e-ISSN 2798-8260

Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora Vol: 6, No 1, 2026, Page: 1-15

Implementasi Kebijakan Pemerintah terhadap Pencegahan Kebocoran Data Pribadi dalam Pelayanan Publik Berbasis Digital

Dedi Mulyadi[1]*, Aji Mulyana[2], Aurelya Carmenita[3], Hasna Laksmi Utami[4], Kaffah Almira Aulia[5], Mugianing Putri[6], Nabila Rahma Alia[7]

Universitas Suryakancana

DOI: https://doi.org/10.53697/iso.v6i1.3473
*Correspondence: Dedi Mulyadi
Email: dedimulyadi53@gmail.com

Received: 09-04-2026
Accepted: 12-05-2026
Published: 28-06-2026

Abstract: *This study aims to analyze the effectiveness of government policy implementation in preventing personal data leaks in digital-based public services after the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), identify factors that hinder its implementation, and formulate strategic efforts to strengthen data protection in the public sector. The research method used is normative legal research with a regulatory, conceptual, and comparative approach, reinforced by secondary empirical data in the form of government agency reports, data breach incident statistics, SPBE indices, and digital literacy reports for the 2023–2025 period.The results of the study show that normatively, the PDP Law provides a comprehensive legal framework that is in line with international standards for personal data protection. However, its implementation in digital public services has not been effective. This is reflected in the increasing number of data breach incidents, namely 144 cases in 2023, 176 cases in 2024, and 198 cases as of October 2025. The main obstacles include weak technical security infrastructure, a lack of uniformity in data security standards between agencies, low human resource competence in the field of cybersecurity, a lack of regular security audits, and the Personal Data Protection Authority not yet functioning optimally. This study concludes that the effectiveness of personal data protection is not only.*

Keywords: *Data Protection Law, Digital Public Services, Government Cybersecurity*

Abstrak: Penelitian ini bertujuan untuk menganalisis efektivitas implementasi kebijakan pemerintah dalam mencegah kebocoran data pribadi pada pelayanan publik berbasis digital setelah berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), mengidentifikasi faktor-faktor penghambat pelaksanaannya, serta merumuskan upaya strategis penguatan perlindungan data di sektor publik. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan, konseptual, dan komparatif, yang diperkuat oleh data empiris sekunder berupa laporan instansi pemerintah, statistik insiden kebocoran data, indeks SPBE, serta laporan literasi digital periode 2023–2025.Hasil penelitian menunjukkan bahwa secara normatif UU PDP telah menyediakan kerangka hukum yang komprehensif dan sejalan dengan standar internasional dalam perlindungan data pribadi. Namun, implementasinya dalam pelayanan publik digital belum efektif. Hal ini tercermin dari meningkatnya insiden kebocoran data, yaitu 144 kasus pada 2023, 176 kasus pada 2024, dan 198 kasus hingga Oktober 2025. Hambatan utama meliputi lemahnya infrastruktur keamanan teknis, ketidakterpaduan standar pengamanan data antarinstansi, rendahnya kompetensi sumber daya manusia di bidang keamanan siber, minimnya audit keamanan berkala, serta belum berfungsinya Otoritas Perlindungan Data Pribadi secara optimal. Penelitian ini menyimpulkan bahwa efektivitas perlindungan data pribadi tidak hanya ditentukan oleh keberadaan regulasi, tetapi juga oleh kesiapan kelembagaan, teknis, dan budaya hukum. Oleh karena itu, direkomendasikan percepatan pembentukan otoritas pengawas independen, penguatan audit keamanan berbasis SPBE, peningkatan kapasitas aparatur negara, serta standardisasi pengamanan data di seluruh instansi pemerintah.

Katakunci: Hukum Perlindungan Data, Pelayanan Publik Digital, Keamanan Siber Pemerint

Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah membawa perubahan besar dalam penyelenggaraan pelayanan public di Indonesia. Pemerintah berupaya memaksimalkan pemanfaatan teknologi digital untuk menningkatkan efisiensi birokrasi, memperkuat transparansi, serta memperluas kemudahan akses layanan bagi Masyarakat. Upaya tersebut diwujudkan melalui penggunaan berbagai sistem dan platform berbasis digital, seperti portal pelayanan terpadu, aplikasi administrasi kependudukan berbasis NIK, layanan Kesehatan daring, hingga integrasi data lintas sektor. Meskipun memberikan kemudahan dan percepatan layanan, perkembangan ini juga menimbulkan tantangan baru berupa meningkatnya risiko kebocoran data pribadi masyarakat sebagai konsekuensi dari tingginya aktivitas pengolahan dan pertukaran data secara elektronik.

Dalam tiga tahun terakhir, transformasi digital layanan public menunjukan pertumbuhan signifikan melalui perluasan penerapan SPBE dan pemanfaatan NIK sebagai identitas digital. Namun, kemajuan ini diikuti oleh peningkatan insiden kebocoran data pribadi, yang mengidikasikan bahwa pencepatan digitalisasi belum sejalan dengan penguatan keamanan data, sehingga menimbulkan kekhawatiran mengenai keamanan sistem, tata kelola data, serta kesiapan Lembaga pemerintah dalam melindungi informasi pribadi masyarakat.

Rangkaian kasus tersebut memperlihatkan bahwa meskipun infrastuktur digital telah dikembangkan, sistem keamanan data sektor publik tetap rentan. Hal ini menujukan adanya kesenjangan antarra regulasi yang berlaku dan implementasinya di lapangan dan belum terintegritas dengan baik. Kondisi ini tidak hanya menurunkan tingkat kepercayaan masyarakat terhadap pemerintah, tetapi juga membuka peluang penyalahgunaan data oleh pihak-pihak yang tidak bertanggung jawab (Sabila et al., 2025).

Dalam tiga tahun terakhir, sejumlah insiden kebocoran data berskala besar yang melibatkan lembaga pemerintah terus terjadi. Pada tahun 2023 misalnya, terungkap kasus kebocoran sekitar 34juta data paspor yang diduga berasal dari server Direktorat Jenderal Imigrasi. Informasi yang terekspos mencakup identitas penting seperti nama lengkap, tanggal lahir, nomor paspor, hingga status kewarganegraan. Insiden ini memicu kekhawatiran mendalam karena data paspor merupakan dokumen sensitif yang sangat rentan disalahgunakan untuk tindakan kriminal, pemalsuan identitas, maupun kejahatan siber lainnya.

Pada tahun 2024, kasus serupa muncul kembali, kali ini melibatkan sekitar 204 juta data kependudukan yang dikelola oleh Dinas Kependudukan dan Pencatatan Sipil (Dukcapil). Data tersebut ditemukan diperjualbelikan di forum gelap (dark web), berisi informasi vital seperti Nomor Induk Kependudukan (NIK), data Kartu Keluarga (KK), Alamat, serta detail kependudukan lainnya. Besarnya skala kebocoran tersebut menimbulkan ancaman serius terhadap privasi dan keamanan masyarakat, mengingat data-data tersebut sangat mudah dimanfaatkan untuk penipuan, pencurian identitas, hingga penyalahgunaan dalam berbagai layanan digital.

Selanjutnya, pada tahun 2025 muncul dugaan kebocoran yang berkaitan dengan data transaksi pelayanan kesehatan disejumlah platfrom rumah sakit daerah. Tidak hanya itu, terdapat indikasi bahwa data penggunaaan aplikasi layanan publik berbasis Nomor Induk Kependudukan (NIK) juga turut terekspos. Dugaan kebocoran ini semakin mengkhawatirkan karena data kesehatan dan data kependudukan termasuk kategori informasi yang sangat sensitive. Penyalahgunaanya berpotensi menganacam kerahasiaan riwayat medis masyarakat, membuka peluang pencurian identitas, serta mengganggu keamanan sistem layanan public yang semakin terintegrasi secara digital.

Rentetan kasus selama tiga tahun berturut – turut ini memperlihatkan bahwa sistem keamanan data di sektor public masih belum kuat dan belum terintegrasi secara menyeluruh. Kondisi ini berpotensi menurunkan kepercayaan public, membuka peluang penipuan digital, phising, pencurian identitas, dan kejahatan siber lain.

Pemerintah telah merespons risiko ini melalui pengesahan Undang – Undang Nomor 27 Tahun 2022 tentang Data Pribadi (UU PDP) sebagai instrument hukum utama perlindungan data. Namun implementasi UU ini dalam pelayanan public masih menghadapi kendala teknis, kelembagaan, serta budaya keamanan data yang belum matang. Oleh karena itu, penting untuk menganalisis sejauh mana kebijakan tersebut telah dilaksanakan, apa hambatannya, dan bagaimana strategi penguatannya.

Pemerintah Indonesia telah mengambil langkah hukum melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai bentuk komitmen dalam memperkuat perlindungan data pribadi warga negara(Satria & Yusuf, 2024). Namun, implementasi kebijakan tersebut dalam pratik pelayanan public berbasis digital masih menghadapi berbagai kendala, seperti lemahnya koordinasi antarinstansi, keterbatasan sumber daya manusia di bidang keamanan siber, serta belum optimalnya infastruktur digital pemerintahan, Oleh karena itu, penting untuk menelaah sejauh mana kebijakan pemerintah telah diimplementasikan secra efektif dalam mencegah kebocoran data pribadi serta faktor-faktor apa saja yang menghambat pelaksanaannya (Kriswandaru et al., 2024).

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada tiga rumusan masalah utama, yaitu bagaimana implementasi kebijakan pemerintah dalam pencegahan kebocoran data pribadi pada pelayanan public berbasis digital, faktor apa saja yang menjadi kendala dalam penerapan kebijakan tersebut, serta upaya apa yang dapat dilakukan untuk meningkatkan efektivitas perlindungan data pribadi di lingkungan pelayanan publik digital.

Adapun tujuan penelitian ini adalah untuk menganalisis pelaksanaan kebijakan pemerintah dalam pencegahan kebocoran data pribadi mengidentifikasikan hambatan yang dihadapi dalam proses implementasinya, dan memberikan rekomendasi strategis guna memperkuat sistem pelindungan data pribadi disektor publik.

Beberapa penelitian sebelumnya telah membahas isu serupa, antara lain penelitian yang dilakukan oleh Susanto (2022) yang menyoroti lemahnya koordinasi antarintansi dalam pelaksanaan perlindungan data, serta Rahayu dan Nugroho (2023) yang menekankan dalamdemikian, kajian yang secara khusus meneliti implementasi kebijakan

pemerintah setelah berlakunya UU PDP dalam konteksnya pelayanan publik berbasis digital masi terbatas. Denagan demikian, penelitian ini diharapkan dapat memberikan kontribusi ilmiah dalam memahami efektivitas kebijakan pemerintah sekaligus memberikan mesukan untuk penguatan tata Kelola perlindungan data pribadi di Indonesia.

Penelitian ini mengkaji tiga isi utama, bagaimana implementasi kebijakan pemerintah dalam mencegah kebocoran data pribadi dilayanan public digital. Apa saja kendala yang menghambat efektivitas kebijakan. Upaya strategis apa yang dapat dilakukan untuk meningkatkan. Penelitian ini diharapkan berkontribusi dalam memperkuat tata kelola perlindungan data disektor publik serta memberikan rekomendasi untuk perbaikan kerangka implementasi UU PDP.

Metodologi

Penelitian ini menggunakan metode hukum normative dengan pendekatan perundang-undangan, konseptual, dan komparatif, serta diperkuat dengan data empiiris sekunder guna memperdalam analisis. Fokus penelitian diarahkan pada norma hukum yang mengatur perlindungan data pribadi, standar keamanan yang wajib diterapkan oleh pengendali data, serta kewajiban hukum instansi public setelah diperlakukannya Undang-Undang perlindungan data pribadi (UU PDP). Sumber data penelitian meliputi bahan hukum primer berupa UU PDP, Peraturan pemerintah Nomor 71 tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik, Permenkominfo Nomor 20 Tahun 2016, dokumen kebijakan sistem pemerintahan berbasis elektronik (SPBE), serta draf regulasi turunan UU PDP.

Selain itu, penelitian ini memanfaatkan bahan hukum sekunder seperti jurnal ilmiah, laporan badan siber dan sandi Negara (BSSN), laporan tahunan kementrian komunikasi dan informatika (kominfo) priode 2023-2025, laporan indeks SPBE nasional, survei literasi digital, serta ensikolpedia dan sumber ilmiah kredibel lainnya. Data pendukung berupa statistic insiden kebocoran data yang tercatat sebanyak 144 insiden pada 2023, meningkat menjadi 176 insiden pada 2024, dan mencapai 198 insiden hingga oktober 2025 dijadikan rujukan unntuk menggambarkan tingkat resiko keamanan data di sektor publik. Nilai indekas SPBE nasional yang berada pada kategori ''cukup'' (rentan 2,3-2,6) dan tingkat literasi digital masyarakat yang berada pada kategori ''sedang'' pada tahun 2023-2025 turut memberiikan konteks empiris terhadap efektivitas tata kelola data nasional. Analisis dilakukan menggunakan metode kualitatif normative dengan mengidentifikasikan norma yang berlaku, mengevaluasi kesesuaian antara ketentuan hukum dan praktik implementasi di lapangan, serta menilai efektivitas penerapan UU PDP berdasarkan teori efektivitas hukum Soekarno Soekanto.

Hasil dan Pembahasan

Implementasi Kebijakan Pemerintah: Kemajuan dan Praktik di Lapangan

Pemerintah Indonesia telah menunjukkan komitmen kuat dalam memperkuat perlindungan data pribadi melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)(Tahun et al., 2023). UU ini hadir sebagai

tonggak penting yang pertama kali memberikan kerangka hukum komprehensif mengenai tata kelola data pribadi di Indonesia. Substansi UU PDP mencakup pengaturan hak-hak subjek data, kewajiban pengendali dan prosesor data, mekanisme pemrosesan data, hingga sanksi administratif dan pidana atas pelanggaran(Republik, 2022). Keberadaan aturan ini menandai pergeseran paradigma dari sekadar kebijakan sektoral menuju regulasi nasional yang menyeluruh. UU PDP juga mengadopsi prinsip-prinsip global seperti *lawfulness*, *transparency*, *purpose limitation*, *data minimization*, *accountability*, dan *security* yang selama ini diterapkan dalam standar internasional seperti General Data Protection Regulation (GDPR) Uni Eropa. Dengan adopsi prinsip tersebut, Indonesia berupaya menghadirkan sistem perlindungan data yang setara dengan standar global, sekaligus memberikan kepastian hukum bagi penyelenggara layanan digital di sektor publik maupun privat(Akbar et al., 2024).

Pelaksanaan UU PDP pada praktiknya didukung oleh berbagai kerangka regulatif yang telah ada sebelumnya, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), yang mengatur kategori penyelenggara sistem elektronik, kewajiban pencadangan data, hingga standar keamanan minimum. Di samping itu, Permenkominfo Nomor 20 Tahun 2016 mengenai Perlindungan Data Pribadi dalam Sistem Elektronik menjadi panduan teknis awal dalam implementasi pengamanan data, mencakup kewajiban notifikasi kebocoran data, penerapan enkripsi, serta kewajiban penyimpanan data di wilayah Indonesia(Jawab et al., 2025). Selain regulasi berbasis teknologi, kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) juga menjadi instrumen strategis dalam integrasi digital antarinstansi pemerintah. SPBE menetapkan standar arsitektur, manajemen risiko keamanan informasi, dan interoperabilitas data lintas instansi. Integrasi ini memperluas pemanfaatan data pribadi untuk pelayanan publik, tetapi juga menuntut peningkatan keamanan yang lebih ketat. Dalam konteks pengawasan, peran Kementerian Komunikasi dan Informatika (Kominfo) sebagai regulator dan Badan Siber dan Sandi Negara (BSSN) sebagai otoritas teknis keamanan siber menjadi sangat penting dalam memastikan implementasi UU PDP berjalan sesuai ketentuan(Aqilla, 2025).

Dalam tataran implementasi di lapangan, sejumlah lembaga pemerintah telah mulai menerapkan pengamanan berbasis teknologi sesuai prinsip-prinsip perlindungan data. Dinas Kependudukan dan Pencatatan Sipil (Dukcapil) misalnya, menerapkan sistem berbasis Nomor Induk Kependudukan (NIK) dengan pengaturan hak akses yang ketat, *role-based access control*, serta autentikasi berlapis bagi lembaga pengguna(No, 2017). Sistem ini terhubung dengan ribuan instansi lain sehingga memerlukan standar keamanan khusus. BPJS Kesehatan juga memperkuat sistem perlindungan data peserta dengan menerapkan *two-factor authentication*, enkripsi data end-to-end, tokenisasi identitas, serta *monitoring* aktivitas sistem untuk mencegah penyalahgunaan akses. Pada Kementerian Kesehatan, pembenahan dilakukan menyeluruh setelah terjadinya kebocoran data aplikasi e-HAC tahun 2021, dengan meningkatkan enkripsi, perbaikan API, serta penguatan kebijakan penyimpanan data medis. Sementara itu, Direktorat Jenderal Imigrasi melakukan perbaikan signifikan terhadap manajemen server setelah insiden kebocoran 34 juta data

paspor pada 2023, termasuk penerapan *zero-trust architecture* yang menuntut verifikasi ketat terhadap setiap akses internal maupun eksternal.

Meskipun berbagai instansi telah menunjukkan kemajuan, temuan penelitian menunjukkan bahwa implementasi kebijakan perlindungan data masih belum berjalan merata di seluruh sektor pemerintahan. Sebagian besar lembaga pemerintah belum memiliki *Data Protection Officer* (DPO) yang seharusnya menjadi garda depan dalam pengawasan tata kelola data pribadi sebagaimana diwajibkan UU PDP. Selain itu, banyak instansi tidak melaksanakan audit keamanan data secara periodik sehingga celah kerentanan tidak teridentifikasi sejak dini. Penggunaan sistem lama (*legacy system*) tanpa pembaruan keamanan juga menjadi faktor yang menambah risiko kebocoran data. Sistem tersebut umumnya tidak memiliki teknologi enkripsi modern, tidak mendukung autentikasi berlapis, serta tidak kompatibel dengan arsitektur keamanan siber yang diwajibkan oleh standar SPBE dan BSSN. Ketidakmerataan ini menyebabkan pelaksanaan kebijakan perlindungan data sangat bergantung pada kapasitas masing-masing instansi, sehingga meskipun kerangka hukum nasional telah tersedia, implementasinya masih jauh dari ideal.

Temuan Lapangan: Penyebab Kebocoran Data 2023–2025

Berdasarkan hasil penelitian, peningkatan insiden kebocoran data pribadi dari tahun 2023 hingga Oktober 2025 menunjukkan pola kerentanan yang konsisten dan berulang pada berbagai instansi pemerintah. Data yang tercatat 144 insiden pada 2023, meningkat menjadi 176 pada 2024, dan mencapai 198 insiden hingga Oktober 2025 menggambarkan bahwa pelaksanaan kebijakan perlindungan data belum mampu mengimbangi percepatan digitalisasi pelayanan publik(Pradhipta1 & Universitas, 2025). Tren kenaikan ini menunjukkan bahwa risiko keamanan data tidak hanya muncul dari faktor teknis, tetapi juga merupakan akumulasi kelemahan struktural, kelembagaan, dan sumber daya manusia. Temuan lapangan mengungkap bahwa terdapat lima penyebab utama yang memicu tingginya insiden kebocoran data dalam kurun waktu tersebut.

Faktor pertama adalah kelemahan keamanan teknis yang masih dominan di banyak instansi pemerintah. Kasus kebocoran 34 juta data paspor tahun 2023 menjadi contoh paling jelas, di mana penyebab utamanya bukan serangan siber canggih, tetapi kesalahan konfigurasi server yang membuat data dapat diakses secara publik(Sari et al., 2024). Kasus serupa terjadi pada kebocoran 204 juta data kependudukan yang dikelola Dukcapil pada 2024, yang dipicu oleh integrasi API lintas instansi yang tidak terkontrol, sehingga pihak ketiga dapat mengakses data secara ilegal(Ndaru et al., 2025). Selain itu, sebagian besar pemerintah daerah masih menggunakan server lokal yang tidak dilindungi dengan *cloud security* tersertifikasi, tidak memiliki sistem enkripsi memadai, serta tidak dilengkapi mekanisme pencadangan data (*backup*) yang aman. Kondisi teknis seperti ini menyebabkan data rentan terhadap pencurian, manipulasi, maupun *ransomware*, terutama ketika perangkat lunak tidak diperbarui secara berkala.

Faktor kedua adalah ketidakamanan integrasi data antarinstansi akibat penggunaan sistem berbasis Nomor Induk Kependudukan (NIK) yang terhubung dengan ribuan

lembaga pengguna. Meskipun integrasi ini memudahkan administrasi dan mempercepat layanan publik, sistem tersebut menjadi sangat rentan ketika standar teknis antarinstansi berbeda-beda(Dwi et al., 2025). Lembaga dengan sistem keamanan rendah dapat menjadi "pintu masuk" bagi pelaku kejahatan siber untuk mengakses database pusat. Penelitian menemukan bahwa banyak instansi pemerintah daerah dan lembaga mitra tidak mengikuti standar keamanan nasional, seperti enkripsi data, autentikasi dua faktor, atau pembatasan akses berbasis peran. Akibatnya, semakin luas penyebaran akses data antarinstansi, semakin besar pula kemungkinan kebocoran data terjadi karena lemahnya salah satu titik akses.

Faktor ketiga adalah kurangnya pengawasan dan audit keamanan secara berkala di berbagai lembaga pemerintah. Hasil penelitian menunjukkan bahwa sebagian besar instansi tidak menjalankan mekanisme audit keamanan rutin, tidak melakukan penilaian risiko (*risk assessment*), dan tidak menerapkan sistem pemantauan aktivitas (*logging monitoring*) yang memadai(M. Saleh, 2025). Tanpa audit, celah keamanan yang muncul tidak teridentifikasi sejak dini, sehingga pelanggaran sering kali baru diketahui setelah terjadi penyalahgunaan data dalam skala besar. Ketiadaan *logging monitoring* juga membuat instansi kesulitan melacak jejak digital pelaku atau mengetahui titik awal kebocoran. Kondisi ini menggambarkan kurangnya kesadaran institusional bahwa keamanan siber membutuhkan pemantauan berkelanjutan, bukan hanya pemasangan perangkat teknologi.

Faktor keempat adalah rendahnya kompetensi sumber daya manusia (SDM) di bidang keamanan data dan keamanan siber. Penyelenggaraan sistem elektronik di instansi pemerintah masih didominasi oleh aparatur yang belum memahami prinsip dasar perlindungan data pribadi. Praktik yang tidak aman, seperti penggunaan kata sandi yang lemah, penggunaan satu akun untuk banyak pegawai, dan penyimpanan data pribadi tanpa enkripsi, masih sering ditemui. Selain itu, banyak operator sistem tidak melakukan pembaruan perangkat lunak (*update patching*) secara berkala, padahal pembaruan tersebut penting untuk menutup celah keamanan yang telah diidentifikasi oleh pengembang(Khoironi, 2020). Rendahnya literasi siber pada ASN menyebabkan prosedur keamanan sering diabaikan, bahkan dianggap sebagai hambatan bagi kelancaran pekerjaan(Sidoarjo et al., 2025).

Faktor kelima adalah belum optimalnya peran otoritas pengawas independen, yaitu Otoritas Perlindungan Data Pribadi (OPDP) yang hingga 2025 belum berfungsi sepenuhnya. Ketiadaan lembaga pengawas yang kuat menyebabkan pengawasan, audit, investigasi, serta penegakan sanksi administratif terhadap pelanggaran data tidak berjalan maksimal. Banyak kasus kebocoran data tidak mendapatkan proses investigasi resmi atau tindak lanjut yang tegas, sehingga tidak menimbulkan efek jera bagi instansi yang lalai. Dalam beberapa kasus, instansi publik hanya memberikan klarifikasi tanpa melakukan perbaikan struktural yang diperlukan. Keadaan ini mengakibatkan pelaksanaan UU PDP kurang efektif, karena regulasi tidak didukung oleh mekanisme penegakan yang kuat dan mandiri.

Secara keseluruhan, temuan penelitian menunjukkan bahwa kebocoran data selama 2023–2025 merupakan hasil dari kombinasi kelemahan teknis, kesenjangan standar

keamanan antarinstansi, minimnya audit internal, rendahnya kompetensi SDM, dan belum berfungsinya lembaga pengawasan yang seharusnya menjadi penjaga utama kepatuhan UU PDP(Soleh et al., 2024). Dengan demikian, keberhasilan implementasi perlindungan data tidak hanya ditentukan oleh regulasi yang kuat, tetapi juga oleh kesiapan teknis, kelembagaan, dan budaya keamanan yang harus dibangun secara menyeluruh di seluruh sektor pemerintahan.

Analisis Efektivitas Implementasi

Evaluasi efektivitas implementasi kebijakan perlindungan data pribadi dalam penelitian ini menggunakan kerangka teori efektivitas hukum Soerjono Soekanto, yang menilai keberhasilan suatu regulasi melalui empat unsur utama: substansi hukum, struktur penegak hukum, sarana dan prasarana, serta budaya hukum masyarakat. Analisis ini menunjukkan bahwa meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah hadir sebagai regulasi yang kuat dan komprehensif, efektivitas pelaksanaannya di lapangan masih terhambat oleh lemahnya koordinasi kelembagaan, ketimpangan infrastruktur, kurangnya sumber daya manusia yang kompeten, serta budaya kepatuhan yang belum terbentuk secara matang(Rinjani & Firmansyah, 2025).

Dari aspek substansi hukum, penelitian ini menemukan bahwa kerangka normatif yang disediakan UU PDP sebenarnya sudah cukup lengkap dan setara dengan standar internasional. UU tersebut mengatur definisi data pribadi, hak-hak subjek data, kewajiban pengendali data, prinsip pemrosesan data, prosedur pelaporan insiden, hingga sanksi administratif, perdata, dan pidana. Namun demikian, kelemahan muncul pada level operasional karena regulasi turunan sebagai pedoman teknis belum seluruhnya disusun atau diterbitkan. Beberapa aspek krusial seperti standar enkripsi nasional, klasifikasi tingkat sensitivitas data, tata cara retensi dan pemusnahan data, serta panduan audit keamanan belum seragam diterapkan di seluruh instansi. Akibatnya, walaupun landasan hukum tersedia, tidak terdapat mekanisme teknis yang baku untuk memastikan seluruh lembaga pemerintah mengimplementasikan aturan tersebut secara konsisten(Press, n.d.). Dengan demikian, substansi hukum yang kuat belum dapat berfungsi secara optimal karena tidak didukung perangkat teknis yang memadai.

Dari unsur struktur penegak hukum, ditemukan bahwa kelembagaan yang bertanggung jawab atas pelaksanaan UU PDP bekerja secara parsial dan tidak terkoordinasi. Kominfo sebagai regulator utama, Dukcapil sebagai pengelola data kependudukan, BPJS sebagai pengelola data kesehatan, serta BSSN sebagai otoritas teknis keamanan siber, memiliki tugas yang berbeda-beda dan belum terintegrasi dalam satu mekanisme kontrol terpadu(Sorisa & Kiareni, 2024). Ketiadaan Otoritas Perlindungan Data Pribadi (OPDP) sebagai lembaga independen khusus yang diamanatkan UU PDP menyebabkan penegakan hukum berjalan tanpa otoritas tunggal yang jelas. Beberapa kasus kebocoran data tidak ditangani secara terpadu, dan instansi cenderung hanya memberikan klarifikasi informatif tanpa pemeriksaan mendalam atau sanksi administratif yang tegas. Fragmentasi struktur ini menunjukkan bahwa efektivitas kebijakan perlindungan data lebih

terhambat oleh lemahnya koordinasi dan ketidakjelasan peran antarinstansi daripada oleh ketiadaan regulasi(Madura, 2025).

Dari aspek sarana dan prasarana, penelitian menemukan bahwa kesiapan infrastruktur keamanan data antarinstansi pemerintah sangat timpang. Di tingkat pusat, beberapa lembaga telah mulai mengadopsi *cloud security* tersertifikasi, menerapkan enkripsi modern, dan membangun pusat data yang relatif lebih aman. Namun sebagian besar instansi pemerintah daerah masih menggunakan server lokal yang tidak dirancang untuk menahan serangan siber modern. Selain tidak didukung sistem enkripsi yang memadai, banyak server daerah tidak memiliki mekanisme pencadangan, *intrusion detection system*, atau pembaruan keamanan (*patching*) yang memadai. Ketimpangan ini semakin diperparah oleh minimnya tenaga ahli keamanan siber bersertifikasi yang mampu mengelola sistem tersebut. Berdasarkan hasil observasi, hanya sebagian kecil instansi yang memiliki staf TI dengan kompetensi keamanan tingkat lanjut, padahal UU PDP mengharuskan adanya pengangkatan pejabat perlindungan data pribadi atau *Data Protection Officer* (DPO). Kekurangan sarana dan SDM ini mengakibatkan standar keamanan tidak dapat diterapkan secara merata, sehingga meningkatkan risiko kebocoran data, terutama pada instansi dengan kapasitas teknis rendah.

Unsur terakhir adalah budaya hukum, yang mencakup tingkat kepatuhan dan kesadaran subjek hukum terhadap aturan yang berlaku. Penelitian ini menemukan bahwa budaya perlindungan data pribadi di kalangan aparatur sipil negara (ASN) masih rendah. Banyak ASN yang mengabaikan prinsip dasar keamanan informasi, misalnya menggunakan kata sandi yang sama untuk berbagai sistem, berbagi akun antarpegawai, atau mengakses sistem menggunakan perangkat pribadi yang tidak aman. Kurangnya literasi keamanan digital menyebabkan aturan dianggap sebagai beban administratif, bukan sebagai kewajiban untuk melindungi hak warga negara(Nuruzzaman et al., 2025). Di sisi lain, masyarakat umum juga belum memahami hak-hak mereka sebagai subjek data, seperti hak mendapatkan informasi pengolahan data, hak mengajukan keberatan, atau hak meminta penghapusan data. Rendahnya kesadaran ini membuat masyarakat jarang melapor, sehingga insiden kebocoran data sering tidak terdeteksi atau tidak mendapatkan tekanan publik yang cukup untuk mendorong perbaikan.

Dari keempat unsur tersebut, penelitian menyimpulkan bahwa kegagalan utama dalam implementasi perlindungan data bukan berasal dari kelemahan regulasi, melainkan dari keterbatasan struktur penegakan, minimnya sarana teknis dan SDM, serta budaya hukum yang belum mendukung keamanan data sebagai prioritas nasional. Dengan demikian, upaya memperkuat efektivitas UU PDP tidak cukup dilakukan melalui penyempurnaan regulasi, tetapi harus mencakup peningkatan kapasitas institusi pengawas, pemerataan infrastruktur keamanan, peningkatan kompetensi ASN, serta pembentukan budaya perlindungan data yang kuat di seluruh lapisan masyarakat.

Upaya Perbaikan yang Dilakukan Pemerintah

Pemerintah telah mengambil langkah struktural yang cukup penting dengan mendorong pembentukan Otoritas Perlindungan Data Pribadi (OPDP) sebagai lembaga

independen yang kelak akan memegang fungsi pengawasan, audit kepatuhan, investigasi pelanggaran, dan pemberian sanksi administratif(Matheus & Gunadi, 2024). Meskipun pembentukan OPDP belum final dan masih dalam proses penyelesaian aturan pelaksanaannya sejumlah laporan menyatakan bahwa peraturan pelaksana (RPP) dan mekanisme kelembagaan sedang dimatangkan sehingga lembaga ini belum beroperasi penuh inisiatif ini dipandang sebagai respons langsung terhadap kebutuhan penegakan yang terpusat dan independen pasca-pemberlakuan UU PDP. Kehadiran OPDP diharapkan menyatukan fungsi pengawasan yang selama ini tersebar dan memberikan instrument penegakan yang lebih jelas dibandingkan model pengawasan yang fragmentaris.

Untuk memperbaiki kapasitas manusia dan respons operasional, Kominfo dan Badan Siber dan Sandi Negara (BSSN) menjalankan program penguatan SDM melalui pelatihan keamanan siber dan program sertifikasi teknis bagi ASN dan operator TI di lembaga publik(Sutra & Haryanto, 2023). Pelatihan yang dilaksanakan mencakup modul dasar hingga lanjutan mengenai keamanan jaringan, manajemen insiden, pengamanan aplikasi, dan etika siber; selain itu BSSN menyediakan jalur sertifikasi bagi auditor keamanan dan asisten auditor, sedangkan Kominfo menjalankan pelatihan yang juga menekankan aspek kebijakan dan kepatuhan regulatif. Upaya ini tidak hanya menargetkan pejabat teknis tetapi juga melibatkan manajer dan pimpinan unit agar budaya keamanan tertanam pada level kebijakan institusi, serta mendorong pembentukan tim respons insiden (CSIRT/internal CERT) di tiap instansi sebagai unit reaksi pertama saat terjadi insiden.

Sejalan dengan penguatan SDM, pemerintah telah mengintensifkan audit keamanan SPBE sebagai bagian dari upaya pengawasan kepatuhan teknis. BSSN menerbitkan standar dan tata cara pelaksanaan audit keamanan SPBE yang merinci objek audit, kriteria penilaian, mekanisme pelaporan, dan tindak lanjut audit sehingga audit tidak lagi bersifat ad-hoc tetapi menjadi bagian rutin dari siklus pengelolaan risiko keamanan informasi. Beberapa kementerian/lembaga pusat telah mulai melakukan audit internal maupun eksternal sesuai kerangka ini, termasuk penilaian desain kontrol, implementasi kontrol, dan efektivitas kontrol. Hasil audit digunakan sebagai dasar perencanaan mitigasi dan penganggaran untuk perbaikan infrastruktur. Namun implementasi audit masih belum merata di tingkat daerah, sehingga ketimpangan risiko tetap ada.

Dalam dimensi kesadaran publik, pemerintah menggalakkan program literasi digital nasional yang memuat materi perlindungan data pribadi tujuannya untuk meningkatkan pemahaman masyarakat tentang hak subjek data, risiko berbagi informasi pribadi, serta prosedur pelaporan apabila terjadi pelanggaran. Program literasi ini dijalankan lewat kombinasi kampanye publik, modul pembelajaran daring, pelatihan komunitas, serta integrasi materi di program pembinaan ASN. Upaya ini penting untuk menciptakan demand-side pressure yakni masyarakat yang lebih paham dan lebih aktif menuntut akuntabilitas yang diharapkan dapat melengkapi supply-side reform (regulasi dan pengawasan) dalam memperbaiki kepatuhan lembaga publik.

Terakhir, pemerintah memperkuat upaya yang berskala internasional dan regional melalui partisipasi dalam kerangka kerja ASEAN dan inisiatif standardisasi lintas negara. Keterlibatan dalam dokumen-dokumen kebijakan ASEAN mengenai ekonomi digital dan

tata kelola data membuka peluang untuk harmonisasi prinsip perlindungan data, pertukaran praktik terbaik, serta kerjasama teknis misalnya dalam aspek transfer data lintas batas, penguatan kapasitas penegakan, atau adopsi standar keamanan. Kerja sama semacam ini membantu Indonesia menyelaraskan kebijakan domestik dengan standar regional/global dan memperluas akses pada sumber daya teknis serta pelatihan yang relevan.

Secara sintetis, upaya-upaya tersebut (pembentukan OPDP, penguatan SDM, audit SPBE berkala, literasi digital, dan kerja sama internasional) membentuk paket kebijakan yang holistik. Namun efektivitasnya masih bergantung pada percepatan aturan pelaksana UU PDP, pendanaan berkelanjutan untuk program audit dan pelatihan, serta kemampuan memastikan pemerataan implementasi terutama di tingkat daerah agar manfaat kebijakan dirasakan secara nasional. Jika diperlukan, saya bisa mengubah paragraf ini menjadi versi yang lebih panjang dengan sub-bagian per langkah (mis. detail program pelatihan BSSN, struktur OPDP yang diusulkan, atau mekanisme audit SPBE) dan menyisipkan kutipan langsung atau lampiran peraturan terkait.

Sintesis: Tingkat Efektivitas Implementasi

Berdasarkan seluruh temuan penelitian, dapat disimpulkan bahwa meskipun kerangka regulatif untuk perlindungan data pribadi terutama melalui UU No. 27/2022 cukup kuat secara normatif, implementasinya di lapangan masih lemah. Kekuatan regulasi terlihat pada cakupan norma (hak subjek data, kewajiban pengendali/prosesor, mekanisme pelaporan dan sanksi), namun kekosongan pada level operasional seperti belum lengkapnya regulasi turunan, pedoman teknis, dan standar implementasi membuat norma tersebut sulit dioperasionalisasikan secara konsisten oleh instansi publik. Dengan kata lain, hukum ada, tetapi instrumen teknis dan panduan penerapan yang diperlukan untuk menerjemahkan kewajiban hukum ke praktik sehari-hari masih belum memadai.

Perkembangan infrastruktur digital pemerintah yang pesat tidak diikuti oleh peningkatan kemampuan keamanan yang sebanding. Transformasi digital telah mendorong adopsi sistem berbasis NIK, interoperabilitas layanan, dan migrasi sebagian layanan ke platform digital; namun hal ini juga menambah kompleksitas permukaan serangan dan kebutuhan pengamanan. Banyak instansi pusat telah memperbarui infrastruktur mereka, tetapi ketimpangan teknis antara pusat dan daerah serta keberadaan *legacy systems* yang rentan menyebabkan keseluruhan ekosistem tetap lemah. Akibatnya, peningkatan jumlah dan kompleksitas layanan digital justru memperbesar eksposur risiko, sehingga terjadinya kebocoran data bukan sekadar masalah teknis lokal melainkan masalah sistemik(Tommy et al., 2025).

Walaupun pemerintah telah mengeluarkan berbagai kebijakan dan inisiatif untuk perlindungan data, penerapan kebijakan tersebut belum konsisten antarinstansi. Fragmentasi kebijakan terlihat pada variasi pedoman teknis, perbedaan kapasitas institusi, dan praktik yang beragam dalam pengelolaan akses data. Ketidakkonsistenan ini muncul karena tidak adanya mekanisme koordinasi yang efektif yang memaksa standar teknis dan prosedural diimplementasikan secara seragam; alih-alih menciptakan jaring pengaman

nasional, variasi implementasi menghasilkan titik-titik lemah yang dapat dieksploitasi. Konsistensi kebijakan membutuhkan instrumen pengatur yang memaksa kepatuhan bukan sekadar himbauan serta alur koordinasi dan pertukaran informasi antar-otoritas yang jelas.

Rendahnya kesadaran keamanan baik di kalangan aparatur negara maupun public menjadi faktor pemicu lain yang menjaga angka kebocoran tetap tinggi. Praktik-praktik sederhana namun krusial (mis. manajemen kata sandi yang buruk, berbagi akun, kurangnya verifikasi akses, malas melakukan *patching*) masih umum terjadi, yang mengindikasikan bahwa perubahan teknologi tidak disertai perubahan perilaku. Di tingkat publik, kelemahan literasi data membuat warga kurang paham haknya sehingga jarang menuntut pertanggungjawaban atau melapor melanggar; hal ini mengurangi tekanan sosial dan politik yang diperlukan untuk memaksa perubahan institusional.

Sintesis temuan menunjukkan bahwa kegagalan relatif dalam pencegahan kebocoran data adalah masalah multidimensional: bukan hanya ketiadaan aturan, melainkan kegagalan pada lapisan implementasi yang melibatkan koordinasi kelembagaan, standarisasi teknis, kapasitas manusia, pengawasan independen, dan budaya kepatuhan. Untuk menjembatani kesenjangan ini diperlukan pendekatan terpadu: (1) mempercepat finalisasi regulasi turunan yang mengikat standar teknis (mis. enkripsi minimum, klasifikasi data, retensi dan pemusnahan), (2) membangun mekanisme koordinasi nasional yang memaksa interoperabilitas aman (mis. perjanjian layanan antar-instansi dan sertifikasi API), (3) melakukan investasi berkelanjutan pada peningkatan SDM (pelatihan bersertifikat, rekrutmen DPO dan tim CSIRT di setiap lembaga), (4) mengaktifkan OPDP dengan kewenangan independen dan kapasitas investigasi + sanksi efektif, serta (5) menjalankan program literasi dan kampanye budaya keamanan yang menyasar ASN dan publik sekaligus.

Secara praktis, efektivitas UU PDP akan meningkat apabila perbaikan teknis dan kelembagaan dipacu serentak: aturan tanpa kapasitas atau pengawasan hanya sempalan teks hukum; infrastruktur tanpa budaya dan SDM hanya memberi false sense of security; sementara pengawasan tanpa pedoman teknis yang jelas akan menghasilkan tindakan yang inkonsisten. Oleh karena itu, rekomendasi kebijakan terarah harus menggabungkan reformasi regulatif, penguatan institusional, peningkatan sumber daya manusia, dan upaya perubahan budaya untuk menurunkan risiko kebocoran data secara signifikan dan berkelanjutan.

Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa implementasi kebijakan perlindungan data pribadi dalam pelayanan publik berbasis digital di Indonesia telah menunjukkan kemajuan normatif melalui pengesahan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, namun efektivitasnya masih belum optimal dalam praktik. Temuan menunjukkan bahwa tingginya insiden kebocoran data pada periode 2023–2025 merupakan implikasi dari ketidakseimbangan antara percepatan digitalisasi dan kesiapan sistem keamanan, yang dipengaruhi oleh lemahnya keamanan teknis, belum meratanya standar perlindungan data antarinstansi, minimnya audit dan pengawasan, rendahnya

kompetensi SDM, serta belum berfungsinya otoritas pengawas independen secara efektif. Implikasi penting dari temuan ini adalah bahwa keberadaan regulasi yang kuat tidak secara otomatis menjamin perlindungan data tanpa dukungan struktur kelembagaan, sarana prasarana, dan budaya hukum yang memadai. Oleh karena itu, penelitian ini merekomendasikan penguatan implementasi UU PDP melalui percepatan pembentukan dan pengoperasian Otoritas Perlindungan Data Pribadi, kewajiban audit keamanan data secara berkala, peningkatan kapasitas SDM aparatur di bidang keamanan siber, serta harmonisasi standar teknis perlindungan data lintas instansi. Untuk penelitian selanjutnya, disarankan dilakukan kajian empiris mendalam pada instansi tertentu atau perbandingan internasional guna menilai praktik terbaik (best practices) perlindungan data publik yang dapat diadaptasi dalam konteks tata kelola digital Indonesia.

Daftar Pustaka

Akbar, M., Pradana, E., & Saragih, H. (2024). Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya. *Journal Of Social Science Research Volume*, *4*, 3412–3425. https://j-innovative.org/index.php/Innovative%0APrinsip

Aqilla, N. P. (2025). PERAN DATA GOVERNANCE DALAM KEAMANAN DAN. *Multidisiplin Ilmu Akademik*, *2*(3), 217–221.

Dwi, S., Siregar, P., Irwan, M., & Nasution, P. (2025). *Peran Data Integration Dalam Mewujudkan Interoperabilitas Sistem Informasi*. *02*(June), 555–560.

Jawab, T., Pidana, H., & Elektronik, P. (2025). *Tanggung Jawab Hukum Pidana Penyelenggara Elektronik Perbankan terhadap Perlindungan Data Pribadi Nasabah*. *5*(2).

Khoironi, S. C. (2020). PENGARUH ANALISIS KEBUTUHAN PELATIHAN BUDAYA KEAMANAN SIPIL NEGARA DI ERA DIGITAL ANALYSIS CYBER SECURITY CULTURE TRAINING NEEDS AS AN EFFORT TO DEVELOP COUNTRY CIVIL APARATURES COMPETENCY IN DIGITAL ERA. *JURNAL STUDI KOMUNIKASI DAN MEDIA*, *24*(1), 37–56. https://jkd.komdigi.go.id/index.php/jskm/article/view/2945

Kriswandaru, A. S., Pratiwi, B., Studi, P., Hukum, I., Studi, P., Hukum, I., Kewirausahaan, P. S., Info, A., Data, P., Hukum, K., Data, P., & Hukum, P. (2024). *Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus*. *2*(4), 740–755. https://doi.org/10.51903/hakim.v2i04.2157

M. Saleh, M. D. F. (2025). *Audit Keamanan Website Layanan Publik Mengacu pada ISO / IEC 27001 : Studi Kasus Dugaan Penyalahgunaan Situs PeduliLindungi*. *3*(7), 554–560.

Madura, U. W. (2025). PERLINDUNGAN HUKUM BAGI KORBAN ATAS KEBOCORAN PUSAT DATA NASIONAL SEMENTARA (PDNs) PERSPEKTIF PERLINDUNGAN DATA PRIBADI. *Jurnal Jendela Hukum*, *12*(September), 89–122. https://www.ejournalwiraraja.com/index.php/FH

Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU. *Justisi*, *10*(1), 20–35.

Ndaru, A. D., Aljawari, M., & Setiawan, M. Y. (2025). *Implementasi REST API Pengelolaan Data Penduduk Multi-Desa Berbasis Laravel dengan Autentikasi Sanctum OpenSID sudah cukup mapan dalam hal fitur internal , banyak implementasi OpenSID di (API) sebagai mekanisme pertukaran data yang fleksibel dan efisien antar sistem (Atmojo et struktur database OpenSID . Laravel dipilih karena memiliki kapabilitas tinggi dalam dokumentasi otomatis API melalui Laravel Scribe (Asnawi et al ., 2024). berbagai konteks , seperti sistem pengarsipan surat di kantor desa dan manajemen data dan efisiensi pelayanan publik . Dari sisi metodologi , pengembangan dilakukan menggunakan*. *3*.

No, J. G. (2017). IMPLEMENTASI ROLE-BASED ACCESS CONTROL (RBAC) PADA PEMANFAATAN DATA KEPENDUDUKAN DITINGKAT KABUPATEN. *Jurnal.Umj*, *November*, 1–2.

Nuruzzaman, M. T., Wirawan, A., Muslimah, U. S., & Setyono, Y. (2025). Kesiapan Aparatur Sipil Negara (ASN) Terhadap Implementasi UU Pelindungan Data Pribadi (UU PDP) The Readiness of Civil Servants (ASN) for the Implementation of the Personal Data Protection Act (PDP Act). *CyberSecurity Dan Forensik Digital*, *8*(1), 63–71.

Pradhipta1, A. P., & Universitas, I. G. N. K. Y. (2025). *ANALISIS REGULASI PERLINDUNGAN DATA PRIBADI TERHADAP KASUS KEBOCORAN DATA DI INDONES*. *3*(7).

Press, U. (n.d.). *Keamanan Digital Dalam Audit Pajak : Integrasi Cyber Security dengan CRM , BDA , dan BI untuk Revolusi Compliance*.

Republik, N. (2022). *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI*. *016999*.

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27 / 2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70–83.

Sabila, S. N., Atman, W., Ilmu, D., Internasional, H., & Hasanuddin, U. (2025). *Studi Kasus Kebocoran Data SIM Card oleh Bjorka : Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia*. *2*.

Sari, H. P., Mulyani, D. I., Nilamsari, M. A., Dimas, D., Sitorus, F., & Harimurti, Y. W. (2024). EFEKTIVITAS HUKUM PERLINDUNGAN DATA PRIBADI. *MEDIA AKADEMIK (JMA)*, *2*(11). https://doi.org/10.62281, Hal XX-XX

Satria, M. K., & Yusuf, H. (2024). *Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Legal Analysis of Doxing Criminal Actions Reviewed Based on Law Number 27 of 2022 Concerning Personal Data Protection*. *1*, 2442–2456.

Sidoarjo, D. K., Astrialita, P., Veteran, U. P. N., & Timur, J. (2025). *Tingkat Literasi Digital ASN Terhadap Aplikasi Kepegawaian*. *4*(1), 6–11.

Soleh, M., Tjenreng, Z., Pacasarjana, S., & Terapan, M. (2024). *STRATEGI PENCEGAHAN KEBOCORAN DATA PELAYANAN PUBLIK*. *11*(1), 1–10.

Sorisa, C., & Kiareni, C. L. (2024). Etika Keamanan Siber : Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia. *Sains Student Research*, *2*(6), 586–593.

Sutra, S. M., & Haryanto, A. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh

Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, *7*(April), 56–69. https://doi.org/10.34010/gpsjournal.v7i1

Tahun, U. U. N. O., Saly, J. N., Artamevia, H., Kheista, K., Juni, B., Gulo, S., Rhemrev, E. A., & Christie, M. (2023). *ANALISIS PERLINDUNGAN DATA PRIBADI TERKAIT*. *1*(3), 145–153.

Tommy, S., Irwan, M., & Nasution, P. (2025). Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah : Studi Kasus Pusat Data Nasional (PDN). *Jurnal Ilmiah Ekonomi Dan Manajemen Vol.3*, *3*(6), 330–346. https://ejurnal.kampusakademik.co.id/index.php/jiem/article/view/5266/4577