JIIC: JURNAL INTELEK INSAN CENDIKIA
https://jicnusantara.com/index.php/jiic
Vol : 03 No: 04, April 2026
E-ISSN : 3047-7824

Keamanan Data Pribadi di Era Digital: Tanggung Jawab Siapa?

Personal Data Security in the Digital Age: Whose Responsibility Is It?

Merisa Juliani
Universitas Islam Riau
Email: risacuuu@gmail.com

Article Info

Article history:
Received : 19-04-2026
Revised : 21-04-2026
Accepted : 23-04-2026
Pulished : 25-04-2026

Abstract

The rapid development of digital technology has transformed social interactions while simultaneously creating serious threats to personal data security. Indonesia is recorded as one of the countries with the highest number of data breaches globally, with more than 111 alleged data leak cases handled by the Ministry of Communication and Information Technology from 2019 to mid-2024. This article aims to analyze the parties responsible for personal data protection in the digital era, namely individuals, digital service providers, and the government. The method applied is normative juridical research using a library research approach that examines laws and regulations, scientific journals, and official institutional reports. The findings show that personal data protection cannot be placed on only one party, but instead constitutes a collective responsibility. Individuals play a role through improving digital literacy and awareness in safeguarding data, companies bear legal and ethical responsibilities in managing user data in accordance with Law Number 27 of 2022 concerning Personal Data Protection, while the government serves as regulator and supervisor through law enforcement and the establishment of an independent supervisory body. In conclusion, personal data security requires synergy between the community, business actors, and the government so that public trust in the digital ecosystem can be maintained.

Keywords: personal data security; digital era; responsibility

Abstrak

Perkembangan teknologi digital yang pesat telah mengubah pola interaksi masyarakat sekaligus menimbulkan ancaman serius terhadap keamanan data pribadi. Indonesia tercatat sebagai salah satu negara dengan kasus kebocoran data tertinggi di dunia, dengan lebih dari 111 kasus dugaan kebocoran data yang ditangani Kementerian Komunikasi dan Informatika sepanjang tahun 2019 hingga pertengahan 2024. Artikel ini bertujuan untuk menganalisis pihak-pihak yang bertanggung jawab atas perlindungan data pribadi di era digital, yaitu individu, perusahaan penyedia layanan digital, dan pemerintah. Metode yang digunakan adalah yuridis normatif dengan pendekatan studi kepustakaan (library research) terhadap peraturan perundang-undangan, jurnal ilmiah, dan laporan lembaga resmi. Hasil kajian menunjukkan bahwa perlindungan data pribadi tidak dapat dibebankan kepada satu pihak saja, melainkan merupakan tanggung jawab kolektif. Individu berperan melalui peningkatan literasi digital dan kesadaran menjaga data, perusahaan bertanggung jawab secara hukum dan etis dalam mengelola data pengguna sesuai Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, sedangkan pemerintah berperan sebagai regulator dan pengawas melalui penegakan hukum serta pembentukan lembaga pengawas independen. Simpulannya, keamanan data pribadi membutuhkan sinergi antara masyarakat, pelaku usaha, dan pemerintah agar kepercayaan publik terhadap ekosistem digital dapat terjaga.

Kata Kunci: keamanan data pribadi; era digital; tanggung jawab.

PENDAHULUAN

Transformasi digital telah menjadi fenomena global yang mengubah hampir seluruh aspek kehidupan manusia. Di Indonesia, tingkat penetrasi internet terus mengalami peningkatan signifikan setiap tahunnya. Berdasarkan hasil Survei Penetrasi Internet yang dirilis oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2024), jumlah pengguna internet di Indonesia telah menembus angka 221 juta orang atau setara dengan 79,5% dari total populasi nasional. Angka ini menunjukkan bahwa masyarakat Indonesia semakin bergantung pada layanan digital dalam berbagai aktivitas sehari-hari, mulai dari berbelanja melalui platform e-commerce, menggunakan layanan perbankan digital, memesan transportasi daring, hingga berkomunikasi melalui media sosial.

Kemudahan yang ditawarkan oleh teknologi digital ternyata menyimpan persoalan serius yang sering kali kurang disadari oleh pengguna, yaitu ancaman terhadap keamanan data pribadi. Dalam beberapa tahun terakhir, Indonesia dihadapkan pada maraknya kasus kebocoran data yang menimbulkan keresahan luas di tengah masyarakat. Data Kementerian Komunikasi dan Informatika mencatat bahwa sepanjang tahun 2019 hingga 14 Mei 2024 terdapat 124 kasus dugaan pelanggaran pelindungan data pribadi, 111 di antaranya merupakan kasus kebocoran data (Kompas.id, 2024). Angka ini menempatkan Indonesia dalam daftar sepuluh negara dengan kebocoran data terbesar di dunia menurut laporan Surfshark, dengan total 156,8 juta data yang bocor sejak 2004 hingga April 2024 (Sibermate, 2024).

Kasus-kasus kebocoran data yang menonjol antara lain peretasan data Direktorat Jenderal Pajak pada September 2024 yang melibatkan sekitar enam juta data Nomor Pokok Wajib Pajak (NPWP), termasuk data Presiden Joko Widodo dan para menterinya (Tempo, 2024). Selain itu, serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) di Surabaya pada Juni 2024 berhasil melumpuhkan layanan 210 instansi pemerintah dengan permintaan tebusan sebesar delapan juta dolar Amerika Serikat (CyberStudio, 2024). Kasus-kasus tersebut membuktikan bahwa ancaman kebocoran data bukan lagi sekadar persoalan teknis, melainkan persoalan sistemik yang memerlukan penanganan menyeluruh.

Kebocoran data pribadi dapat menimbulkan dampak yang sangat merugikan. Data yang jatuh ke tangan pihak yang tidak bertanggung jawab berpotensi disalahgunakan untuk berbagai tindakan kriminal seperti penipuan digital, pencurian identitas, pengambilalihan akun, hingga pembobolan rekening nasabah. Menurut Disemadi dkk. (2023), dampak kebocoran data tidak hanya bersifat finansial, tetapi juga dapat merusak reputasi individu serta menurunkan kepercayaan publik terhadap penyelenggara layanan digital. Di sisi lain, survei Katadata Insight Center menemukan bahwa 34,3% masyarakat Indonesia merasa khawatir terhadap kemungkinan penyalahgunaan data pribadi mereka di internet (Katadata, 2023).

Pemerintah Indonesia sebenarnya telah merespons persoalan tersebut dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) pada 17 Oktober 2022. Undang-undang ini menjadi tonggak penting karena merupakan regulasi pertama yang secara komprehensif mengatur perlindungan data pribadi di Indonesia (JDIH Kota Semarang, 2023). Namun demikian, implementasi dan penegakan UU PDP masih menghadapi berbagai tantangan, termasuk belum terbentuknya lembaga pengawas independen yang diamanatkan undang-undang (Kompas.id, 2025).

Permasalahan keamanan data pribadi tidak dapat dipahami hanya sebagai persoalan teknis atau hukum semata. Rendahnya literasi digital masyarakat turut menjadi faktor yang memperparah situasi. Hasil survei APJII tahun 2025 menunjukkan bahwa 41% pengguna internet di Indonesia tidak menyadari bahwa akun atau perangkat mereka pernah mengalami masalah keamanan, dan penggunaan langkah proteksi seperti autentikasi dua faktor (Two-Factor Authentication) masih sangat minim (Internet Sehat, 2025). Kondisi ini menunjukkan bahwa perlindungan data pribadi merupakan isu multidimensi yang memerlukan kolaborasi lintas pihak.

Berdasarkan latar belakang tersebut, artikel ini bertujuan untuk menjawab pertanyaan utama: siapakah sebenarnya yang bertanggung jawab atas keamanan data pribadi di era digital? Kajian ini akan menganalisis peran individu sebagai pengguna teknologi, peran perusahaan sebagai pengendali data, serta peran pemerintah sebagai regulator dan pengawas, sekaligus mengkaji bagaimana sinergi ketiganya dapat menciptakan ekosistem perlindungan data pribadi yang lebih kokoh di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan studi kepustakaan (library research). Menurut Soekanto dan Mamudji (2015), penelitian yuridis normatif merupakan penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan mengadakan penelusuran terhadap peraturan-peraturan dan literatur yang berkaitan dengan permasalahan yang diteliti. Pendekatan ini dipilih karena kajian keamanan data pribadi bersifat normatif-konseptual dan berkaitan erat dengan peraturan perundang-undangan yang berlaku.

Sumber data dalam penelitian ini terdiri atas tiga jenis bahan hukum. Pertama, bahan hukum primer berupa Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Kedua, bahan hukum sekunder berupa jurnal ilmiah nasional yang relevan, buku teks, dan hasil penelitian terdahulu. Ketiga, bahan hukum tersier yang meliputi laporan resmi lembaga seperti APJII, Kementerian Komunikasi dan Informatika, Badan Siber dan Sandi Negara (BSSN), serta pemberitaan media daring yang kredibel.

Teknik pengumpulan data dilakukan melalui studi dokumentasi, yaitu dengan menghimpun, membaca, mencatat, dan mengklasifikasikan berbagai bahan hukum serta literatur yang berkaitan dengan tema penelitian. Data yang terkumpul kemudian dianalisis secara kualitatif dengan metode deskriptif-analitis. Menurut Sugiyono (2019), analisis kualitatif merupakan proses penyusunan data secara sistematis dengan mengorganisasikan data, menjabarkan ke dalam unit-unit, menyusun pola, memilih mana yang penting dan mana yang akan dipelajari, serta membuat simpulan. Hasil analisis kemudian disajikan secara deskriptif untuk menjawab permasalahan mengenai tanggung jawab para pihak terhadap keamanan data pribadi di era digital.

HASIL DAN PEMBAHASAN

Kondisi Keamanan Data Pribadi di Indonesia

Kondisi keamanan data pribadi di Indonesia berada pada tingkat yang cukup memprihatinkan. Laporan Indonesian Cyber Security Forum 2024 yang dikutip oleh Kompas.id (2025) menyebutkan bahwa lebih dari 2,3 miliar catatan data pribadi milik warga Indonesia beredar di berbagai forum gelap (dark forum) dalam kurun waktu tiga tahun terakhir. Angka ini menempatkan Indonesia sebagai salah satu target utama kejahatan siber di kawasan Asia Tenggara.

Data Badan Siber dan Sandi Negara (BSSN) sepanjang tahun 2023 mencatat 103 dugaan insiden kebocoran data di Indonesia, dengan mayoritas sebesar 69% terjadi di sektor administrasi pemerintahan (Sibermate, 2024). Kondisi ini menunjukkan bahwa instansi pemerintah, yang seharusnya menjadi garda terdepan dalam melindungi data masyarakat, justru menjadi sektor paling rentan terhadap serangan siber. Selain itu, pada 2023 Indonesia juga mengalami lebih dari 350 juta insiden serangan siber yang menyebabkan kerugian mencapai satu juta dolar Amerika Serikat atau setara dengan Rp15,9 miliar (Tempo, 2024).

Kasus-kasus besar yang terjadi memperkuat gambaran tersebut. Pada Mei 2021, sebanyak 279 juta data peserta Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan diduga bocor dan dijual di dark web, termasuk nama, Nomor Induk Kependudukan (NIK), alamat, nomor telepon, dan riwayat kesehatan (CyberStudio, 2024). Pada Juli 2023, data kependudukan Direktorat Jenderal Dukcapil Kementerian Dalam Negeri diduga bocor sebanyak 337 juta data. Selanjutnya pada Juli 2023 pula, dilaporkan 35 juta data paspor Warga Negara Indonesia beredar di dark web (Tempo, 2024). Rentetan kasus ini menunjukkan bahwa perlindungan data pribadi di Indonesia belum berjalan sebagaimana mestinya.

Tanggung Jawab Individu sebagai Pengguna Teknologi

Individu sebagai pengguna teknologi memiliki tanggung jawab pertama dalam menjaga keamanan data pribadinya. Menurut Daeng dkk. (2023), setiap pengguna internet perlu memiliki kesadaran dan pengetahuan yang memadai tentang pentingnya melindungi informasi pribadi di ruang digital. Kesadaran ini meliputi pemahaman tentang jenis data yang harus dilindungi, cara mengelola kata sandi yang aman, serta kehati-hatian dalam membagikan informasi pribadi di media sosial.

Sayangnya, hasil survei APJII (2025) menunjukkan bahwa 41% pengguna internet di Indonesia tidak menyadari bahwa akun atau perangkat mereka pernah mengalami masalah keamanan. Penggunaan fitur keamanan seperti autentikasi dua faktor dan Virtual Private Network (VPN) juga masih sangat minim, bahkan banyak pengguna yang tidak pernah mengganti kata sandi sejak akun dibuat (Internet Sehat, 2025). Kondisi ini berbanding lurus dengan rendahnya tingkat literasi digital sebagian masyarakat Indonesia, yang menurut Widya Security (2024) terbukti menjadi faktor utama meningkatnya kerentanan pengguna terhadap kejahatan siber.

Literasi digital sendiri terdiri atas empat pilar, yaitu digital skill, digital culture, digital safety, dan digital ethics (Widya Security, 2024). Pilar digital safety menjadi aspek yang paling berkaitan langsung dengan perlindungan data pribadi. Budiono dkk. (2025) menjelaskan bahwa rendahnya digital safety pengguna menjadikan mereka rentan terhadap serangan phishing, yaitu manipulasi psikologis untuk memperoleh data sensitif. Oleh karena itu, peningkatan kesadaran

pengguna mengenai pentingnya verifikasi sumber informasi, pengelolaan kata sandi yang kuat, serta penggunaan fitur keamanan tambahan menjadi keharusan di era digital ini.

Lebih lanjut, Astriani (2020) menegaskan bahwa perlindungan data pribadi memerlukan pendekatan preventif dari sisi pengguna melalui penerapan praktik keamanan dasar seperti tidak sembarangan mengklik tautan yang tidak jelas, tidak membagikan One-Time Password (OTP) kepada siapapun, serta memverifikasi keaslian aplikasi atau situs sebelum memberikan informasi pribadi. Dengan demikian, individu memiliki peran kunci sebagai lini pertahanan pertama dalam ekosistem perlindungan data pribadi.

Tanggung Jawab Perusahaan Penyedia Layanan Digital

Perusahaan penyedia layanan digital, yang dalam UU PDP disebut sebagai Pengendali Data Pribadi, memegang tanggung jawab besar dalam melindungi data pengguna. Pasal 20 Undang-Undang Nomor 27 Tahun 2022 mewajibkan Pengendali Data Pribadi untuk memiliki dasar hukum yang sah dalam memproses data pribadi, baik berupa persetujuan subjek data maupun dasar hukum lain yang diatur undang-undang (BPK, 2022). Selain itu, Pasal 35 dan 36 UU PDP mewajibkan perusahaan untuk melindungi dan memastikan keamanan data pribadi dari pemrosesan yang tidak sah, akses yang tidak sah, dan tindakan kejahatan siber lainnya.

Studi yang dilakukan oleh Saputra dkk. (2024) dalam kasus kebocoran data Tokopedia tahun 2020 menunjukkan bahwa perusahaan e-commerce memiliki kewajiban ganda, yaitu tanggung jawab hukum dan tanggung jawab etis. Secara hukum, perusahaan dapat dikenakan sanksi administratif, perdata, bahkan pidana apabila terbukti lalai dalam melindungi data pengguna. Secara etis, perusahaan memiliki kewajiban moral untuk menjaga kepercayaan konsumen yang telah mempercayakan data pribadinya kepada platform digital yang mereka kelola.

Causa Jurnal Hukum dan Kewarganegaraan (2024) menegaskan bahwa pelanggaran data dapat menyebabkan kerugian finansial yang signifikan bagi pelaku usaha, termasuk denda administratif, hilangnya kepercayaan konsumen, dan tingginya biaya pemulihan data. Berdasarkan UU PDP, sanksi administratif dapat berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, hingga denda administratif hingga 2% dari pendapatan tahunan perusahaan. Bahkan sanksi pidana berupa penjara paling lama enam tahun dan/atau denda paling banyak Rp6 miliar dapat dijatuhkan bagi pelanggaran berat (JDIH Kemenko Infra, 2022).

Untuk memenuhi tanggung jawab tersebut, perusahaan perlu membangun sistem keamanan berlapis. HAM Perlindungan Data Pribadi (Media Akademik, 2024) merekomendasikan beberapa langkah yang harus dilakukan perusahaan, yaitu (a) menyediakan kebijakan privasi yang mudah dipahami pengguna, (b) melakukan audit keamanan data secara berkala, (c) membatasi akses data pribadi hanya kepada pihak yang berwenang, dan (d) menyelenggarakan pelatihan keamanan siber bagi seluruh karyawan. Dengan demikian, perusahaan tidak hanya memenuhi aspek kepatuhan hukum, tetapi juga membangun budaya perlindungan data pribadi yang berkelanjutan.

Tanggung Jawab Pemerintah sebagai Regulator dan Pengawas

Pemerintah memiliki peran strategis dalam menciptakan ekosistem perlindungan data pribadi yang kuat melalui tiga fungsi utama, yaitu sebagai regulator, pengawas, dan fasilitator edukasi publik. Sebagai regulator, pemerintah telah mengesahkan UU PDP pada 17 Oktober 2022

yang menjadi payung hukum komprehensif pertama di Indonesia untuk perlindungan data pribadi (JDIH Kota Semarang, 2023). UU ini mengatur secara rinci mengenai asas, jenis data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, transfer data lintas negara, serta ketentuan sanksi administratif dan pidana (BPK, 2022).

Keberadaan UU PDP memberikan harmonisasi dengan standar internasional seperti General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa (Fakultas Hukum Untar, 2025). Harmonisasi ini penting karena data pribadi sering kali mengalir lintas negara melalui berbagai platform digital global. Namun, keberlakuan UU PDP masih menghadapi berbagai tantangan implementasi. Salah satu tantangan terbesar adalah belum terbentuknya lembaga pengawas independen yang diamanatkan oleh undang-undang. Kompas.id (2025) melaporkan bahwa meski sudah lebih dari tiga tahun sejak UU PDP disahkan, pembentukan lembaga pengawas data pribadi yang independen belum juga terealisasi.

Fungsi kedua pemerintah adalah sebagai pengawas atas pengelolaan data pribadi oleh berbagai pihak. Pengawasan ini mencakup pemantauan kepatuhan pengendali data terhadap ketentuan UU PDP, penanganan laporan pelanggaran data, serta penindakan terhadap pelaku kejahatan siber. Sayangnya, kapasitas pengawasan pemerintah masih terbatas. Hal ini terlihat dari sulitnya pengusutan kasus-kasus kebocoran data besar yang sebagian besar pelakunya belum berhasil diidentifikasi dan diadili. Sukamta (2024) dalam JDIH DPR menekankan bahwa komitmen pemerintah dan institusi terkait untuk berbenah diri menjadi kunci utama dalam menjaga keamanan data masyarakat.

Fungsi ketiga adalah sebagai fasilitator edukasi publik. Pemerintah melalui Kementerian Komunikasi dan Informatika bersama Siberkreasi telah menjangkau lebih dari 14,6 juta masyarakat Indonesia melalui program literasi digital sejak tahun 2021 (Pemkab Pesisir Selatan, 2023). Program ini berfokus pada empat pilar literasi digital: keterampilan digital, budaya digital, etika digital, dan keamanan digital. Meski demikian, cakupan program ini masih perlu diperluas, mengingat jumlah pengguna internet Indonesia yang telah mencapai 221 juta orang (APJII, 2024). Kolaborasi lintas sektor antara pemerintah, sektor swasta, dan institusi pendidikan menjadi kunci agar literasi digital masyarakat dapat meningkat secara signifikan.

Sinergi Tiga Pilar dalam Perlindungan Data Pribadi

Berdasarkan analisis di atas, dapat dipahami bahwa keamanan data pribadi tidak dapat dibebankan kepada satu pihak saja. Diperlukan sinergi yang harmonis antara tiga pilar utama: individu, perusahaan, dan pemerintah. Menurut Disemadi dkk. (2023), perlindungan data pribadi di era digital membutuhkan pendekatan multi-stakeholder karena tidak ada satu pihak pun yang mampu menjamin keamanan data secara mandiri. Setiap pihak memiliki peran yang saling melengkapi dalam membangun ekosistem perlindungan data yang tangguh.

Individu bertanggung jawab untuk meningkatkan literasi digital dan menerapkan praktik keamanan dasar secara konsisten. Perusahaan bertanggung jawab membangun sistem keamanan yang kuat dan patuh pada ketentuan hukum. Pemerintah bertanggung jawab menciptakan regulasi yang jelas, melakukan pengawasan yang ketat, dan memfasilitasi edukasi publik. Apabila salah satu pilar ini lemah, maka keseluruhan sistem perlindungan data akan ikut melemah. Sebaliknya, jika

ketiga pilar berjalan beriringan dan saling mendukung, Indonesia dapat membangun sistem perlindungan data yang setara dengan standar internasional (Fakultas Hukum Untar, 2025).

KESIMPULAN

Berdasarkan pembahasan yang telah dipaparkan, dapat disimpulkan bahwa keamanan data pribadi di era digital merupakan isu strategis yang memerlukan tanggung jawab kolektif dari tiga pihak utama: individu, perusahaan penyedia layanan digital, dan pemerintah. Tingginya kasus kebocoran data di Indonesia, yang tercatat mencapai 111 kasus sepanjang 2019 hingga pertengahan 2024, menunjukkan bahwa sistem perlindungan data pribadi di Indonesia masih jauh dari kata optimal.

Individu sebagai pengguna teknologi memiliki tanggung jawab untuk meningkatkan literasi digital, terutama pada aspek digital safety, agar mampu melindungi data pribadinya dari berbagai ancaman siber. Perusahaan penyedia layanan digital sebagai pengendali data memiliki kewajiban hukum dan etis untuk membangun sistem keamanan yang kuat sesuai dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pemerintah memegang peran sebagai regulator, pengawas, dan fasilitator edukasi publik, yang keberhasilannya sangat bergantung pada pembentukan lembaga pengawas independen dan penegakan hukum yang tegas.

Sinergi antara ketiga pilar tersebut menjadi kunci utama dalam mewujudkan ekosistem perlindungan data pribadi yang kokoh. Tanpa kolaborasi yang harmonis antara masyarakat, pelaku usaha, dan pemerintah, perlindungan data pribadi di era digital akan tetap menjadi persoalan laten yang sewaktu-waktu dapat menimbulkan kerugian besar, baik secara finansial maupun sosial.

SARAN

Berdasarkan simpulan di atas, beberapa saran yang dapat penulis berikan adalah sebagai berikut. Pertama, bagi masyarakat, perlu meningkatkan kesadaran dan pengetahuan tentang keamanan digital melalui kegiatan literasi digital yang diselenggarakan pemerintah maupun lembaga swadaya masyarakat, serta menerapkan praktik keamanan dasar seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, dan kehati-hatian dalam membagikan informasi pribadi di ruang digital.

Kedua, bagi perusahaan penyedia layanan digital, disarankan untuk melakukan investasi yang memadai dalam sistem keamanan siber, menyelenggarakan audit keamanan data secara berkala, serta memberikan pelatihan keamanan siber kepada seluruh karyawan. Perusahaan juga perlu menyusun kebijakan privasi yang transparan dan mudah dipahami pengguna, serta mematuhi seluruh ketentuan UU PDP.

Ketiga, bagi pemerintah, disarankan untuk segera membentuk lembaga pengawas independen perlindungan data pribadi sebagaimana diamanatkan UU PDP, memperkuat kapasitas penegakan hukum terhadap pelaku kejahatan siber, serta memperluas cakupan program literasi digital hingga menjangkau seluruh lapisan masyarakat, termasuk di daerah rural. Selain itu, pemerintah perlu memperkuat kerja sama internasional dalam penanganan kejahatan siber lintas negara. Keempat, bagi peneliti selanjutnya, kajian ini dapat dikembangkan lebih lanjut melalui pendekatan empiris untuk mengukur efektivitas implementasi UU PDP dan tingkat kesiapan para pihak dalam menjalankan tanggung jawabnya.

DAFTAR PUSTAKA

APJII. (2024). *Survei Penetrasi Pengguna Internet Indonesia 2024.* Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia. Diakses dari https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Astriani, R. (2020). Perlindungan data pribadi dalam era digital: Tantangan dan solusi. *Jurnal Ilmiah Hukum*, 20(2), 241–254.

Badan Pemeriksa Keuangan. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.* Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Diakses dari https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Budiono, B., Fadillah, F. R., & Arinudin, N. (2025). The dangers of phishing to personal data security. *Formosa Journal of Applied Sciences*, 4(3), 831–844.

Causa: Jurnal Hukum dan Kewarganegaraan. (2024). Tanggung jawab hukum dan ekonomi dalam perlindungan data pribadi di era digital. *Causa: Jurnal Hukum dan Kewarganegaraan*, 7(12), 31–40. https://doi.org/10.3783/causa.v7i12.7183

CyberStudio. (2024). *5 kasus kebocoran data pribadi di Indonesia dan penanganannya.* Diakses dari https://cyberstudio.id/blog/kasus-kebocoran-data-pribadi-di-indonesia/

Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., & Saputra, H. (2023). Perlindungan data pribadi dalam era digital: Tinjauan terhadap kerangka hukum perlindungan privasi. *Innovative: Journal of Social Science Research*, 3(6), 2898–2905.

Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). Perlindungan data pribadi di era digital: Mengapa kita perlu peduli? *Sang Sewagati Journal*, 1(2), 66–90.

Fakultas Hukum Universitas Tarumanagara. (2025). *Perlindungan data pribadi: Implementasi UU No. 27 Tahun 2022 dan tantangan penegakannya.* Diakses dari https://fh.untar.ac.id/2025/09/11/perlindungan-data-pribadi-implementasi-uu-no-27-tahun-2022-dan-tantangan-penegakannya/

Internet Sehat. (2025). *Lanskap pengguna internet Indonesia 2025: Koneksi meluas, literasi masih lemas.* Diakses dari https://internetsehat.id/2025/08/08/lanskap-pengguna-internet-indonesia-2025-koneksi-meluas-literasi-masih-lemas/

JDIH Kemenko Infra. (2022). *UU No. 27/2022: Pelindungan data pribadi.* Diakses dari https://jdih.kemenkoinfra.go.id/uu-no-272022-pelindungan-data-pribadi

JDIH Kota Semarang. (2023). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP): Menjaga keamanan dan privasi data warga negara.* Diakses dari 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

Kompas.id. (2024). *Kasus kebocoran data terulang, ada apa?* Diakses dari https://www.kompas.id/baca/ekonomi/2024/09/24/kasus-kebocoran-data-terulang-ada-apa

Kompas.id. (2025). *Kebocoran data pribadi terus mengancam, lembaga pengawas tak kunjung dibentuk.* Diakses dari https://www.kompas.id/artikel/en-kebocoran-data-pribadi-terus-mengancam-lembaga-pengawas-tak-kunjung-dibentuk

Media Akademik. (2024). HAM perlindungan data pribadi: Tantangan dan solusi. *Jurnal Media Akademik.* Diakses dari https://jurnal.mediaakademik.com/index.php/jma/article/download/2598/2042

Pemerintah Kabupaten Pesisir Selatan. (2023). *Kondisi literasi digital masyarakat Indonesia.* Diakses dari https://berita.pesisirselatankab.go.id/berita/detail/kondisi-literasi-digital-masyarakat-indonesia

Saputra, H., Ketia, G., Situmorang, B., Napitupulu, D. F., Siagian, Y. E., Sihaloho, C. N., Sitanggang, C. B., & Pinem, D. A. (2024). Analisis tanggung jawab etis dan hukum perusahaan e-commerce terhadap perlindungan data pribadi konsumen: Studi kasus kebocoran data Tokopedia 2020. *Scientific Journal of Reflection: Economic, Accounting, Management and Business*, 9(1), 120–127.

Sibermate. (2024). *Krisis kebocoran data pribadi: Tata kelola yang buruk di Indonesia.* Diakses dari https://sibermate.com/hrmi/krisis-kebocoran-data-pribadi-tata-kelola-yang-buruk-di-indonesia

Soekanto, S., & Mamudji, S. (2015). *Penelitian hukum normatif: Suatu tinjauan singkat* (Cet. ke-17). Jakarta: Rajawali Pers.

Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D.* Bandung: Alfabeta.

Tempo. (2024). *Polemik data pribadi: 5 kasus kebocoran data di Indonesia selama 2023–2024.* Diakses dari https://www.tempo.co/digital/polemik-data-pribadi-5-kasus-kebocoran-data-di-indonesia-selama-2023-2024-2052924

Widya Security. (2024). *Pentingnya literasi digital untuk keamanan siber Indonesia.* Diakses dari https://widyasecurity.com/2024/03/21/pentingnya-literasi-digital-untuk-keamanan-siber-indonesia/