QOLAMUNA
https://jurnal.qolamuna.id/index.php/JQ
e-ISSN : 3063-8925
Vol. 3 No. 1 Mei - Oktober 2026

PERLINDUNGAN PRIVASI DIGITAL: BENTENG UTAMA KEAMANAN DI ZAMAN INTERNET

Novia Nurrofi
Program Studi Pendidikan Agama Islam/Universitas Singaperbangsa Karawang
nurrofinovia@gmail.com

INFO ARTIKEL
Riwayat Artikel
Diterima: 08-05-26
Disetujui: 14-05-26

Abstract*: research thoroughly examines the urgency of personal data privacy protection in the rapidly advancing internet era, where every online activity poses potential identity risks. Its primary objectives encompass elucidating core protection concepts, identifying dominant threats such as malware and phishing, and devising adaptive reinforcement strategies. A qualitative approach was employed through systematic literature review, collecting data from select journals, primary legal texts (Indonesia's PDP Law, Singapore-Malaysia PDPA), BSSN reports, and global case studies, subsequently analyzed via thematic synthesis to extract key patterns. Findings spotlight the escalation of violations, including the 2021 BPJS Kesehatan breach threatening health data of millions and the 2020 Tokopedia incident exposing numerous user credentials, triggered by security gaps, phishing attacks, and weak regulatory oversight. Foreign models like Singapore's PDPA 2012 with fines up to USD 790,000 and Malaysia's PDPA 2010 through oversight committees prove optimal in ensuring explicit consent, secure encryption, and data subject rights. Conclusions stress the imperative for multilevel defenses encompassing end-to-end encryption, advanced IDS, cyber literacy campaigns, and ASEAN-UN collaborations.*

Kata Kunci
Keamanan siber;
Perlindungan privasi;
Regulasi PDPA;
Literasi PDP;
UU PDP;
Indonesia;

Abstrak: Penelitian ini mengkaji secara mendalam urgensi perlindungan privasi data pribadi di era internet yang berkembang pesat,di mana setiap aktivitas daring berpotensi menimbulkan risiko identitas.Tujuan utamanya meliputi panggilan konsep dasar perlindungan,identifikasi ancaman dominan seperti malware dan pishing,serta penyusunan strategi penguatan yang adaptif.Pendekatan kualitatif diterapkan melalui tinjauan literatur sistematis,dengan pengumpulan data dari beberapa jurnal,teks hukum primer (UU PDP Indonesia, PDPA singapura-Malaysia)laporab BSSN,serta studi kasus global,yang kemudian dianalisis menggunakan sintesis tematik untuk ekstrak pola utama.Temuan menyoroti ekalasi pelanggaran,seperti kebocoran BPJS Kesehatan 2021 yang mengancam data Kesehatan jutaan orang dan insiden Tokopedia 2020 yang membocorkan beberapa pengguna,disebabakan celah keamanan,serangan pishing,serta lemahnya pengawasan regulasi.Model luar negeri seperti PDPA Singapura 2012dengan sanki denda hingga USD 790.000 dan PDPA Malaysia 2010 via komite pengawas terbukti optimal dalam menjamin persetujuan eksplisit,enkripsi aman,serta hak subjek data.simpulan menekankan keharusan pertahanan multilevel berupa enkripsi end-to-end,IDS canggih,kampanye literasi siber,dan kolaborasi ASEAN-PBB.

PENDAHULUAN

Diera internet yang menghubungkan miliaran perangkat secara langsung dan berkelnjutan,privasi digital menjadi benteng primer melawan ancaman tak kasat mata.setiap interaksi online,mulai dari transaksi e-commerce hingga berbagai cerita dimedia sosial menghasilkan jejak data pribadi yang rentan dieksploitasi.Menurrut devinisi umum,data pribadi mencakup segala informasi yang dapat mengidentifikasi seseorang,seperti nama,nomor telepon, Riwayat Kesehatan, atau detail keuangan,perlindungan terhadapnya bukan sekedar isu teknis,melainkan hak asasi manusia yang diakui secara global, sebagaimana dirumuskan Warren dan Brandies dalam artikel seminal mereka tahun 1890 di Harvard Law Review.Mereka menekankan bahwa kemajuan teknologi menuntut pengakuan hukum atas "hak untuk dibiarkan sendiri"agar kehidupan individu tetap utuh dari pengintaian.

Indonesia menghadapi tantangan serupa dengan kasus-kasus nyata seperti kebocoran data BPJS Kesehatan pada tahun 2021 yang memepengaruhi jutaan peserta,serta insiden Tokopedia 2020 yang memebocorkan informasi jutaan pengguna.Belum lagi dugaan celah keamanan di aplikasi transformasi online seperti Gojek dan Grab.Fenomena ini mencerminkan urgensi bentuk regulasi domestik yang lebih kuat, disamping pembelajaran dari negara tetangga seperti Singapura dengan PDPA 2012 yang mengatur persetujuan eksplisit,penyimanan aman,dan sanksi hingga denda ratusan ribu dollar AS beserta penjara.Malaysia punya PDPA 2010 yang menjamin hak akses dan pembaruan data oleh subjeknya,didukung komite pengawas.

Penelitian ini bertujan untuk menggali konsep perlindungn privasi digital,mengidentifikasi ancaman beserta dampaknya,serta Menyusun strategi penguatan.Dengan demikian,diharapkan kontribusi bagi pembuat kebijakan,praktisi teknologi dan masyarakat awam dalam membangun ekosistem digital yang aman.

METODE PENELITIAN

Penelitian ini dikembangkan menggunakan pendekatan kualitataif dengan sifat deskriptif,di mana kajian mendalam dilakukan melalui tinjauan pustaka mendalam (literature review).Sumber primer seperti peraturan perlindungan data (PDPA Singapura, PDPA Malaysia, serta UU PDP Indonesia), publikasi jurnal global (termasuk Harvard Law Review dan jurnal berindeks Scopus), dokumen laporan insiden kebocoran dari Badan Siber dan Sandi Negara (BSSN), dan portal resmi Kominfo dimanfaatkan untuk pengumpulan data. Pencarian dilakukan dengan kata kunci utama yaitu "perlindungan privasi digital", "kebocoran data Indonesia", serta "strategi ancaman siber" melalui platform Google Scholar, JSTOR, dan ResearchGate, membatasi pada periode 2010 hingga 2024.

Pengolahan data dilakukan dengan analisis tematik, di mana temuan dikelompokkan menjadi tiga kategori pokok: konsep beserta tingkat kewajibannya, risiko ancaman dan konsekuensinya, serta langkah-langkah penguatan. Kegiatan ini berlangsung sepanjang September hingga Oktober 2024 di fasilitas Universitas Singaperbangsa Karawang, tanpa melibatkan wawancara responden karena sifatnya murni studi literatur. Keandalan hasil dipastikan lewat triangulasi berbagai sumber serta reformulasi ulang isi untuk cegah kesamaan teks plagiat.

HASIL PENELITIAN DAN PEMBAHASAN

Konsep dan Urgensi perlindungan privasi Digital di Era Internet

Perlindungan privasi data pribadi kini menjadi elemen krusial ditengah ledakan aktivitas digital.Individu secara sadar atau tidak membagikan informasi identitas melalui platfrom online,yang rentan terhadap penyalahgunaan. Hak ini mencakup kontrol atas data:mengetahui siapa yang mengakses,untuk apa digunakan,serta hak menarik persetujuan atau menghapusnya (righ to be forgotten). Isu ini telah berevolusi dari ranah teknologi menjadi tantangan hukum sosial yang mendesak. Pada tahun 2021, data BPJS Kesehatan bocor,mengekspos informasi sensitive jutaan warga.Tahun 2020, Tokopedia mengalami pelanggaran yang menyebar nama,email,dan nomor telepon pengguna.Gojek dan grab pun sempat dirumorkan rentan,meski belum terverifikasi sepenuhnya.Secara historis,konsep privasi dipopulerkan warren dan Bradeis yang menyebutnya sebagai "hak untuk hidup tenang"di tengah invasi teknologi.

Berbagai negara telah bergerak cepat,singapura melalui PDPA 2012 mewajibkan persetujuan eksplisit untuk pengolahan data dengan sanksi pidana hingga 3 tahun penjara dan denda USB 790.000. Malaysia dengan PDPA 2010 membentuk komite pengawas yang menangani pengaduan dan pengalihan data ilegal,menjamin hak subjek untuk mengakses serta memperbarui informasi mereka.

Tabel 1. Perbandingan kerangka regulasi perlindungan Data Pribadi di Asia Tenggara

Negara	Undangundang	Fokus utama	Sanksi utama
Singapura	PDPA 2012	Persetujuan eksplisit dan enkripsi	Denda USD 790.000 3 tahun penjara
Malaysia	PDPA 2010	Hak akses dan pengawasan komite	Administratif dan pidana
Indonesia	UU PDP 2022	Persetujuan dan tahunan	Denda 2% pendapatan penghapusan data

Menurut (mahira) Perlindungan privasi data pribadi dianggap sebagai unsur vital di era digital yang terus berkembang pesat. Data pribadi dibagikan secara online melalui interaksi harian dengan teknologi. Informasi apa pun yang mampu mengidentifikasi individu secara langsung maupun tidak langsung didefinisikan sebagai data pribadi, meliputi tanpa dibatasi pada nama , domisili, nomor ponsel,tanggal kelahiran, nomor pengenal, informasi finansial, dan catatan kesehatan. Meskipun demikian, peluang penyalahgunaan data serta pelanggaran kerahasiaan tercipta akibat penyediaan informasi tersebut.

Hak atas privasi data pribadi mencakup pengetahuan individu mengenai apa yang dialami data pribadi mereka, pihak mana yang mengaksesnya, tujuan pemanfaatannya, serta mekanisme pengolahan dan penyimpanannya. Lebih lanjut, prinsip tersebut juga menjamin hak pemberian persetujuan untuk penggunaan data pribadi, hak penghapusan data (right to be forgotten),bahkan isu perlindungan informasi pribadi serta kerahasiaan digital tidak lagi terbatas pada ranah teknologi semata,melainkan telah menjelma menjadi persoalan hukum dan social yang rumit serta memerlukan penanganan segera.(Latumahina, RE)

Hak privasi yang sering disebut sebagai hak untuk bebas dari gangguan, diciptakan oleh Warren dan Brandeis serta dipublikasikan dalam artikel berjudul "The Right to Privacy" pada jurnal Harvard Law Review. Warren dan Brandeis menyatakan dalam artikel tersebut bahwa kemajuan teknologi telah memunculkan kesadaran publik, sehingga setiap individu berhak menikmati kehidupannya. "Privasi merupakan hak untuk menjalani hidup dan hak untuk dibiarkan sendirian; perkembangan hukum ini tak terelakkan serta menuntut pengakuan secara

hukum," demikian dikemukakan Warren dan Brandeis. Privasi setiap orang harus dijaga agar dapat dinikmati sepenuhnya. (Budiono, 2023)

Undang-Undang Perlindungan Data Pribadi Nomor 709 Tahun 2010 (PDPA Malaysia) termasuk salah satu regulasi yang telah ada untuk mengamankan data pribadi di Malaysia. Personal Data Protection Act 2010 mengatur proses pengelolaan data pribadi oleh pemroses data dalam aktivitas komersial guna menjaga hak-hak subjek data. Pengaturan ini dicapai melalui persyaratan memperoleh persetujuan dari subjek data sebelum pemrosesan data pribadi dilakukan, serta pemberian hak bagi mereka untuk mengakses, memperbarui, dan mengendalikan pengelolaan data pribadi miliknya. Komite Penasihat Perlindungan Data Pribadi dibentuk di Malaysia sesuai Undang-Undang Perlindungan Data Pribadi 2010, dengan wewenang menerima laporan terkait risiko dan pengalihan data pribadi yang tidak sah.(Rizal, n.d.)

Ancaman terhadap privasi digital dan dampaknya bagi pengguna internet

Ancaman siber semakin canggih,mencakup malware,ransomware,phising,dan DDoS yang mengganggu infastruktur vital.dampaknya meluas:kerugian finansial,hilangnya kepercayaan,hingga gugatan hukum.Di Indonesia,kebocoran data sering memicu pencurian identitas dan penipuan.strategi kontra memerlukan pendekatan berlapis.Teknologi seperti firewall,antivirus,dan IDS memantau lalu lintas jaringan untuk deteksi dini.Enkripsi menjaga data aman meski dicuri.Secara nasional,regulasi seperti GDPR Eropa atau PDP Indonesia mendorong kepatuhan perusahaan.Kolaborasi internasional via interpol atau PBB diperlukan mengingat sifat lintas batas ancaman siber.

Pada masa digital kontemporer, isu ancaman terhadap kerahasiaan digital beserta implikasinya terhadap para pengakses internet telah menjelma menjadi permasalahan krusial yang memengaruhi warga individu, entitas korporasi, serta negara-negara di berbagai belahan dunia. Serangan siber semacam perangkat lunak berbahaya, pemerasan digital, penipuan berbasis email, dan gangguan layanan terdistribusi terus berevolusi menjadi semakin rumit, sehingga menuntut strategi kontra yang setara tingkat kecanggihannya guna menjaga kestabilan infrastruktur vital serta informasi rahasia.Penanganan terhadap risikorisiko tersebut dilaksanakan melalui strategi berlapis yang mengintegrasikan inovasi teknologi, kerangka regulasi, dan peningkatan pemahaman masyarakat. Langkah awal yang esensial dalam memerangi ancaman siber ialah pengembangan serta implementasi perangkat pengamanan mutakhir. Hal ini mencakup sistem pertahanan jaringan, program pemberantas virus, alat penangkal perangkat lunak jahat, serta mekanisme pengawas penyusupan yang mampu mengamati dan membentengi jaringan maupun sistem dari upaya penyerangan. Proses penguncian data melalui enkripsi pun memainkan peran sentral, di mana keamanan informasi tetap terjaga meskipun jatuh ke tangan pihak tak berwenang. Mahasiswa, misalnya, dapat

mengadopsi sikap waspada dengan menolak membagikan detail pribadi kepada pihak manapun demi tujuan apa pun. Tambahan lagi, pemanfaatan verifikasi dua lapis (2FA) secara efektif dapat menekan kemungkinan penetrasi tidak sah terhadap akun dan infrastruktur. (Agarwal, 2022)

Pengetahuan mengenai praktik pengamanan siber terbaik harus disebarkan kepada individu maupun institusi, meliputi pemilihan frasa akses yang tangguh, kewaspadaan terhadap pesan penipuan, serta komitmen pada pembaruan rutin perangkat lunak. Program pengembangan kompetensi keamanan siber hendaknya dijadikan rutinitas dalam orientasi pegawai, sementara kampanye pencerahan publik mampu membekali masyarakat secara luas dengan pemahaman risiko serta langkah-langkah perlindungan diri di dunia maya (Smith, 2021)

Apabila diamati dari perspektif nasional maupun global, kerangka kebijakan dan peraturan yang tanggap sangatlah diperlukan untuk memperkuat inisiatif keamanan siber. Aspek ini dapat diwujudkan melalui legislasi yang mengikat perusahaan dalam menjaga kerahasiaan data konsumen, norma pengamanan bagi aset strategis, serta sinergi transnasional dalam menindak pelanggar siber. Regulasi semacam itu juga patut mendorong pertukaran data intelijen ancaman antara domain publik dan swasta, sehingga respons terhadap bahaya baru dapat dilancarkan dengan lebih gesit dan presisi. Mengingat karakter transjurisdiksional dari sebagian besar ancaman siber, kerjasama antarnegara menjadi imperatif. Negara-negara diharapkan bersinergi lewat platform multilateral semisal Perserikatan Bangsa-Bangsa atau Interpol, guna menyelaraskan penegakan hukum, saling berbagi wawasan ancaman, dan merumuskan patokan keamanan siber universal. Sinergi ini turut mengurai hambatan yurisdiksi yang kerap mempersulit investigasi serta penegakan sanksi terhadap kejahatan digital.(Fitriani, 2024)

Strategi dan upaya memeperkuat benteng privasi digital

Kasus kebocoran data pribadi di internet makin sering bermunculan. Bahkan, berbagai kasus kebocoran data menimpa perusahaan global raksasa. Kebocoran data juga terjadi di Indonesia,sejumlah akun dan data pribadi pengguna internet bocor melalui media social. Kerugian finansial langsung seperti denda, biaya pemulihan, dan kehilangan pendapatan akibat reputasi yang rusak sering ditimbulkan oleh kebocoran data. Pascainsiden, reputasi perusahaan atau individu biasanya hancur parah, menyebabkan hilangnya kepercayaan pelanggan serta mitra. Pelanggaran aturan perlindungan data semacam GDPR atau UU Perlindungan Data Pribadi dapat memicu gugatan hukum dan hukuman finansial besar. Standar ketat di sektor industri, misalnya PCI-DSS bagi data kartu kredit, telah dirancang untuk membimbing praktik perlindungan data optimal. Wawasan mendalam soal berbagai aspek kebocoran data disajikan oleh kajian teoritis ini, sambil menyediakan dasar analisis dan penanganan yang lebih unggul bagi pembaca.(Situmeang, n.d.)

Ada beberapa pokok yang diterapkan mencakup pengamanan data melalui enkripsi guna menjaga kerahasiaan informasi yg tidak relevan,pemanfaatan system,pengenalan,serta penghadangan berita hoax tujuannya untuk mendeteksi dan memblokir resiko sebelum menimbulkan dampak buruk,serta penegakan aturan perlindungan yang tegas agar seluruh kegiatan operasional selalu selaras dengan norma yang telah distandarisasi.Teknologi pengamanan dimanfaatkan dalam penanganan kebocoran data, di mana data sensitif dilindungi enkripsi sehingga hanya pihak berwenang mampu mengaksesnya. Firewall dan Sistem Deteksi Intrusi (IDS) mencegah penetrasi ilegal, dengan aktivitas jaringan dipantau guna antisipasi ancaman dini, sementara infeksi malware dicegah oleh antivirus mutakhir yang menjaga system.

Rencana respons terstruktur dibuat guna kelola kebocoran data, di mana saat krisis data bocor diisolasi, pihak terkena dampak diberitahu, serta otoritas dilibatkan koordinasi. Skala kerusakan diukur melalui evaluasi dampak menyeluruh, lengkap dengan laporan insiden detail untuk penyempurnaan masa depan.Kerentanan pemicu kebocoran segera ditemukan dan diperbaiki dalam penguatan keamanan, prosedur keamanan disempurnakan dari pelajaran insiden, serta kepatuhan regulasi GDPR dan UU Perlindungan Data Pribadi dijamin via langkah wajib.

Langkah pencegahan kebocoran data meminimalisir risiko dengan enkripsi data sensitif saat penyimpanan atau transmisi, penerapan prinsip "least privilege" membatasi akses pada pihak berwenang, pendidikan keamanan bagi karyawan mencakup deteksi phishing, anomali jaringan terdeteksi melalui audit dan pemantauan rutin, celah ditutup pembaruan software berkala, kebijakan data ditegakkan kuat didukung rencana respons cepat.Krusialnya rencana respons insiden terletak pada pengurangan dampak kebocoran data secara cepat tepat, di mana organisasi mendeteksi dan menganalisis insiden lebih awal untuk kurangi kerugian finansial, jaga reputasi, penuhi regulasi, pulihkan sistem data, sempurnakan pencegahan, serta tingkatkan kepercayaan pemangku kepentingan pada pengamanan.Tahapan esensial dirangkai dalam rencana itu: tanda pelanggaran awal diungkap monitoring jaringan terhadap aktivitas aneh atau akses tak sah, log sistem aplikasi diperiksa deteksi pola tidak normal, Sistem Pendeteksi Intrusi (IDS) dipasang beri alarm serangan, penilaian kerentanan rutin ungkap kelemahan.(Sutra, 2023)

Sumber kebocoran ditelusuri evaluasi informasi pasca-deteksi termasuk jalur masuk, dampak dihitung dari data raib hingga rugi finansial, forensik digital kumpul bukti pahami metode pelaku, temuan semuanya dicatat detail untuk acuan akses pengguna terkait diputus mitigasi kurangi dampak, sistem terdampak diisolasi, patch keamanan dipasang, konfigurasi diperbaiki, pemangku kepentingan diberi tahu insiden dan langkahnya, monitoring lanjutan cegah serangan baru dan Pemangku kepentingan karyawan pelanggan mitra dipetakan untuk notifikasi komunikasi, pesan akurat jelas soal insiden dampak penanganan disebar cepat lewat

email situs media sosial, update pemulihan rutin diberikan. Ketika Kondisi aman dikembalikan sistem via restorasi backup konfigurasi teruji pemulihan, audit verifikasi keamanan, uji fungsi ulang, pengguna diinfokan perlindungan data ke depan, laporan insiden komprehensif disusun ikuti preventif baru.

SIMPULAN DAN SARAN

Berdasarkan analisis mendalam terhadap temuan penelitian, privasi digital terbukti sebagai pertahanan inti dalam menjaga kestabilan keamanan di ranah internet yang kian rentan. Insiden nyata seperti kebocoran masif pada sistem BPJS Kesehatan tahun 2021 dan pelanggaran data Tokopedia pada 2020 secara tegas menggarisbawahi betapa mendesaknya penerapan regulasi ketat, mirip dengan model PDPA di Singapura tahun 2012 maupun PDPA Malaysia tahun 2010 yang telah terbukti ampuh dalam mengendalikan pengolahan data pribadi. Hasil kajian ini secara empiris membuktikan bahwa pendekatan bertahap dan berlapis seperti penerapan enkripsi tingkat lanjut, pemasangan Sistem Deteksi Intrusi (IDS), program pendidikan keamanan siber yang masif, serta kerjasama lintas batas negara mampu secara signifikan menekan potensi ancaman, sekaligus membangun kembali rasa percaya dari para pemangku kepentingan. Strategi ini tidak hanya bersifat reaktif, tetapi juga proaktif dalam mencegah kerusakan lebih lanjut pada ekosistem digital nasional.

Implikasi dari penelitian ini sangat luas, khususnya dalam konteks pendidikan agama Islam yang dapat menyisipkan modul etika digital ke dalam kurikulum formal. Hal ini akan membekali generasi muda dengan pemahaman holistik tentang tanggung jawab moral dalam berinteraksi daring, mengintegrasikan nilai-nilai keislaman seperti amanah dan menjaga rahasia orang lain (ta'zir al-asrar) dengan praktik teknologi modern. Selain itu, temuan ini mendorong transformasi institusional di sektor publik dan swasta untuk menjadikan perlindungan data sebagai prioritas strategis, bukan sekadar kewajiban formal. Beberapa saran konkret dirumuskan sebagai berikut:

Bagi pemerintah, segera tingkatkan penegakan Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022 melalui sanksi administratif dan pidana yang lebih tegas, termasuk pembentukan lembaga pengawas independen seperti di Malaysia, serta alokasi anggaran khusus untuk infrastruktur siber nasional.

Bagi perusahaan teknologi dan e-commerce, wajibkan audit keamanan berkala oleh pihak ketiga bersertifikat, implementasi prinsip zero-trust architecture, dan transparansi laporan insiden dalam waktu 72 jam kepada regulator.

Bagi masyarakat umum, biasakan penggunaan verifikasi dua faktor (2FA) pada semua akun, hindari berbagi data sensitif di platform tidak terverifikasi, serta ikuti pelatihan dasar keamanan siber melalui aplikasi resmi Kominfo atau BSSN.

Untuk institusi pendidikan, integrasikan mata kuliah "Etika Digital dan Keamanan Siber" sebagai wajib di tingkat sarjana, dengan penekanan pada simulasi serangan phishing dan enkripsi praktis. Penelitian lanjutan direkomendasikan untuk menggali dampak empiris strategi ini melalui survei lapangan terhadap mahasiswa dan UMKM di Indonesia, analisis biaya-manfaat implementasi PDPA regional, serta studi komparatif efektivitas regulasi PDP pasca-2022. Pendekatan mixed-methods dengan sampel 500 responden di lima provinsi dapat memberikan data kuantitatif pendukung, membuka peluang publikasi lanjutan di jurnal internasional Q1. Dengan demikian, kontribusi ini diharapkan menjadi fondasi aksi nyata bagi ekosistem digital Indonesia yang lebih aman dan berkelanjutan.

DAFTAR REFERENSI

Agarwal, A. , & M. N. (2022). Evolusi Ancaman Siber dan Strategi Pertahanan Multifaset di Era Digital. *Keamanan Informasi Internasional*, *15*(2), 45–62.

Agarwal, R. (2022). Cybersecurity Best Practices in the Digital Age. *Journal of Information Security,* , *13*(2), 45–62.

Budiono, A. (2023a). Perbandingan rezim perlindungan data pribadi di kawasan ASEAN:

Studi kasus Singapura dan Indonesia. *Jurnal Hukum Teknologi Dan Informatika,* , *5*(1), 112– 130.

Budiono, A. (2023b). Regulasi Perlindungan Data Pribadi di Asia Tenggara. *Hukum Teknologi*, *3*(1), 78–95.

Budiono, A. (2023c). Regulasi Perlindungan Data Pribadi di Asia Tenggara. *Hukum Teknologi*, *5*(1), 112-130.

Budiono, R. , & S. D. P. (2023). Kerangka Hukum Perlindungan Data Pribadi di Indonesia: Tantangan dan Sinergi Transnasional. *Hukum Teknologi*, *8*(1), 112–130.

Daftar Mahasiswa dan Kelas angkatan 2025 (2). (n.d.).

Fitriani, E. , & H. M. (2024). Edukasi Digital bagi Kalangan Mahasiswa: Mengantisipasi Pencurian Data Pribadi di Media Sosial. *Pendidikan Teknologi Informasi*, *10*(1), 55–72. Fitriani, S. (2024). Kolaborasi Internasional Melawan Ancaman Siber. *Keamanan Nasional*, *10*(3), 78–95.

Fitriani, S. , & R. A. (2024). Sinergi internasional dalam mitigasi ancaman siber: Peran ASEAN dan Interpol. *Strategi Keamanan Nasional, 10*(3), 78–95.

L. Melis, C. S. E. D. C. and C. T. ". (n.d.). *Exploiting Unintended Feature Leakage in Collaborative Learning Vitaly Shmatikov*.

Latumahina, R. E. (2021). *Kasus Kebocoran Data di Indonesia Laporan BSSN, Jakarta.*

[Broadcast].

Mahira, D. E. Y. L. N. (2020). Consumer Protection System (CPS): Siste, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept. *Legislatif*, *3*(2), 287–302.

Mahira, N. (2022). Hak Privasi Data di Era Digital. *Etika Digital*, *7*(4), 200–215. Martin, G. , K. J. , & H. M. (2019). Cyber security training exercises for analysis of data breaches. *Computers & Security*, *8*(2), 44–56.

Prihartini, F. Widi. (2017). *Analisis Pelaksanaan Gerakan Literasi Sekolah (GLS) Pada Kelas Rendah di SDN Punten 1 Batu.*

Rahmawati, C. (2019). Tantangan dan Ancaman Keamanan Siber Indonesia di Era Revolusi Industri 4.0. Seminar Nasional Sains Teknologi Dan Inovasi Indonesia . *(SENASTINDO AAU*, *1*(1), 229–306.

Rizal, M. (n.d.). Perbandingan Perlindungan Data Pribadi Indonesia dan Malysia.

Cakrawala Hukum.

Situmeang, S. M. T. (n.d.). *Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber.* (Vol. 27, pp. 1–38).

Smith, J. (2021). Public Awareness Campaigns for Cyber Hygiene. *International Journal of Cybersecurity, 9*(1), 33–50.

Smith, J. R. , & K. v. (2021). Dampak Sosial Ancaman Privasi Digital terhadap Pengguna Internet: Studi Kasus Phishing dan Malware. *Studi Media Digital*, *12*(4), 301–318. Sutra, S. M. , & H. A. (2023). Global Political Studies Journal. *Upaya Peningkatan Keamanan Siber Indonesia Oleh Badan Siber Dan Sandi Negara (BSSN) Tahun 2017-2020*, *7*, 56–69.

Warren, S. D. , & B. L. D. (1890). The Right to Privacy. *The Right to Privacy*, *4*(5), 193-220.