JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 766-773
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Analisis Penerapan Keamanan Siber dalam Melindungi Data Pribadi Pengguna Pada Era Transformasi Digital

Marisa Siregar[1], Rahmadhani Dongoran[2], Manisa Safitri Tanjung[3], Dennis Alhaadi Effendi[4], Sahat Parulian Sitorus[5]

[1,2,3,4,5]Universitas Labuhanbatu, Indonesia

Email: risasiregar@gmail.com

ABSTRAK

Penerapan teknologi informasi yang pesat pada era transformasi digital berdampak signifikan terhadap pola pengumpulan, pemrosesan, dan penyimpanan data pribadi pengguna. Kemajuan ini disertai peningkatan ancaman kejahatan siber seperti serangan phishing, pelanggaran data, dan penipuan digital melalui rekayasa sosial. Penelitian ini bertujuan menganalisis penerapan keamanan siber dalam melindungi data pribadi pengguna serta mengidentifikasi tantangan implementasi regulasi perlindungan data pribadi di Indonesia. Metode yang digunakan adalah penelitian normatif-hukum dengan pendekatan konseptual, yang mengkaji peran lembaga negara seperti Badan Siber dan Sandi Negara (BSSN) dan Direktorat Tindak Pidana Siber (*Dittipidsiber*) dalam penanganan pelanggaran data pribadi. Hasil penelitian menunjukkan bahwa meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah memberikan kerangka hukum yang jelas, implementasinya masih menghadapi tantangan dalam aspek teknis, koordinasi kelembagaan, dan literasi digital masyarakat. Diperlukan sinergi kuat antara regulasi, pengawasan, dan pendidikan publik untuk mewujudkan perlindungan data pribadi yang efektif dan berkelanjutan di era digital. Kata Kunci: keamanan siber, data pribadi, transformasi digital, perlindungan data, UU PDP 1.

Kata Kunci: Sistem Pendukung Keputusan, *Simple Additive Weighting*, SAW, Menu Paket Hemat, Ayam Geprek Nahla.

ABSTRACT

The rapid advancement of information technology in the digital transformation era has significantly impacted patterns of collecting, processing, and storing user personal data. This progress is accompanied by an increase in cybercrime threats such as phishing attacks, data breaches, and digital fraud through social engineering. This study aims to analyze cybersecurity implementation in protecting user personal data and identify challenges in enforcing personal data protection regulations in Indonesia. Using a normative-legal research method with a conceptual approach, this study examines the role of state institutions such as the National Cyber and Crypto Agency (BSSN) and the Cyber Crime Directorate (*Dittipidsiber*) in handling personal data breaches. The results indicate that although Law Number 27 of 2022 on Personal Data Protection (UU PDP) has established a clear legal framework, its implementation still faces challenges in technical aspects, institutional coordination, and public digital literacy. Strong synergy between regulation, supervision, and public education is required to achieve effective and sustainable personal data protection in the digital era. Keywords: cybersecurity, personal data, digital transformation, data protection, UU PDP.

Keywords: Decision Support System, Simple Additive Weighting, SAW, Value-for-Money Menu, Ayam Geprek Nahla.

PENDAHULUAN

Perkembangan teknologi digital pada abad ke-21 telah mengubah paradigma fundamental kehidupan masyarakat global. Era transformasi digital yang ditandai oleh adopsi internet, komputasi awan, kecerdasan buatan, big data, dan teknologi 5G telah menciptakan ekosistem baru yang memungkinkan interaksi, kerja, dan transaksi dilakukan secara cepat, efisien, dan lintas batas. Indonesia, sebagai negara dengan populasi digital terbesar di Asia Tenggara, mengalami pertumbuhan signifikan dalam penetrasi internet yang kini mencapai lebih dari 70% dari total populasi (Bappenas, 2025).

Di tengah ekspansi digital yang masif ini, data pribadi pengguna mencakup nama, nomor identitas, informasi keuangan, riwayat kesehatan, hingga perilaku konsumen semakin menjadi aset strategis dalam ekosistem ekonomi digital. Perusahaan memanfaatkan data tersebut untuk personalisasi layanan, analisis pasar, dan peningkatan pengalaman pengguna. Namun, ketika data pribadi bocor atau disalahgunakan, individu 2 dapat menanggung kerugian material dan non-material yang serius, mulai dari penipuan finansial, kerusakan reputasi, hingga pelanggaran privasi yang mendalam (Darul Huda, 2024).

Indonesia mencatat sejumlah insiden pelanggaran data yang mengkhawatirkan, termasuk kebocoran data 27 juta anggota BPJS Kesehatan pada tahun 2021 dan serangan terhadap Pusat Data Nasional (PDN) pada tahun 2024. Kejadian-kejadian ini menggarisbawahi betapa lemahnya tata kelola keamanan siber pada institusi publik dan swasta, serta menuntut penguatan kerangka regulasi maupun kapasitas teknis secara menyeluruh

Penelitian ini berpijak pada tiga landasan teori utama. *Pertama*, teori keamanan siber (*cybersecurity*) yang merujuk pada serangkaian praktik, teknologi, dan proses yang dirancang untuk melindungi sistem, jaringan, dan data dari serangan digital atau akses tidak sah. Prinsip dasar keamanan siber dikenal dengan CIA Triad, yang mencakup *Confidentiality* (kerahasiaan data), *Integrity* (keutuhan data), dan *Availability* (ketersediaan data) (Direktorat Jenderal PU, 2024).

Kedua, teori perlindungan data pribadi yang merujuk pada seperangkat hak, kewajiban, dan prinsip untuk melindungi informasi pribadi dari penggunaan tidak sah. Prinsip-prinsip tersebut meliputi pembatasan tujuan (purpose limitation), minimasi data (data minimization), kualitas data (data quality), keamanan data (data security), dan keterbukaan informasi (transparency), sebagaimana diadopsi dalam UU PDP Nomor 27 Tahun 2022.

Ketiga, teori rekayasa sosial (social engineering) dalam konteks keamanan siber, yang merujuk pada teknik manipulasi psikologis untuk mendorong individu memberikan 3 informasi sensitif atau melakukan tindakan yang membahayakan keamanan sistem. Serangan phishing merupakan manifestasi paling umum dari social engineering yang terus berkembang bentuk dan kecanggihannya (Appisi, 2025).

METODE PENELITIAN

Penelitian ini menggunakan metode hukum normatif dengan pendekatan konseptual untuk menganalisis ketentuan hukum yang berlaku terkait perlindungan data pribadi dan keamanan siber di Indonesia, terutama setelah berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pendekatan konseptual digunakan untuk mengkaji perspektif teoretis mengenai keamanan siber, perlindungan data pribadi, dan rekayasa sosial, sehingga memungkinkan analisis yang mencakup dimensi hukum, teknis, dan sosial secara terpadu. Sumber data penelitian terdiri atas data primer dan data sekunder. Data primer meliputi UU PDP, peraturan pemerintah terkait keamanan siber yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN) serta Kementerian Komunikasi dan Informatika, dokumen resmi BSSN berupa laporan, standar, dan kebijakan keamanan siber nasional, serta laporan tindak pidana siber dari Direktorat Tindak Pidana Siber (*Dittipidsiber*) Kepolisian Republik Indonesia.

Data sekunder diperoleh dari jurnal ilmiah nasional dan internasional yang membahas keamanan siber, perlindungan data, dan transformasi digital yang diterbitkan dalam rentang tahun 2015–2025, laporan kebijakan dari Pemerintah Indonesia, OECD, World Bank, dan UNESCO, serta studi kasus pelanggaran data BPJS Kesehatan tahun 2021 dan Pusat Data Nasional (PDN) tahun 2024 sebagai referensi empiris. Data dikumpulkan melalui studi literatur, analisis dokumen, dan studi kasus. Dari 45 artikel yang teridentifikasi melalui Google Scholar dan berbagai basis data akademik lainnya, sebanyak 12 artikel dipilih sebagai sumber analisis kualitatif berdasarkan relevansi topik. Selanjutnya, data dianalisis menggunakan pendekatan deskriptif-analitik yang mencakup klasifikasi data berdasarkan topik dan relevansi, identifikasi pola dan tren implementasi keamanan siber, analisis komparatif antara regulasi yang berlaku dan implementasi praktis, serta evaluasi efektivitas kebijakan dan identifikasi kesenjangan yang masih ada.

HASIL DAN PEMBAHASAN

Ancaman Keamanan Siber yang Menargetkan Data Pribadi

Ancaman keamanan siber terhadap data pribadi pengguna terus berkembang dalam hal bentuk, skala, dan kecanggihannya. kajian terhadap berbagai literatur dan laporan resmi mengidentifikasi empat kategori ancaman utama yang paling dominan di era transformasi digital.

Phishing dan rekayasa sosial

Serangan phishing merupakan ancaman paling dominan dalam lanskap keamanan siber saat ini. phishing adalah modus penipuan digital yang bertujuan memperoleh data pribadi secara tidak sah melalui rekayasa sosial dan manipulasi psikologis. pelaku menggunakan email, pesan singkat (*sms phishing*), atau situs web palsu yang tampak otentik untuk mengelabui pengguna agar secara sukarela menyerahkan informasi sensitif seperti kata sandi, nomor kartu kredit, dan data

identifikasi lainnya (appisi, 2025). teknik rekayasa sosial dalam serangan phishing memanfaatkan emosi manusia, seperti rasa urgensi, ketakutan, atau ketertarikan pada imbalan. pelaku kerap mengatasnamakan institusi tepercaya seperti bank, lembaga pemerintah, atau perusahaan ternama untuk meningkatkan kredibilitas pesan. dampak serangan phishing sangat serius: pengguna dapat mengalami penipuan finansial, pencurian identitas, hilangnya akses akun, hingga kerusakan reputasi yang berkepanjangan.

Malware dan Ransomware

5 malware (perangkat lunak berbahaya) merupakan ancaman siber yang dirancang untuk merusak, mengganggu, atau mengakses sistem tanpa izin pengguna. jenis malware yang umum digunakan meliputi trojan, worm, spyware, adware, dan rootkit, yang masing-masing memiliki mekanisme serangan dan dampak yang berbeda terhadap kerahasiaan data pribadi (juliani & hartono, 2025). ransomware merupakan varian malware yang secara khusus mengenkripsi data korban dan meminta tebusan untuk memulihkan akses. ransomware dapat menyebar melalui jaringan dan menginfeksi banyak perangkat sekaligus, sehingga menimbulkan kerugian yang berlipat ganda. dalam konteks institusi publik, serangan ransomware dapat melumpuhkan layanan kritis dan mengekspos data pribadi jutaan pengguna, sebagaimana yang terjadi pada insiden pdn tahun 2024.

Pencurian identitas digital dan kebocoran data

pencurian identitas digital merupakan aktivitas pengambilan dan penyalahgunaan informasi identitas pribadi seseorang tanpa izin, yang bertujuan untuk penipuan finansial, akses ilegal ke akun, atau aktivitas kriminal lainnya. informasi yang menjadi sasaran meliputi nomor identitas (nik), nomor paspor, tanggal lahir, alamat, kata sandi, dan data keuangan. pelaku memperoleh informasi tersebut melalui berbagai sarana, termasuk serangan phishing, malware, pelanggaran basis data, dan eksploitasi celah keamanan sistem. kebocoran data (data breach) berskala besar merupakan manifestasi paling merusak dari ancaman siber terhadap data pribadi. kasus kebocoran 27 juta data anggota bpjs kesehatan pada tahun 2021 dan serangan terhadap pusat data nasional (pdn) pada tahun 2024 menjadi bukti nyata lemahnya tata kelola keamanan siber di institusi publik indonesia. dampaknya mencakup kerugian finansial langsung bagi individu, penyalahgunaan akun, pelanggaran privasi yang mendalam, dan erosi kepercayaan masyarakat terhadap layanan digital pemerintah (unpak, 2026).

Peran keamanan siber dalam perlindungan data pribadi

Dalam menghadapi berbagai ancaman siber yang semakin kompleks, penerapan teknologi keamanan siber menjadi pilar utama perlindungan data pribadi. empat teknologi kunci yang paling banyak diterapkan mencakup firewall, enkripsi, antivirus, dan autentikasi dua faktor.

a. Firewall

Firewall adalah sistem keamanan yang mengontrol aliran data antara jaringan berdasarkan aturan yang telah ditetapkan. dengan memfilter paket data yang masuk dan keluar, firewall dapat mencegah akses tidak sah dari luar jaringan sekaligus menghalangi transmisi data yang mencurigakan dari dalam jaringan. firewall berperan sebagai garis pertahanan pertama yang melindungi infrastruktur digital dari serangan phishing, malware, dan upaya penyusupan lainnya (direktorat jenderal pu, 2024).

b. Enkripsi

Enkripsi merupakan teknologi yang mengubah data menjadi format tidak terbaca tanpa kunci dekripsi yang sesuai, sehingga data tidak dapat diakses oleh pihak yang tidak berwenang. enkripsi diterapkan pada data yang disimpan (data at rest) maupun data yang ditransmisikan (data in transit), memberikan lapisan perlindungan yang esensial terhadap pencurian data dan penyadapan komunikasi. penerapan enkripsi yang konsisten, terutama menggunakan standar modern seperti aes-256, merupakan komponen kritis dalam arsitektur keamanan data pribadi (bssn, 2024).

c. Antivirus dan deteksi ancaman

Perangkat lunak antivirus dirancang untuk mendeteksi, mencegah, dan menghapus malware dari perangkat pengguna. antivirus modern bekerja secara real-time dengan membandingkan file dan aktivitas sistem terhadap basis data ancaman yang terus diperbarui, serta menggunakan analisis perilaku (behavioral analysis) untuk mendeteksi malware baru yang belum dikenal. teknologi ini menjadi komponen esensial dalam perlindungan endpoint, yakni titik akhir jaringan yang paling rentan terhadap infiltrasi malware.

d. autentikasi dua faktor (2fa)

Autentikasi dua faktor (two-factor authentication/2fa) adalah mekanisme verifikasi identitas yang mensyaratkan dua jenis bukti autentikasi yang berbeda: sesuatu yang diketahui pengguna (kata sandi), dan sesuatu yang dimiliki pengguna (kode otp, token fisik, atau biometrik). implementasi 2fa secara signifikan mengurangi risiko pembobolan akun, bahkan ketika kata sandi pengguna telah bocor melalui serangan phishing atau pelanggaran data. adopsi 2fa yang luas di berbagai layanan digital 7 merupakan langkah preventif yang direkomendasikan oleh bssn dan standar keamanan internasional (polteksci, 2025).

e. peran lembaga negara

Selain teknologi, lembaga negara memainkan peran yang tidak kalah penting dalam ekosistem perlindungan data pribadi. badan siber dan sandi negara (bssn) bertanggung jawab atas pengawasan dan koordinasi keamanan siber nasional, pengembangan standar dan kebijakan, serta pemantauan infrastruktur kritis digital.

bssn juga berwenang melakukan audit keamanan siber dan memberikan sertifikasi kepada institusi yang memenuhi standar yang ditetapkan. direktorat tindak pidana siber (*Dittipidsiber*) kepolisian ri bertugas menyelidiki dan menindak kejahatan siber, termasuk kasus phishing dan pelanggaran data pribadi, serta berkoordinasi dengan bssn dalam penanganan insiden. sementara itu, kementerian komunikasi dan informasi berperan dalam pengembangan regulasi dan kebijakan perlindungan data pribadi, termasuk implementasi uu pdp dan koordinasi lintas lembaga (*Dittipidsiber*, 2024).

Tantangan Implementasi Perlindungan Data Pribadi

Meskipun uu pdp telah meletakkan fondasi hukum yang relatif komprehensif, implementasinya di lapangan masih menghadapi empat kategori tantangan yang saling berkaitan. pertama, keterbatasan kapasitas teknis. banyak institusi publik maupun swasta belum memiliki infrastruktur keamanan siber yang memadai untuk memenuhi standar perlindungan data sebagaimana diamanatkan uu pdp. keterbatasan anggaran dan sumber daya manusia yang terampil di bidang keamanan siber memperparah kondisi ini, sehingga risiko pelanggaran data tetap tinggi (uniikom, 2024). kedua, koordinasi kelembagaan yang belum optimal. penanganan ancaman siber memerlukan sinergi antara bssn, *Dittipidsiber*, kementerian komunikasi dan informasi, serta regulator sektoral. namun, tumpang tindih kewenangan dan belum adanya mekanisme koordinasi yang baku menyebabkan respons terhadap insiden keamanan sering tidak efisien dan tidak konsisten. ketiga, rendahnya literasi digital masyarakat. tingkat kesadaran publik tentang pentingnya perlindungan data pribadi masih sangat rendah. banyak pengguna yang tidak 8 menyadari risiko serangan phishing, tidak menerapkan kata sandi yang kuat, atau membagikan informasi pribadi secara sembrono di platform digital. kondisi ini menjadikan pengguna sebagai titik lemah terbesar dalam rantai keamanan siber (balitbangda, 2025). keempat, terbatasnya kapasitas penegakan hukum. meskipun uu pdp menetapkan sanksi yang cukup berat bagi pelanggar, kapasitas aparat penegak hukum dalam mengungkap dan menindak kejahatan siber masih belum sebanding dengan kompleksitas dan volume kasus yang terjadi. investigasi digital membutuhkan keahlian teknis khusus dan perangkat forensik yang belum merata tersedia di seluruh jajaran kepolisian (polteksci, 2025).

Solusi dan rekomendasi

Untuk mengatasi tantangan tersebut, diperlukan pendekatan terpadu yang mencakup penguatan regulasi, peningkatan kapasitas teknis, perbaikan koordinasi kelembagaan, dan intensifikasi edukasi publik. dalam aspek regulasi, pemerintah perlu segera menerbitkan peraturan pelaksana uu pdp yang bersifat teknis dan operasional, membentuk otoritas perlindungan data independen sebagaimana dipraktikkan di uni eropa melalui general data protection regulation (gdpr), serta

memastikan konsistensi penegakan sanksi terhadap pelanggar untuk menciptakan efek jera. dalam aspek teknis, seluruh institusi yang mengelola data pribadi wajib mengimplementasikan standar keamanan minimum yang ditetapkan bssn, meliputi enkripsi data, autentikasi multifaktor, pemantauan sistem secara real-time, dan prosedur respons insiden yang terdokumentasi. investasi dalam infrastruktur keamanan siber perlu diprioritaskan, khususnya pada institusi pemerintah yang menyimpan data pribadi dalam skala besar. dalam aspek koordinasi, perlu dibentuk mekanisme koordinasi lintas lembaga yang terstruktur dan responsif, mencakup pembagian informasi ancaman secara real-time, protokol eskalasi insiden yang jelas, serta pelatihan bersama antara bssn, *Dittipidsiber*, dan regulator sektoral. dalam aspek literasi digital, program edukasi publik tentang keamanan siber perlu diintegrasikan ke dalam kurikulum pendidikan formal di semua jenjang, serta 9 disebarluaskan melalui kampanye media yang masif dan berkelanjutan. fokus edukasi mencakup cara mengenali serangan phishing, pentingnya penggunaan kata sandi yang kuat dan unik, serta hak-hak individu sebagai subjek kesimpulan data sebagaimana dijamin oleh uu pdp (unesco, 2023).

KESIMPULAN

Penelitian ini menyimpulkan bahwa ancaman keamanan siber terhadap data pribadi pengguna di era transformasi digital semakin beragam dan canggih, dengan phishing sebagai ancaman paling dominan, diikuti oleh malware, ransomware, dan pencurian identitas digital. kasus kebocoran data bpjs kesehatan (2021) dan pdn (2024) menjadi bukti nyata lemahnya tata kelola keamanan siber pada institusi publik indonesia. teknologi keamanan siber, yakni firewall, enkripsi, antivirus, dan autentikasi dua faktor, memainkan peran yang sangat penting dalam melindungi data pribadi, didukung oleh peran strategis lembaga negara seperti bssn dan *Dittipidsiber*. meskipun uu pdp nomor 27 tahun 2022 telah memberikan landasan hukum yang komprehensif, implementasinya masih terhambat oleh keterbatasan kapasitas teknis, koordinasi kelembagaan yang belum optimal, rendahnya literasi digital masyarakat, dan terbatasnya kapasitas penegakan hukum. oleh karena itu, diperlukan sinergi kuat antara penguatan regulasi, peningkatan kapasitas teknis institusi, perbaikan koordinasi lintas lembaga, dan intensifikasi edukasi publik untuk mewujudkan perlindungan data pribadi yang efektif, konsisten, dan berkelanjutan di era digital. pemerintah, sektor swasta, dan masyarakat perlu bersama sama membangun ekosistem digital yang aman dan tepercaya sebagai fondasi transformasi digital yang inklusif dan berkeadilan.

DAFTAR PUSTAKA

Appisi, e. (2025). Perlindungan keamanan data pribadi di era digital menghadapi serangan phishing. Ejournal hukum, https://ejournal.appisi.or.id/index.php/hukum/article/view/290 (290), 1–12.

Badan siber dan sandi negara. (2024). Standar keamanan siber untuk infrastruktur kritis digital.

Bappenas. (2025). Transformasi digital indonesia: strategi dan kebijakan. Kementerian ppn/bappenas.

Bssn. Balitbangda, l. (2025). Protecting privacy in the digital era: personal data security in indonesia. Jurnal ilmu pemerintahan https://doi.org/10.35450/jip.v13i1.915 (jip), 13(1), 915–930.

Darul huda, o. (2024). Perlindungan data pribadi di era digital: tantangan dan solusi dalam sistem perbankan.

Digital data protection: global trends and best practices. Oecd publishing. Republik indonesia. (2022). Undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi.

Digital literacy and data protection education in southeast asia. Unesco. Unpak, j. (2026).

Dittipidsiber polri. Juliani, s., & hartono, b. (2025).

Evaluasi kebijakan keamanan siber terhadap privasi data dalam sistem informasi akuntansi digital. International journal of economics, social science (ijess), https://ejournal.pkmpi.org/index.php/ijess/article/view/185 (185), 1–14. Kementerian komunikasi dan informasi. (2023).

Indonesia cybersecurity policy toward data and privacy protection: a structured literature review. Jurnal teknologi dan rekayasa informatika (injuratech), (19664), https://ojs.unikom.ac.id/index.php/injuratech/article/view/19664 1–18. Unesco. (2023).

Jurnal manajemen pelayanan publik (jmp), (13504), 1 20. Https://journal.unpak.ac.id/index.php/jmp/article/view/13504 world bank. (2024). Indonesia digital economy report: security and privacy challenges. World bank.

Media hukum indonesia (mhi), (846), 1–15. Https://ojs.daarulhuda.or.id/index.php/mhi/article/view/846 direktorat jenderal pembangunan infrastruktur, pekerjaan umum. (2024).

Panduan perlindungan data pribadi untuk masyarakat. Kementerian komunikasi dan informasi ri. Oecd. (2023).

Pentingnya keamanan siber dalam era digital https://djps.pu.go.id/storage/bulletins/bulletin-2-filepdf-z9lkn0me.pdf [buletin]. Direktorat tindak pidana siber kepolisian ri. (2024).

Sekretariat negara. 11 polteksci, i. (2025). Personal data protection in the era of digital transformation: challenges and solutions in the indonesian cyber law framework. Indonesian cyber law review (iclr), 2(1), 1–15. Https://doi.org/10.59261/iclr.v2i1.15 uniikom, o. (2024).