Maeswara : Jurnal Riset Ilmu Manajemen dan Kewirausahaan
Volume. 3 Nomor. 3 Juni 2025
e-ISSN : 2988-5000; p-ISSN : 2988-4101, Hal. 01-11
DOI: https://doi.org/10.61132/maeswara.v3i3.1750
Available online at: https://journal.arimbi.or.id/index.php/Maeswara

Perlindungan Data Privasi dalam Sistem Database Digital: Regulasi, Tinjauan Etika, dan Strategi Teknis

Nurkhaliza[1], Muhammad Irwan Padli Nasution[2],
[1,2] Universitas Islam Negeri Sumatera Utara

Alamat: Jl. IAIN No. 1, Gaharu, Kec. Medan Timur, Kota Medan, Sumatera Utara
Korespondensi penulis:[1] khaliza1036@gmail.com ,[2] irwannst@uinsu.ac.id

Abstract. *Digital transformation in Indonesia has increased dependence on digital database systems, so that personal data protection has become a crucial issue. This research aims to analyze the urgency of protecting personal data in digital database systems in Indonesia from regulatory, ethical and technical strategy aspects. The method used is literature study and document analysis of regulations, ethical practices and data protection technology. The research results show that even though Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) has been passed, its implementation still faces challenges in the form of low digital literacy, weak law enforcement, and not yet optimal monitoring infrastructure. Additionally, implementing ethical principles and technical strategies, such as encryption, access control, and privacy by design, is critical to strengthening data security. This research concludes that effective personal data protection can only be realized through synergy between strong regulations, the application of digital ethics, and adequate technical strategies, in order to safeguard individual privacy rights in the digital era.*

Keywords*: Personal data protection, digital database system, privacy, digital ethics, regulations, PDP Law*

Abstrak. Transformasi digital di Indonesia telah meningkatkan ketergantungan terhadap sistem database digital, sehingga perlindungan data pribadi menjadi isu krusial. Penelitian ini bertujuan untuk menganalisis urgensi perlindungan data pribadi dalam sistem database digital di Indonesia dari aspek regulasi, etika, dan strategi teknis. Metode yang digunakan adalah studi literatur dan analisis dokumen terhadap regulasi, praktik etika, serta teknologi perlindungan data. Hasil penelitian menunjukkan bahwa meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah disahkan, implementasinya masih menghadapi tantangan berupa rendahnya literasi digital, lemahnya penegakan hukum, dan belum optimalnya infrastruktur pengawasan. Selain itu, penerapan prinsip etika dan strategi teknis, seperti enkripsi, kontrol akses, dan privacy by design, sangat penting untuk memperkuat keamanan data. Penelitian ini menyimpulkan bahwa perlindungan data pribadi yang efektif hanya dapat terwujud melalui sinergi antara regulasi yang kuat, penerapan etika digital, dan strategi teknis yang memadai, guna menjaga hak privasi individu di era digital.

Kata kunci: Perlindungan data pribadi, sistem database digital, privasi, etika digital, regulasi, UU PDP.

1. LATAR BELAKANG

Transformasi digital yang pesat telah mengubah cara kita berinteraksi, bekerja, dan menyimpan data. Sektor publik maupun swasta kini semakin bergantung pada sistem database digital untuk mengelola informasi pribadi, termasuk nama, alamat, identitas finansial dsb. Meskipun kemajuan ini memberikan banyak manfaat, peningkatan ketergantungan pada sistem berbasis teknologi ini turut meningkatkan risiko kebocoran dan penyalahgunaan data pribadi.

Kasus kebocoran data pribadi yang semakin marak menjadi sorotan utama dalam perdebatan mengenai perlindungan data pribadi di Indonesia. Salah satu contoh kasus serius yang diungkap oleh Yaputra (2024) adalah kebocoran 4,7 juta data ASN (Aparatur Sipil Negara), serta dugaan bocornya data NPWP milik jutaan warga, termasuk data pribadi presiden. Kasus ini memperlihatkan adanya kelemahan dalam pengelolaan dan pengamanan

Received: Maret 30, 2025; Revised: April 30, 2025; Accepted: Mei 13, 2025;
Online Available : Mei 16, 2025;

sistem database di Indonesia, yang belum sesuai dengan standar keamanan dan etika yang seharusnya.

Dalam konteks transformasi digital, perlindungan data pribadi tidak hanya berkaitan dengan upaya preventif terhadap kebocoran, tetapi juga dengan bagaimana data tersebut dikelola dan diproses oleh berbagai pihak yang terlibat, baik pemerintah maupun sektor swasta. Peningkatan risiko peretasan dan penyalahgunaan data memerlukan penataan regulasi yang lebih efektif dan penerapan prinsip etika yang lebih kuat dalam tata kelola database digital.

Oleh karena itu, penting untuk mengevaluasi secara mendalam regulasi yang ada terkait perlindungan data pribadi serta melihat sejauh mana prinsip etika diterapkan dalam pengelolaannya. Penelitian ini bertujuan untuk membahas urgensi perlindungan data pribadi dalam konteks regulasi yang berlaku serta praktik pengelolaan database digital yang memenuhi standar keamanan dan etika, guna menciptakan sistem yang lebih aman dan terpercaya di era digital ini. Dengan menggunakan metode studi literatur dan analisis dokumen, penelitian ini akan memberikan wawasan yang lebih dalam mengenai tantangan dan strategi dalam perlindungan data pribadi di Indonesia.

2. KAJIAN TEORITIS

Privasi di Era Digiral

Sesuai dengan Pasal 1 angka 1 Permenkominfo Nomor 20 Tahun 2016, data pribadi adalah informasi yang berkaitan dengan identitas seseorang dan harus dijaga kerahasiaannya. Rizky Ardiansyah & Ardiana (2023) turut menekankan bahwa informasi yang memungkinkan seseorang dikenali harus diperlakukan sebagai data pribadi dan dilindungi secara ketat. Hal ini menegaskan bahwa perlindungan data pribadi bukan hanya kewajiban hukum, tetapi juga tanggung jawab etis dalam pengelolaan sistem elektronik.

Saat ini Internet telah menjadi jembatan penghubung komunikasi antar berbagai pihak yang memudahkan manusia untuk melakukan aktivitas. Namun, di balik kemudahan yang ditawarkan oleh internet, terdapat tantangan yang harus dihadapi pengguna, terutama seiring dengan meningkatnya jumlah pengguna internet. Salah satu tantangan utama tersebut adalah menjaga keamanan data pribadi.

Warren berpandangan bahwa privasi adalah hak yang melekat pada setiap individu dan patut mendapat perlindungan dari lembaga peradilan. Gagasan ini menunjukkan bahwa perlindungan data pribadi bukan sekadar isu teknis, melainkan menyangkut martabat, kebebasan berekspresi, dan ruang pribadi seseorang yang harus dijaga dari penyalahgunaan maupun pelanggaran. Terdapat tiga prinsip penting dalam privasi (Priscyllia, 2019) :

a. Prinsip pertama yaitu ”*right to be alone*” sebagai prinsip dasar privasi seseorang. Ada empat jenis pelanggaran privasi yang dapat terjadi, yaitu: menggunakan gambar seseorang di luar konteks yang semestinya (misalnya, memakai foto orang untuk mendeskripsikan kasus KDRT yang terjadi), menunjukkan data pribadi seperti nama atau nomor telepon untuk tujuan komersial, mengungkapkan keburukan sendiri ke publik, serta tidak memberi kesempatan bagi seseorang untuk menikmati hak atas privasinya.
b. Prinsip kedua yaitu suatu data pribadi seseorang yang ditulis oleh orang lain, seperti rekam medis, data pajak, informasi asuransi, atau catatan kriminal. Data ini berisiko disalahgunakan oleh pihak yang mengumpulkannya atau memprosesnya, sehingga dapat menjadi pelanggaran terhadap hak privasi pemilik informasi tersebut.
c. Prinsip ketiga yaitu privasi terhadap komunikasi yang dilakukan seseorang secara daring (*online*).

Dikarenakan sebagian besar aktivitas masyarakat di era globalisasi telah berevolusi yang awalnya konvensional beralih ke platform digital, keamanan data pribadi menjadi isu yang semakin krusial di era digital saat ini. Banyak pihak yang tanpa disadari membagikan informasi sensitif melalui berbagai platform digital, mulai dari media sosial hingga layanan daring lainnya.

Ketika data pribadi disalahgunakan oleh pihak yang tidak bertanggung jawab, risiko seperti pencurian identitas dan penipuan semakin marak. Oleh karena itu, penting bagi setiap individu agar memahami hak-hak atas data pribadinya serta menerapkan langkah-langkah perlindungan yang memadai dalam aktivitas digital sehari-hari.

Regulasi Perlindungan Data Privasi

Perlindungan data pribadi memiliki landasan konstitusional yang kuat di Indonesia. Pasal 28G ayat (1) UUD 1945 menyatakan bahwa *“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”* (Aisyah et al., 2024). Ketentuan ini menegaskan bahwa data pribadi termasuk dalam aspek “perlindungan diri pribadi” yang seharusnya dilindungi oleh negara.

Secara praktis, perlindungan data pribadi belum sepenuhnya terimplementasi secara efektif karena selama bertahun-tahun Indonesia belum memiliki regulasi yang secara khusus dan komprehensif mengatur perlindungan data pribadi. Ketiadaan regulasi khusus menjadi salah satu alasan penting lahirnya RUU Perlindungan Data Pribadi (UU PDP), yang akhirnya disahkan pada tahun 2022. Undang-undang ini hadir sebagai respon terhadap maraknya kasus

kebocoran data dan semakin pentingnya data sebagai aset strategis di era digital. Meskipun UU PDP mengatur persetujuan eksplisit, kasus-kasus seperti data NPWP menunjukkan belum ada mekanisme pelaporan yang berjalan efektif. Selain itu, Indonesia belum memiliki data protection authority yang independen sebagaimana direkomendasikan GDPR.

Aisyah dkk. (2024) menjelaskan bahwa UU PDP tidak hanya memperjelas kedudukan hukum data pribadi sebagai objek perlindungan HAM, tetapi juga memberikan landasan hukum yang jelas bagi masyarakat dan pelaku usaha dalam pengelolaan data pribadi. Dalam hal ini, UU PDP menjadi jembatan antara hak asasi warga negara dan kebutuhan akan regulasi yang adaptif terhadap perkembangan teknologi.

Meskipun sudah disahkan, implementasi UU PDP masih menghadapi banyak tantangan. Saputra dkk. (2024) menyebut bahwa lemahnya infrastruktur hukum dan keterbatasan lembaga pengawasan seperti otoritas pengawas perlindungan data menjadi hambatan utama dalam penerapan UU ini. Ini menjadi bukti bahwa pengesahan undang-undang saja tidak cukup tanpa pengawasan yang efektif, hak-hak atas data pribadi akan tetap rentan dilanggar.

Konsep Etika Pengelolaan Database Digital

Etika berperan penting dalam menjaga data pribadi. Menurut Saputra dkk. (2024), etika dalam privasi dan keamanan data mencakup prinsip-prinsip penghormatan terhadap hak individu atas kerahasiaan informasi pribadi, serta kewajiban untuk menggunakan data hanya untuk tujuan yang sah. Namun, dalam praktiknya pelanggaran privasi seringkali berakar pada kelalaian atau ketidaktahuan terhadap prinsip-prinsip etis tersebut. Seperti menyalahgunakan data untuk tujuan komersil atau penyebaran data tanpa izin pemilik data.

Etika digital juga harus menjadi bagian dari kesadaran kolektif masyarakat modern, khususnya dalam mengakses serta mendistribusikan informasi melalui media sosial. Tanpa pemahaman etis yang memadai, pengguna media digital berpotensi melanggar hak orang lain secara tidak sadar, misalnya dengan membagikan data pribadi pihak ketiga tanpa izin (Saputra et al., 2024).

Lebih lanjut, etika berkaitan erat dengan keamanan data. Penggunaan teknologi seperti enkripsi, *firewall*, dan otentikasi bukan hanya tindakan teknis semata, tetapi juga wujud dari tanggung jawab etis dalam menjaga data dari akses yang tidak sah. Etika keamanan, sebagaimana dikemukakan oleh Saputra dkk. (2024) menjadi pendorong lahirnya teknologi yang dirancang untuk mengantisipasi serangan siber dan pelanggaran keamanan.

Dalam konteks sistem database digital, etika pengelolaan data menjadi semakin penting. Pengumpulan dan penyimpanan informasi pribadi di berbagai basis data daring menuntut adanya prinsip-prinsip etika yang kuat, termasuk kejelasan otorisasi akses, transparansi

penggunaan data, serta hak subjek data untuk mengontrol data pribadinya. Pengabaian terhadap prinsip ini berisiko melahirkan pelanggaran hak privasi dalam skala besar.

Dalam layanan konseling *online*, misalnya, penting bagi konselor untuk menjelaskan secara transparan mengenai aspek kerahasiaan data kepada konseling. Hal ini tidak hanya diwajibkan oleh standar profesional, tetapi juga merupakan bentuk tanggung jawab moral. Ketidakpatuhan terhadap prinsip ini dapat menimbulkan konsekuensi serius, mulai dari pelanggaran hukum hingga hilangnya kepercayaan publik (Saputra et al., 2024).

Strategi Teknis Perlindungan Privasi dalam Sistem Database

Perlindungan privasi dalam sistem database membutuhkan kombinasi berbagai teknik dan strategi yang disesuaikan dengan jenis data dan kebutuhan organisasi. Berikut adalah pendekatan teknis utama yang dapat diterapkan:

a. Enkripsi Data

Enkripsi mengonversi data menjadi format tidak terbaca (*ciphertext*) menggunakan algoritma seperti AES-256 atau RSA. Teknik ini melindungi data baik saat disimpan (*data at rest*) maupun ditransfer (*data in transit*). Contoh penerapannya adalah mengenkripsi kolom database yang mengandung informasi sensitif (seperti NIK atau nomor rekening) atau menggunakan protokol TLS untuk transmisi data. Penelitian Ujung & Nasution (2023) menegaskan bahwa enkripsi mengurangi risiko kebocoran data hingga 80% jika terjadi peretasan atau akses fisik tidak sah ke server.

b. Kontrol Akses dan Otorisasi

Prinsip *least privilege* dan *role-based access control* (RBAC) membatasi akses berdasarkan peran pengguna. Misalnya, staf HR hanya bisa mengakses data karyawan, sedangkan tim keuangan tidak memiliki akses ke data medis. Multi-factor authentication (MFA) seperti kombinasi password + OTP atau biometrik juga wajib diterapkan untuk verifikasi identitas. Menurut Ramadhani (2024), 60% pelanggaran data terjadi akibat kesalahan konfigurasi hak akses, sehingga kontrol ketat ini menjadi kunci pencegahan.

c. *Firewall* dan Keamanan Jaringan

Firewall bertindak sebagai filter lalu lintas jaringan dengan memblokir port tidak perlu (misal: port 1433 untuk SQL Server) dan membatasi koneksi eksternal ke database. Segmentasi jaringan memisahkan database dari jaringan publik, sementara SSL/TLS mengenkripsi koneksi antara aplikasi dan database. Studi yang dilakukan Daulay (2023) menyebutkan firewall mengurangi serangan brute-force dan SQL injection hingga 70%.

d. Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS)

IDS memantau aktivitas jaringan untuk mendeteksi pola mencurigakan (misal: percobaan akses massal atau query tidak biasa), sedangkan IPS secara otomatis memblokir serangan seperti DDoS atau eksploitasi kerentanan. Teknologi ini menggunakan metode *signature-based detection* (mengenali pola serangan dikenal) atau *anomaly-based detection* (mendeteksi penyimpangan dari perilaku normal). Implementasi IDS/IPS yang disebutkan dalam penelitian oleh Ramadhani et al. (2024) ini sebagai solusi proaktif untuk mitigasi serangan zero-day.

e. Audit dan Monitoring

Audit rutin (bulanan/triwulanan) memeriksa log akses, perubahan konfigurasi, dan aktivitas user. Tools seperti SIEM (*Security Information and Event Management*) mengumpulkan dan menganalisis log dari database, server, dan aplikasi untuk mendeteksi ancaman secara real-time. Contoh kasus: audit log membantu mengidentifikasi karyawan yang mencoba mengunduh data sensitif tanpa izin. Penelitian Ujung & Nasution (2023) menekankan bahwa 90% insiden keamanan terdeteksi melalui analisis log.

f. Backup dan Recovery

Backup harian/mingguan dengan skema 3-2-1 (3 salinan data, 2 media berbeda, 1 lokasi *offsite*) memastikan data dapat dipulihkan setelah serangan ransomware atau bencana. Enkripsi backup wajib diterapkan untuk mencegah pencurian data cadangan. Daulay et al. (2023) merekomendasikan simulasi pemulihan data (*disaster recovery drill*) secara berkala untuk memvalidasi keandalan sistem.

g. Kepatuhan Regulasi

Regulasi seperti GDPR (Eropa) atau UU PDP (Indonesia) mewajibkan organisasi menerapkan *privacy by design*, termasuk notifikasi kebocoran data dalam 72 jam dan penghapusan data sesuai permintaan pengguna (*right to erasure*). Penerapan kebijakan ini didukung oleh Rahmadani et al. (2024), yang mencatat bahwa kepatuhan mengurangi denda hukum hingga 95% pada kasus pelanggaran data.

h. Teknologi Baru

Penerapan teknologi baru juga menjadi salah satu strategi perlindungan privasi dalam sistem database. Beberapa teknologi baru yang bisa diterapkan adalah sebagai berikut:

1) Blockchain: Membuat catatan transaksi database yang tidak dapat diubah (*immutable*), cocok untuk audit trail.
2) AI/ML: Mendeteksi anomali akses dengan analisis perilaku pengguna (*user behavior analytics*).

3) Homomorphic Encryption: Memungkinkan komputasi data terenkripsi tanpa perlu dekripsi, ideal untuk analisis data sensitif.

Studi yang dilakukan oleh Ujung et al. (2023) memprediksi bahwa teknologi ini akan menjadi standar keamanan database dalam 5 tahun ke depan.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dengan pendekatan kualitatif deskriptif. Data yang dianalisis merupakan data sekunder yang diperoleh dari berbagai sumber, seperti jurnal ilmiah yang terindeks Google Scholar, Garuda, dan Sinta, lalu dari dokumen hukum, dan laporan kebijakan terkini terkait perlindungan data pribadi di Indonesia. Melalui studi literatur, penelitian ini bertujuan untuk mengumpulkan, merangkum, dan menganalisis informasi guna memperoleh pemahaman mendalam mengenai regulasi, prinsip etika, dan aspek teknis dalam pengelolaan data pribadi. Metode kualitatif deskriptif dipilih karena tujuan utama penelitian ini adalah menggambarkan fenomena perlindungan data pribadi secara menyeluruh dari aspek hukum, etika, dan teknologi. Dengan memanfaatkan data sekunder dan analisis mendalam, penelitian ini memberikan gambaran komprehensif mengenai tantangan dan strategi perlindungan data pribadi di era digital.

Selain itu, penelitian ini juga menggunakan analisis dokumen untuk mengkaji isi Undang-Undang Perlindungan Data Pribadi (UU PDP) serta laporan kebocoran data yang terjadi di Indonesia. Pendekatan ini memungkinkan penilaian terhadap efektivitas regulasi dan praktik pengelolaan data pribadi berdasarkan sumber-sumber yang kredibel.

4. HASIL DAN PEMBAHASAN

Kelemahan Implementasi Hak Privasi di Indonesia

Walaupun Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai tonggak regulasi perlindungan data, implementasinya di lapangan masih jauh dari harapan. Salah satu hambatan utama adalah belum terbentuknya lembaga pengawas independen yang secara khusus bertugas sebagai otoritas perlindungan data. Berbeda dengan Uni Eropa yang memiliki *European Data Protection Board* (EDPB) sebagai badan pengawas yang kuat dan independen, Indonesia masih dalam tahap perencanaan pembentukan lembaga serupa. Akibatnya, penegakan hukum terhadap pelanggaran data pribadi menjadi lemah dan tidak konsisten.

Contoh nyata pada kasus kebocoran data BPJS Kesehatan dikemukakan oleh Nur Indrajaya (2021), di mana data pribadi sekitar 279 juta penduduk diduga bocor ke publik.

Sayangnya, hingga kini belum ada mekanisme pemulihan yang transparan dan sanksi tegas kepada pengendali data yang lalai. Hal ini menunjukkan bahwa prinsip-prinsip dasar perlindungan data, seperti persetujuan eksplisit dari pemilik data dan hak untuk menghapus data (*right to erasure*), belum sepenuhnya diterapkan dalam praktik sehari-hari. Lemahnya sistem pelaporan dan penegakan hukum membuat masyarakat masih sangat rentan terhadap penyalahgunaan data pribadi.

Tantangan Etika dalam Pengelolaan Data Pribadi

Selain aspek hukum, dimensi etika juga menjadi isu krusial dalam tata kelola data pribadi. Banyak organisasi, baik di sektor publik maupun swasta, masih menggunakan data pribadi tanpa memberikan penjelasan yang memadai kepada pengguna mengenai tujuan dan risiko penggunaan data tersebut. Kurangnya transparansi ini diperparah oleh rendahnya pemahaman masyarakat mengenai hak-haknya sebagai subjek data, seperti hak untuk menolak penggunaan data untuk kepentingan komersial atau pemasaran.

Etika digital juga menuntut institusi untuk bertanggung jawab menjaga keamanan data yang mereka kelola. Namun, dalam praktiknya, masih banyak lembaga yang menyimpan data sensitif tanpa perlindungan dasar seperti enkripsi atau autentikasi ganda. Pelanggaran semacam ini, meskipun kadang tidak disengaja, tetap menunjukkan kegagalan dalam memenuhi prinsip tanggung jawab (*accountability*) dan kehati-hatian (*due diligence*). Studi oleh Aisyah et al. (2024) menemukan bahwa hanya sekitar 42% lembaga publik di Indonesia yang telah memiliki kebijakan etik formal terkait perlindungan data. Hal ini menandakan perlunya peningkatan kesadaran dan edukasi etika digital di semua lini.

Evaluasi Strategi Teknis dan Infrastruktur Keamanan

Dari sisi teknis, perlindungan data pribadi dalam sistem database digital sangat bergantung pada penerapan teknologi keamanan yang mutakhir. Strategi seperti enkripsi data, kontrol akses berbasis peran (RBAC), *multi-factor authentication* (MFA), *firewall*, dan sistem deteksi serta pencegahan intrusi (IDS/IPS) telah terbukti efektif mengurangi risiko kebocoran data di sektor swasta. Namun, adopsi teknologi ini di sektor publik masih sangat terbatas.

Penelitian Ujung et al. (2023) menunjukkan bahwa penggunaan enkripsi dapat menurunkan risiko kebocoran data hingga 80%, tetapi hanya sekitar 34% institusi pemerintah yang menerapkan enkripsi secara menyeluruh. Selain itu, audit keamanan sistem secara berkala belum menjadi standar wajib, sehingga banyak pelanggaran yang tidak terdeteksi. Prinsip "*privacy by design*", yaitu memastikan keamanan sejak tahap perancangan sistem, juga masih jarang diimplementasikan. Padahal, penerapan prinsip ini sangat penting untuk memastikan perlindungan data sejak awal.

Studi Kasus Kebocoran Data dan Isu Pertukaran Internasional

Kasus kebocoran data NPWP dan ASN yang diungkap oleh Cenvysta & Gunadi (2024) dalam konteks implementasi sistem *Automatic Exchange of Information* (AEoI) menyoroti tantangan baru dalam era globalisasi data. Ketika data pribadi dipertukarkan lintas negara, risiko penyalahgunaan semakin besar jika negara mitra tidak memiliki perlindungan hukum yang setara. Tanpa adanya klausul perlindungan privasi yang jelas dalam kerja sama internasional, data sensitif milik warga negara Indonesia dapat diakses dan disalahgunakan oleh pihak ketiga di luar negeri.

Ketiadaan lembaga pengawas yang aktif dan regulasi teknis yang rinci memperbesar risiko ini. Indonesia perlu memastikan bahwa setiap kerja sama internasional dilengkapi dengan perjanjian perlindungan data yang sepadan dengan standar nasional, agar data warga negara tetap aman di mana pun berada.

Sinkronisasi Kebijakan dan Literasi Digital

Fragmentasi regulasi antar sektor, seperti perbankan, kesehatan, dan pendidikan, menjadi tantangan tersendiri dalam upaya perlindungan data pribadi. Setiap sektor memiliki standar dan mekanisme perlindungan yang berbeda, sehingga sulit untuk melakukan audit dan penegakan hukum lintas sektor secara efektif. Hal ini menimbulkan celah yang dapat dimanfaatkan oleh pihak-pihak tidak bertanggung jawab.

Selain itu, rendahnya literasi digital masyarakat Indonesia menjadi faktor penghambat utama. Banyak pengguna tidak menyadari risiko membagikan data pribadi di media sosial atau melalui aplikasi yang tidak kredibel. Oleh karena itu, strategi perlindungan data tidak cukup hanya mengandalkan regulasi dan teknologi, tetapi juga harus mencakup edukasi dan peningkatan kesadaran masyarakat. Literasi digital yang baik akan membuat masyarakat lebih waspada dan mampu melindungi data pribadinya sendiri.

5. KESIMPULAN DAN SARAN

Penelitian ini menggarisbawahi betapa pentingnya perlindungan data pribadi dalam sistem database digital, khususnya di Indonesia. Meskipun Indonesia telah memiliki Undang-Undang Perlindungan Data Pribadi (UU PDP), pelaksanaannya masih menghadapi banyak tantangan, seperti rendahnya pemahaman masyarakat tentang literasi digital, keterbatasan infrastruktur keamanan, serta penegakan hukum yang lemah. Oleh karena itu, untuk menciptakan sistem yang lebih aman dan dapat dipercaya, diperlukan kerjasama yang erat antara kebijakan hukum, kesadaran etis, dan teknologi yang terus berkembang.

Secara etis, perlindungan data pribadi harus menjadi tanggung jawab bersama. Tidak hanya sebagai kewajiban hukum, tetapi juga sebagai bagian dari rasa saling menghormati dan menjaga hak privasi setiap individu. Pengelolaan data yang transparan dan penuh tanggung jawab harus menjadi dasar dari setiap interaksi digital.

Di sisi teknis, langkah-langkah seperti enkripsi, kontrol akses yang ketat, serta penggunaan sistem deteksi dan pencegahan ancaman (IDS/IPS) menjadi kunci untuk melindungi data pribadi dari kebocoran atau penyalahgunaan. Selain itu, prinsip *privacy by design* yang diterapkan sejak awal dalam setiap desain sistem database sangat penting untuk mengurangi risiko pelanggaran di masa depan.

Keseluruhan, perlindungan data pribadi yang efektif memerlukan keselarasan antara kebijakan hukum yang kuat, penerapan etika yang mendalam, serta adopsi teknologi yang sesuai. Semua pihak baik pemerintah, dunia usaha, maupun masyarakat yang memiliki peran penting dalam menjaga dan menghormati privasi setiap individu dalam dunia digital yang semakin maju ini.

DAFTAR REFERENSI

Aisyah, A. P., Aprilia, A., Andini, P., Syahida, S., Azzahra, S. M., & Supiyandi. (2024). Perlindungan Data Pribadi dan Etika Media Sosial di Era Digital. *Jurnal Pendidikan Tambusai*, *8*(2), 28236–28238.

Cenvysta, M., & Gunadi, A. (2024). KONSEP TANGGUNG JAWAB NEGARA TERHADAP KEWAJIBAN MELINDUNGI DATA PRIBADI MASYARAKAT DI INDONESIA (STUDI KASUS KEBOCORAN DATA NPWP MASYARAKAT INDONESIA). *Jurnal Hukum Lex Generalis*, *5*(12), 3–11.

Daulay, A. P. E., Febriana, V., Kita, A. D. A., Gunawan, S., & Nurbaiti. (2023). Keamanan dalam Sistem Database Sebagai Sumber Informasi Manajemen Terhadap Perlindungan Data. *Edu Society: Jurnal Pendidikan, Ilmu Sosial Dan Pengabdian Kepada Masyarakat*, *3*(2), 988–991. https://doi.org/10.56832/edu.v3i2.357

Nur Indrajaya, I. (2021). *Dugaan Kebocoran Data Pribadi Penduduk, BPJS Kesehatan Terancam Sanksi Berlapis*. AyoBandung.Com. https://www.ayobandung.com/finansial/pr-79724031/dugaan-kebocoran-data-pribadi-penduduk-bpjs-kesehatan-terancam-sanksi-berlapis

Priscyllia, F. (2019). PERLINDUNGAN PRIVASI DATA PRIBADI PERSPEKTIF PERBANDINGAN HUKUM. *JATISWARA*, *34*(3), 240–243.

Rahmadani, A. E., Pangestu, Y., & Halizhah, N. (2024). Perlindungan Data Pribadi Dalam Era Digital: Tantangan dan Solusi. *Media Hukum Indonesia (MHI)*, *2*(4), 115–137.

Rizky Ardiansyah, M., & Ardiana, R. (2023). Kewajiban Dan Tanggung Jawab Hukum Perdata Dalam Perlindungan Privasi Data Pasien Dalam Layanan Kesehatan Digital Mohamad

Rizky Ardiansyah. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *1*(4), 279–280.

Saputra, C. D., Saputra, G. S., & Aprilliani, F. (2024). Perspektif Hukum terhadap Privasi dan Perlindungan Data Pribadi di Era Digital. *Jurnal Ilmu Hukum, Humaniora, Dan Politik*, *5*(1), 799–810. https://doi.org/https://doi.org/10.38035/jihhp. https://creativecommons.org/licenses/by/4.0/

Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *JISKA: Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44. http://jurnal.unidha.ac.id/index.php/jteksis

Yaputra, H. (2024). *Daftar Kebocoran Data Pribadi di Era Jokowi, Paling Banyak di Instansi Pemerintah*. TEMPO. https://www.tempo.co/politik/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah--7403