 27 Tahun 2022, fakta bahwa pelanggaran data masih terus terjadi, bahkan di lembaga pemerintahan, memperlihatkan adanya kelemahan mendasar dalam tata kelola, standar keamanan, serta mekanisme pengawasan dan penegakan hukum di Indonesia (Pradhipta & Yudiantara, 2025).

ALTERNATIF SOLUSI

Policy brief ini menawarkan sejumlah alternatif solusi yang dapat dipertimbangkan sebagai langkah strategis dalam memperkuat sistem perlindungan data pribadi dan menata ulang tata kelola keamanan digital nasional.

01 *National Cloud Security Sandbox*

Sebagai langkah strategis mengatasi kerentanan data nasional, diusulkan implementasi *National Cloud Security Sandbox* sebagai fase wajib pra-operasional bagi seluruh layanan publik digital. Mekanisme ini bekerja dengan menyediakan lingkungan replika infrastruktur *cloud* yang terisolasi, di mana setiap sistem yang akan diluncurkan wajib melalui pengujian ketahanan (*stress-testing*) secara intensif.

Dengan merangkul komunitas peretas etis (*ethical hacker*) melalui skema *Bug Bounty* nasional yang terstandarisasi, pemerintah dapat mendeteksi celah keamanan secara masif dan kreatif sebelum sistem tersebut bersentuhan dengan data masyarakat yang asli. Melalui platform pelaporan terpusat, setiap temuan teknis akan diverifikasi oleh otoritas siber untuk segera diperbaiki, sehingga risiko kebocoran akibat kesalahan konfigurasi maupun kelalaian manusia dapat dimitigasi sepenuhnya sejak dalam tahap simulasi.

02 Skema Kompensasi bagi Korban Kebocoran Data

Besarnya kerugian ekonomi akibat penipuan digital dan kebocoran data menegaskan bahwa respons kebijakan tidak cukup bersifat preventif, tetapi juga perlu mengakomodasi pendekatan restoratif. Pemerintah dapat mempertimbangkan pembentukan skema kompensasi atau dana perlindungan bagi korban kejahatan siber, khususnya masyarakat yang mengalami kerugian finansial akibat kelemahan sistem maupun kelalaian pengelola data. Metode ini sudah diterapkan di beberapa negara contohnya Korea Selatan yang melakukan ganti rugi sebesar $1,18 miliar atau 1,69 triliun rupiah kepada 33,7 juta akun atas kebocoran data, di mana perusahaan Coupang sebagai penanggung jawab akan memberikan voucher 50.000 won kepada setiap orang (reuters.com. 2025). Mekanisme ini dapat dirancang melalui koordinasi dengan Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) guna memastikan proses verifikasi, pemulihan dana, dan penyelesaian sengketa berjalan cepat, transparan, dan terintegrasi.

03 Pembenahan Tata Kelola Keamanan dan Perlindungan Data

Sebagai langkah untuk mengejar ketertinggalan tata kelola pertahanan siber nasional, diusulkan percepatan operasionalisasi Lembaga Pengawas Perlindungan Data Pribadi (Otoritas PDP) yang benar-benar independen dan bebas dari intervensi birokrasi kementerian. Urgensi ini didasarkan pada kebutuhan akan entitas yang memiliki kekuatan hukum untuk mengaudit serta menjatuhkan sanksi administratif tegas bagi instansi publik maupun swasta yang lalai dalam menjaga data masyarakat sesuai amanat UU PDP. Penguatan ini harus dibarengi dengan pengesahan aturan turunan yang mewajibkan penerapan standar internasional ISO 27001 sebagai syarat mutlak operasional bagi setiap pengelola data strategis. Standarisasi ini dapat diukur melalui indeks atau pendekatan kuantitatif lainnya, sehingga setiap penyelenggara sistem elektronik memiliki panduan teknis yang seragam, teruji secara global, dan mengikat secara hukum.

04 Penguatan Ekosistem Pelaporan & Transparansi Insiden Siber

Pemerintah perlu membangun portal publik insiden siber sebagai wadah resmi yang dapat diakses masyarakat dan organisasi untuk melihat serta mempelajari insiden yang telah terjadi. Selain itu, perlu diterapkan kewajiban *disclosure* terbuka atas insiden signifikan, yaitu aturan yang mewajibkan organisasi atau perusahaan mengumumkan secara resmi kepada publik jika terjadi insiden besar yang berdampak pada layanan, data, atau kepercayaan pengguna.

Praktik internasional menunjukkan efektivitas pendekatan ini, seperti Uni Eropa melalui ENISA yang mendorong portal insiden publik, Amerika Serikat lewat SEC yang mewajibkan perusahaan melaporkan insiden material dalam 4 hari, dan Singapura dengan *Cybersecurity Labelling Scheme* yang mewajibkan pengumuman terbuka atas kerentanan perangkat IoT. Dengan mengadopsi langkah serupa, Indonesia dapat memperluas ekosistem pelaporan insiden siber, melibatkan masyarakat, akademisi, dan industri, sehingga sistem keamanan nasional menjadi lebih tangguh dan transparan.

REKOMENDASI

Policy brief ini mendorong penguatan tata kelola perlindungan data pribadi melalui pendekatan yang lebih sistematis dan terintegrasi. Pemerintah perlu mendorong pengujian keamanan sistem digital sebelum dioperasikan melalui mekanisme *security sandbox*, mempercepat pembentukan lembaga pengawas perlindungan data pribadi yang independen, serta membangun ekosistem pelaporan dan transparansi insiden siber yang lebih terbuka. Selain itu, perlu dipertimbangkan skema kompensasi bagi masyarakat yang terdampak kebocoran data sebagai bentuk perlindungan dan pemulihan kerugian. Langkah-langkah tersebut diharapkan dapat memperkuat keamanan ekosistem digital nasional sekaligus meningkatkan kepercayaan publik terhadap transformasi digital di Indonesia.

DAFTAR PUSTAKA

- CNN Indonesia. (2024). Buruk Keamanan Siber di Indonesia Akibat Egosektoral. https://www.cnnindonesia.com/nasional/20240627100303-20-1114729/buruk-keamanan-siber-di-indonesia-akibat-egosektoral
- HumasPolri. (2026). Waspada Pandemi Kejahatan Siber, Polrestabes Medan Ungkap Data Mengejutkan dan Ajak Warga Perketat Keamanan Digital. https://humas.polri.go.id/news/detail/2252762-waspada-pandemi-kejahatan-siber-polrestabes-medan-ungkap-data-mengejutkan-dan-ajak-warga-perketat-keamanan-digital
- Media Indonesia. (2025). Ini Tren Ancaman Siber 2025, Dari Ransomware hingga Deepfake. https://mediaindonesia.com/teknologi/825592/ini-tren-ancaman-siber-2025-dari-ransomware-hingga-deepfake?utm_source=copilot.com
- Telkom University. (2025). Security by Design:Strategi Membangun Perangkat Lunak yang Aman Sejak Awal. https://bse.telkomuniversity.ac.id/f09f9492-security-by-design-strategi-membangun-perangkat-lunak-yang-aman-sejak-awal/