CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 10 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

MENJAGA PRIVASI DI ERA DIGITAL PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI DI INDONESIA

Muhamad Fadilah Kurniawan[1*], Eltsaabita Ronaa Eftria[2], Dian Eka Prastiwi[3]

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pamulang,
Kota Tangerang Selatan, Indonesia

Email: muhammadfadilah03@e-mail.com[1*], eltsaabitare@e-mail.com[2], Dekaprastiwi@e-mail.com[3]

ABSTRAK

Era digital telah membawa kemudahan dalam pengelolaan dan pertukaraan data, namun disisi lain meningkatkan resiko pelanggaran privasi dan kebocoran data pribadi. Di Indonesia, sejumlah insiden kebocoran data besar seperti kasus Bank Syariah Indonesia, IndiHome, dan serangan ransomware pada Pusat Data Nasional Sementara (PDNS) menyoroti urgensi perlindungan data pribadi yang lebih kuat. Data pribadi kini menjadi aset berharga yang rentan terhadap pencurian, penyalahgunaan, dan pelanggaran privasi, sehingga memerlukan perlindungan hukum yang jelas dan tegas. Pemerintah Indonesia telah menegesahkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) sebagai upaya membangun ekosistem digital yang aman dan terpercaya. Namun, implementasi UU PDP menghadapi berbagai tantangan, mulai dari kebutuhan aturan turunan, penegakan hukum yang efektif, sinkronisasi regulasi, literasi masyarakat yang masih rendah. Perlindungan data pribadi harus menjadi tanggung jawab bersama antara pemerintah, sektor swasta, dan masyarakat. Penguatan sistem keamanan digital, peningkatan literasi, serta penegakan hukum yang tegas sangat diperlukan agar hak privasi masyarakat terlindungi secara optimal di tengah pesatnya transformasi digital di Indonesia.

Kata Kunci: Perlindungan Data Pribadi, Privasi Digital, Kebocoran Data, Keamanan Siber, Undang-Undang No. 27 Tahun 2022.

ABSTRACT

The digital era has brought significant convenience in the management and exchange of data, but it has also increased the risk of privacy violations and personal data breaches. In Indonesia, several major incidents such as the Bank Syariah Indonesia data

Article History
Received: Juni 2025
Reviewed: Juni 2025
Published: Juni 2025
Plagirism Checker No 234
Prefix DOI:
10.8734/CAUSA.v1i2.365

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 10 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

breach, IndiHome data leak, and the ransomware attack on the Temporary National Data Center (PDNS) highlight the urgent need for stronger personal data protection. Personal data has become a valuable asset that is vulnerable to theft, misuse, and privacy violations, thus requiring clear and firm legal safeguards. The Indonesian government has responded by enacting Law No. 27 of 2022 concerning Personal Data Protection as an effort to build a secure and trustworthy digital ecosystem. However, the implementation of this law still faces various challenges, including the need for derivative regulations, effective law enforcement, regulatory synchronization, and low public literacy. Personal data protection must be a shared responsibility among the government, private sector, and society. Strengthening digital security systems, increasing literacy, and multi-stakeholder collaboration are crucial to ensure that citizens' privacy rights are optimally protected in the digital transformation era.

***Keywords**: Personal Data Protection, Digital Privacy, Data Breach, Cybersecurity, Undang-Undang No. 27 Tahun 2022.*

PENDAHULUAN

Kemajuan dalam bidang teknologi digital telah merevolusi pola interaksi antarmanusia, metode kerja, serta sistem pengelolaan informasi. Dalam konteks ini, teknologi digital dapat dipahami sebagai perangkat yang beroperasi tanpa ketergantungan pada tenaga kerja manual, melainkan mengandalkan mekanisme otomatis yang didasarkan pada sistem komputer atau format data yang dapat diproses oleh komputer. Pada dasarnya, teknologi digital merupakan sistem perhitungan berkecepatan tinggi yang dirancang untuk mengumpulkan informasi dalam bentuk angka atau kode digital. Sistem komunikasi digital ini beroperasi menggunakan sinyal listrik komputer yang bersifat diskrit dan memanfaatkan sistem bilangan biner untuk membentuk kode digital. Proses pengolahan kode digital tersebut dilakukan oleh komputer, sebagai contoh adalah konversi gambar dari kamera video yang awalnya berupa gelombang cahaya kemudian diubah menjadi pixel digital. Meski demikian, kemajuan teknologi ini turut menghadirkan permasalahan baru, khususnya dalam hal keamanan informasi pribadi di era yang ditandai dengan intensitas penggunaan data yang tinggi oleh berbagai entitas. (Hadijah, 2024)

Di Indonesia, perlindungan hak privasi telah diatur dalam berbagai regulasi, seperti UUD 1945 Pasal 28H ayat 4, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Permen Kominfo No. 20 Tahun 2016. (Mahameru et al., 2023) Meski demikian, sejumlah kejadian kebocoran data besar, seperti yang telah terjadi pada Bank Syariah Indonesia, Pusat Data Nasional Sementara (PDNS) (Husnul, 2025) dan IndiHome. (Firdaus, 2024) Menunjukkan bahwa keamanan data pribadi masih menjadi masalah serius. Data pribadi yang bocor tidak hanya mengancam privasi individu, tetapi juga berpotensi menimbulkan kerugian finansial, psikologis, dan sosial akibat penyalahgunaan oleh pihak tidak bertanggung jawab.

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 10 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Materi yang dikumpulkan dari berbagai artikel menunjukkan bahwa data pribadi kini menjadi aset berharga yang sangat rentan terhadap ancaman pencurian, penyalahgunaan, dan pelanggaran privasi. Ancaman terhadap data pribadi dapat muncul akibat kesalahan manusia (human error), serangan malware, manipulasi psikologi (social engineering), serta lemahnya sistem keamanan digital. Selain itu, rendahnya literasi masyarakat dan belum optimalnya penegakan hukum juga memperparah risiko kebocoran data di Indonesia.

Kebaruan ilmiah dari artikel ini terletak pada pemaparan komprehensif mengenai urgensi perlindungan data pribadi di era digital, dengan menyoroti contoh-contoh nyata insiden kebocoran data dan tantangan implementasi regulasi yang ada. Artikel ini menyajikan sintesis dari berbagai sumber aktual untuk memberikan gambaran utuh tentang permasalahan dan kebutuhan perlindungan hukum data pribadi di Indonesia.

Permasalahan utama yang diangkat dalam kajian ini adalah bagaimana tantangan perlindungan data pribadi di Indonesia di tengah pesatnya transformasi digital dan maraknya insiden kebocoran data.

Tujuan dibuatnya artikel ini adalah untuk menguraikan urgensi perlindungan hukum terhadap data pribadi di Indonesia, menganalisis faktor-faktor penyebab kebocoran data, serta menyoroti tantangan implementasi regulasi perlindungan data pribadi berdasarkan kasus-kasus yang terjadi di Indonesia saat ini.

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur (library research) dengan pendekatan deskriptif, di mana seluruh data dan informasi yang dianalisis diperoleh dari sumber-sumber yang tersedia secara daring. Pengumpulan data tidak dilakukan melalui survei lapangan, wawancara langsung, atau eksperimen, melainkan dengan menelusuri dan mengkaji artikel-artikel, berita, dokumen resmi, serta publikasi ilmiah yang relevan dengan topik perlindungan data pribadi di Indonesia.

HASIL PEMBAHASAN

Urgensi Perlindungan Privasi di Era Digital

1) Penjelasan tentang kebocoran data

Kebocoran data ini adalah kondisi dimana informasi sensitif atau pribadi seseorang terekspos dan dapat diakses oleh pihak yang tidak berwenang. Kebocoran data sangat erat kaitannya dengan pembobolan data, yaitu pembobolan data secara sengaja oleh peretas. Ketika data penting bisa langsung dilihat oleh peretas melalui situs yang dibuat olehnya, dengan itu peretas dapat dengan mudah mengakses dan memanfaatkannya untuk tujuan merugikan, seperti penipuan atau pencurian identitas. (Ashari, 2022)

Dari penjelasan ini ada beberap faktor utama yang menyebabkan data-data bisa bocor, yaitu:

a) Kesalahan manusia (human error):

Banyak data bocor terjadi karena kelalaian pengguna, seperti memasukan data pribadi ke situs atau aplikasi yang tidak aman, menggunakan software bajakan, atau salah mengirim email yang berisi informasi sensitif. Kebiasaan mencari aplikasi gratis atau tergiur iming-iming bonus sering

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 14 No 10 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

membuat orang tanpa sadar memberikan data pribadinya ke pihak yang tidak bertanggung jawab.

b) Serangan malware:

Malware adalah program berbahaya yang dapat masuk ke perangkat melalui email, situs web, atau aplikasi palsu. Salah satu jenis malware yaitu spyware, bisa diam-diam mengumpulkan data pribadi pengguna dan mengirimkannya ke pihak ke tiga tanpa sepengetahuan korban. Malware memanfaatkan kelengahan pengguna dan celah keamanan sistem untuk mencuri data.

c) Manipulasi psikologi (social engineering):

Metode ini memanfaatkan teknik penipuan, seperti phising, dimana pelaku menyamar sebagai pihak terpercaya dan mengelabui korban agar memberikan informasi sensitif. Contohnya, korban menerima email atau SMS yang tampak resmi dan berisi tautan palsu yang meminta data pribadi. Jika korban mengeklik tautan tersebut, data mereka langsung bisa dicuri oleh pelaku.

Selain dari ketiga faktor utama di atas, kebocoran data juga bisa terjadi akibat kelemahan sistem keamanan, perangkat yang hilang, atau penggunaan kata sandi yang lemah.

2) Dampak Kebocoran Data Nasional

Ketika informasi pribadi warga negara mengalami kebocoran secara massal, hal ini menciptakan rangkaian masalah kompleks yang mempengaruhi berbagai sendi kehidupan masyarakat, mulai dari aspek perekonomian hingga kondisi mental individu. Konsekuensi yang ditimbulkan tidak sebatas pada hilangnya uang secara langsung, namun juga mengakibatkan dampak berkelanjutan berupa merosotnya tingkat kepercayaan masyarakat terhadap sistem teknologi informasi yang ada di negara ini. Situasi terekspos nya data pribadi memberikan kesempatan emas bagi para penjahat digital untuk melancarkan aksi-aksi ilegal seperti pemerasan, tindak penipuan, serta penyalahgunaan jati diri seseorang. Informasi yang terekspos umumnya berisi hal-hal yang bersifat rahasia, antara lain NIK, catatan keuangan pribadi, serta jejak aktivitas digital setiap orang. (Bua & Idris, 2025, hlm. 107)

Kondisi sistem keamanan data yang masih lemah ditambah dengan penggunaan password yang mudah ditebak menjadikan infrastruktur digital mudah ditembus melalui serangan brute force maupun credential stuffing, sehingga memungkinkan terjadinya pencurian informasi dalam skala besar. Dilihat dari sudut pandang ekonomi, kerugian akibat bocornya data sangat besar mengingat perusahaan maupun instansi pemerintah yang terkena dampak terpaksa mengeluarkan dana dalam jumlah besar untuk memperbaiki sistem, melakukan penyelidikan, dan memberikan ganti rugi kepada pihak-pihak yang dirugikan. Di sisi lain, warga yang informasi pribadinya bocor berpotensi menjadi sasaran penipuan online (phishing), tindak pemerasan, serta pencurian identitas yang tidak hanya merugikan dari segi materi tetapi juga berdampak pada kesehatan mental.

Kebocoran data nasional juga menyebabkan gangguan layanan publik penting seperti sistem perpajakan, keimigrasian, dan pendidikan, yang semakin memperparah

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 10 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

dampak sosial dan ekonomi. Penurunan kepercayaan publik terhadap pemerintah dan penyelenggara layanan digital dapat menghambat partisipasi masyarakat dalam layanan digital dan program pemerintah, serta menimbulkan kecemasan dan ketidakpastian dalam penggunaan teknologi digital.

Implementasi dan Tantangan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Penerapan regulasi yang tercantum dalam UU No. 27 Tahun 2022 mengenai Perlindungan Data Pribadi memiliki sasaran utama untuk memperkuat pemahaman dan ketaatan masyarakat dalam hal pengamanan informasi pribadi di Indonesia. Regulasi ini diharapkan mampu memberikan perlindungan yang lebih baik bagi data pribadi setiap orang serta mengurangi kejadian kebocoran informasi yang dapat merugikan warga negara. Peraturan tersebut mencakup berbagai hal mulai dari prinsip dasar, kategori informasi pribadi, hak-hak pemilik data, tanggung jawab pengelola dan pemroses informasi, sampai dengan hukuman administratif dan pidana bagi yang melanggar ketentuan perlindungan data pribadi. (Saly et al., 2023)

Sebagai ilustrasi konkret mengapa pengamanan data pribadi sangat penting, pada bulan Juni 2024 lalu, Pusat Data Nasional Sementara (PDNS) yang berlokasi di Surabaya mendapat serangan malware ransomware sehingga menyebabkan gangguan pada berbagai layanan masyarakat, termasuk sistem imigrasi, dan baru dapat berfungsi normal kembali setelah beberapa hari. Peristiwa ini memperlihatkan betapa lemahnya sistem keamanan data dan seberapa besar dampak buruk dari serangan cyber terhadap pelayanan masyarakat, serta menunjukkan urgensi adanya sistem proteksi data yang tangguh. (Husnul, 2025)

Dasar hukum dari peraturan ini bersumber pada pertimbangan yang disebutkan dalam UUD 1945, terutama pada Pasal 28G ayat (1), yang menggarisbawahi bahwa setiap warga negara memiliki hak untuk memberikan perlindungan kepada diri sendiri, keluarga, kehormatan, martabat, serta kekayaan yang dimilikinya. Hak terhadap informasi pribadi merupakan hak kepemilikan yang secara alamiah dimiliki oleh setiap orang sebagai pemilik data tersebut. Pengamanan informasi pribadi ini berlaku untuk seluruh individu, baik yang berkewarganegaraan Indonesia maupun warga negara asing yang berada di Indonesia, yang berkaitan dengan semua proses pengelolaan data pribadi mulai dari pengumpulan hingga pengolahannya. (Saly et al., 2023)

UU No. 27 Tahun 2022 juga menekankan bahwa pihak yang mengelola data pribadi memiliki kewajiban untuk menjaga dan menjamin keamanan informasi pribadi yang dikelolanya, serta memberikan jaminan hukum yang tegas terhadap hak-hak pemilik data pribadi. Dengan berlakunya undang-undang ini, diharapkan dapat terbentuk lingkungan digital yang aman, dapat dipercaya, dan terbuka untuk semua, sambil meningkatkan pemahaman masyarakat tentang betapa pentingnya menjaga keamanan data pribadi dalam aktivitas sehari-hari. (Nit, 2024)

Tantangan Implementasi di Lapangan

Tantangan Utama UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP):

1) Implementasi Aturan Turunan

UU PDP baru mengatur prinsip-prinsip umum perlindungan data pribadi, namun banyak konsep yang masih bersifat umum dan membutuhkan aturan pelaksana (peraturan pemerintah, peraturan menteri, dsb.) agar dapat diimplementasikan secara efektif. Pemerintah masih memiliki pekerjaan rumah

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 10 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

untuk mempercepat pembuatan aturan pelaksana ini agar pelaksanaan UU PDP tidak terhambat.

2) Penegakan Hukum dan Pengawasan

Pengawasan terhadap pelaksanaan UU PDP masih menjadi tantangan besar. Diperlukan lembaga pengawas yang independen, memiliki sumber daya memadai, serta kewenangan jelas untuk menindak pelanggaran. Tanpa pengawasan yang kuat, efektivitas perlindungan data pribadi akan sulit tercapai.

3) Sinkronisasi dengan Regulasi Lain

UU PDP harus selaras dengan berbagai peraturan perundang-undangan lain yang juga mengatur data pribadi, seperti UU ITE, UU Kesehatan, dan UU Perbankan. Ketidaksinkronan dapat menimbulkan tumpang tindih kewenangan, kebingungan pelaku usaha, dan celah hukum yang bisa dimanfaatkan pihak tidak bertanggung jawab.

4) Ancaman Penyalahgunaan dan Perdagangan Data

Risiko penyalahgunaan data pribadi, termasuk jual beli data secara ilegal, masih tinggi. Pelaku usaha dan pengendali data harus sangat berhati-hati dalam memproses data, karena ancaman pidana (penjara hingga 6 tahun dan/atau denda hingga Rp 6 miliar) dapat menanti jika terjadi pelanggaran. (Jannah, 2022)

5) Peningkatan Kesadaran Masyarakat

Mayoritas warga negara belum menguasai secara menyeluruh mengenai hak-hak yang mereka miliki dalam hal informasi pribadi, oleh karena itu dibutuhkan program pembelajaran yang berkelanjutan dan mendalam.

6) Kesiapan Infrastruktur

Instansi pemerintahan dan dunia usaha harus membangun sistem pendukung yang layak guna menjamin keamanan serta perlindungan terhadap informasi pribadi warga. (Artikel JDIH, 2024)

Strategis dan Penguatan Perlindungan Data Pribadi

1) Kebutuhan peningkatan keamanan sistem dan infrastruktur digital

Untuk menjalankan aturan tersebut dengan baik, lembaga-lembaga yang bertugas harus memiliki kemampuan yang memadai dan terus ditingkatkan secara berkelanjutan. Hal ini meliputi:

a. Penguatan infrastruktur teknologi, seperti sistem komputer dan jaringan yang aman dan handal.
b. Pengembangan sumber daya manusia (SDM) melalui pelatihan dan sertifikasi agar para petugas dan staf memiliki pengetahuan dan keterampilan yang sesuai.
c. Pembentukan mekanisme koordinasi yang efektif antar lembaga agar kerja sama berjalan lancar dan tidak terjadi tumpang tindih tugas.

Khusus untuk penegakan hukum, aparat yang menangani kasus kejahatan siber dan pelanggaran data pribadi harus diberikan pelatihan khusus dan alat yang memadai agar mereka dapat bekerja secara profesional dan efektif dalam menangani kasus-kasus tersebut.

2) Edukasi dan literasi digital masyarakat

Masyarakat juga perlu mendapatkan edukasi yang menyeluruh dan mudah dipahami mengenai pentingnya perlindungan data pribadi. Strategi yang bisa dilakukan antara lain:

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 10 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

a. Melakukan kampanye literasi digital yang menjangkau semua lapisan masyarakat, dari anak-anak hingga orang dewasa, agar mereka memahami cara menjaga data pribadi secara aman saat menggunakan teknologi digital.
b. Mengintegrasikan materi tentang perlindungan data pribadi ke dalam kurikulum pendidikan di sekolah sehingga generasi muda sejak dini sudah paham pentingnya hal ini.
c. Bekerja sama dengan sektor swasta dan organisasi masyarakat sipil untuk menyebarkan informasi dan praktik terbaik tentang perlindungan data pribadi secara luas.

Dengan langkah-langkah ini, diharapkan masyarakat menjadi lebih sadar dan aktif dalam menjaga data pribadinya, serta mendukung upaya pemerintah dalam melindungi privasi digital secara menyeluruh.

3) Penguatan Regulasi dan Harmonisasi Peraturan

Prioritas utama adalah memperkuat aturan-aturan yang mengatur perlindungan data pribadi. Ini termasuk mempercepat pembuatan aturan pelaksana dari Undang-Undang Perlindungan Data Pribadi (UU PDP) yang sudah ada. Selain itu, penting juga untuk menyelaraskan aturan-aturan yang sudah ada di berbagai sektor agar tidak saling bertentangan dan dapat berjalan secara efektif bersama-sama. Dalam proses ini, kita harus memperhatikan perkembangan teknologi yang terus berubah dengan cepat dan mengikuti standar serta praktik terbaik yang berlaku di dunia internasional. Namun, semua itu harus tetap disesuaikan dengan kondisi dan kebutuhan khusus di Indonesia agar aturan yang dibuat benar-benar efektif dan relevan. (Wibowo et al., 2025)

KESIMPULAN

Perlindungan data pribadi di era digital merupakan isu yang semakin krusial di Indonesia, seiring dengan meningkatnya insiden kebocoran data dan ancaman terhadap privasi individu. Meskipun pemerintah telah mengesahkan UU No. 27 Tahun 2022 sebagai kerangka hukum perlindungan data pribadi, implementasi di lapangan masih menghadapi berbagai tantangan, seperti kebutuhan aturan turunan, pengawasan yang efektif, sinkronisasi regulasi, serta rendahnya literasi masyarakat terkait pentingnya menjaga data pribadi. Kasus-kasus kebocoran data yang terjadi pada institusi besar menunjukkan bahwa perlindungan data tidak hanya menjadi tanggung jawab pemerintah, tetapi juga membutuhkan peran aktif sektor swasta dan masyarakat. Kolaborasi multi-pihak, penguatan sistem keamanan digital, dan peningkatan kesadaran masyarakat sangat diperlukan untuk mewujudkan ekosistem digital yang aman dan terpercaya, sehingga hak privasi setiap individu dapat terlindungi secara optimal di tengah pesatnya transformasi digital di Indonesia.

DAFTAR PUSTAKA

Bua, I. I. T., & Idris, N. N. I. (2025, Mei). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. *Desentralisasi : Jurnal Hukum, Kebijakan Publik, dan Pemerintahan*, *Volume 2, Nomor. 2*(E-ISSN: 3063-2803), 107. https://doi.org/10.62383/desentralisasi.v2i2.653

Mahameru, D. E., Nurhalizah, A., Wildan, A., Badjeber, o. o. H., & Rahmadia, M. M. H. (2023, Desember). *IMPLEMENTASI UU PERLINDUNGAN DATA PRIBADI TERHADAP KEAMANAN*

INFORMASI IDENTITAS DI INDONESIA. *Jurnal Esensi Hukum*, *Volume 5 No. 2*(E-ISSN: 2761-2982), 115. https://journal.upnvj.ac.id/index.php/esensihukum/index

Saly, J. N., Artamevia, H., Kheista, K., Saputra Gulo, B. J., Rhemrev, E. E. A., & Christie, M. (2023, Oktober). *ANALISIS PERLINDUNGAN DATA PRIBADI TERKAIT UU NO.27 TAHUN 2022*. *Jurnal Serina Sosial Humaniora*, *Vol. 1, No. 3*(ISSN-L 2987-1506), 145-153.

Wibowo, Y., DPW, I. A., & Ismiyanto. (2025). *Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi*. *Jurnal Serambi Hukum*, *Vol 18 No 01*.

Ashari, M. (2022, March 22). *Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi*. Website DJKN. Retrieved June 22, 2025, from https://www.djkn.kemenkeu.go.id/artikel/baca/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html

Jannah, L. M. (2022, September 21). *UU Perlindungan Data Pribadi dan Tantangan Implementasinya – Fakultas Ilmu Administrasi UI*. Fakultas Ilmu Administrasi UI. Retrieved June 22, 2025, from https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/

Firdaus, A. (2024, June 27). *Kasus Kebocoran Data Pribadi di Indonesia: 10 Kejadian Terbesar yang Perlu Diketahui*. Medcom.id. Retrieved June 22, 2025, from https://www.medcom.id/teknologi/news-teknologi/8koPDdWK-kasus-kebocoran-data-pribadi-di-indonesia-10-kejadian-terbesar-yang-perlu-diketahui

Hadijah, S. (2024, November 6). *Teknologi Digital: Pengertian, Perkembangan, Kelebihan dan Kekurangannya*, cermati.com. https://www.cermati.com/artikel/teknologi-digital

Artikel JDIH. (2024, December 2). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP): Menjaga Keamanan dan Privasi Data Warga Negara*. JDIH - Kota Semarang. Retrieved June 22, 2025, from https://jdih.semarangkota.go.id/artikel/view/undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-pdp-menjaga-keamanan-dan-privasi-data-warga-negara

Nit. (2024, December 17). *UU Perlindungan Data Pribadi untuk Ekosistem Digital yang Aman, Terpercaya, dan Inklusif di Bidang Pengadaan Barang/Jasa*. LKPP. Retrieved June 22, 2025, from https://www.lkpp.go.id/read/bu/uu-perlindungan-data-pribadi-untuk-ekosistem-digital-yang-aman-terpercaya-dan-inklusif-di-bidang-pengadaan-barang-jasa

Husnul, F. (2025, February 13). *Pelajaran Berharga dari 10 Kasus Kebocoran Data Perusahaan di Indonesia!* Gudang SSL. Retrieved June 22, 2025, from https://gudangssl.id/blog/kasus-kebocoran-data-perusahaan/