EKOMA : Jurnal Ekonomi, Manajemen, Akuntansi
Vol.4, No.6, September 2025

Strategi Penguatan Keamanan Informasi Digital dalam Menghadapi Ancaman Siber: Studi Kasus Kementrian Kominfo

Hilma Harmen[1], Afifah Nida Suhaila Boru Dalimunthe[2], Desi Irawan Lestari[3], Fikri Al Kautsar[4], Jekson Sihombing[5], Tasya Chintain Boru Simanjuntak[6], Miftahuss'aidah[7]
[1,2,3,4,5,6,7] Manajemen, Fakultas Ekonomi, Universitas Negeri Medan, Indonesia
E-mail: E-mail: hilmaharmen@unimed.ac.id[1], afifahsuhailah29@gmail.com[2], desiirawan2005@gmail.com[3], fikrialkautsar2704@gmail.com[4], jeksons21@gmail.com[5], tasyachintainss@gmail.com [6],miftahussaidah72@gmail.com[7]

Article History:
Received: 22 Mei 2025
Revised: 01 Agustus 2025
Accepted: 21 Agustus 2025

Keywords: *keamanan informasi digital, ancaman siber, Kominfo.*

Abstrak: *Penelitian ini menganalisis strategi penguatan keamanan informasi digital di Indonesia dalam menghadapi ancaman siber, dengan fokus pada peran Kementerian Komunikasi dan Informatika (Kominfo). Metode kualitatif digunakan untuk menelaah literatur dan kebijakan terkait. Hasil penelitian menunjukkan bahwa penguatan keamanan informasi dilakukan melalui empat pendekatan utama: regulasi dan kebijakan, pengembangan sumber daya manusia, implementasi teknologi keamanan, dan edukasi publik. Strategi ini penting untuk menjaga kedaulatan digital serta membangun ekosistem digital yang aman dan terpercaya di Indonesia.)*

PENDAHULUAN

Era digital telah mengubah secara signifikan hampir semua aspek kehidupan di Indonesia. Perubahan ini tampak melalui metode komunikasi individu, cara organisasi mengelola operasional, sampai pergeseran perekonomian nasional ke arah ekonomi digital. Pemakaian teknologi informasi dan komunikasi (TIK) yang semakin berkembang telah mendorong proses digitalisasi dalam berbagai bidang, menjadikan Indonesia sebagai salah satu negara dengan pertumbuhan ekonomi digital tercepat secara global (Wahidin & Wati, 2024). Akan tetapi, perkembangan ini juga disertai oleh bertambahnya risiko dan kompleksitas ancaman siber, seperti peretasan, malware, pencurian data, dan serangan siber terencana yang menargetkan individu, perusahaan, serta institusi pemerintah (Alfi et al., 2023).

Data terbaru menunjukkan bahwa selama kuartal pertama tahun 2024, Indonesia mengalami hampir 6 juta serangan siber, yang menandakan tingginya tingkat risiko di ruang digital nasional. Ancaman-ancaman ini tidak hanya memengaruhi aspek teknis, tetapi juga dapat mengganggu stabilitas sosial, perekonomian, dan politik, serta mengurangi kepercayaan publik terhadap sistem digital yang ada. Serangan seperti phishing, serangan Denial of Service Terdistribusi (DDoS), ransomware, dan kebocoran informasi saat ini menjadi tantangan nyata yang harus dihadapi untuk memastikan kelangsungan transformasi digital nasional (Ananta et al., 2024).

Dalam situasi ini, Kementerian Komunikasi dan Informatika (Kominfo) memainkan peran penting sebagai penggerak utama kebijakan keamanan informasi digital di Indonesia. Kominfo memiliki tugas menyusun regulasi, membangun infrastruktur keamanan siber, dan meningkatkan kesadaran serta kapasitas sumber daya manusia (SDM) di sektor keamanan informasi (Rai et al.,

2022). Salah satu serangan siber yang dapat kita ketahui sekarang adalah pembobolan system QRIS.

Menurut (Zulkarnaen et al., 2024) pembobolan QRIS (Quick Response Code Indonesian Standard) menjadi perhatian serius seiring dengan meningkatnya penggunaan pembayaran digital di Indonesia. Studi kasus nyata, seperti nasabah BCA yang kehilangan Rp68,5 juta melalui transaksi QRIS tanpa otorisasi, mengindikasikan kerentanan sistem meskipun standar keamanan telah diterapkan. Penelitian terbaru menunjukkan bahwa 44,2% kepuasan pengguna QRIS dipengaruhi oleh faktor keamanan aplikasi dan teknologi informasi

Di samping itu, Kominfo juga berfungsi sebagai jembatan antara instansi pemerintah dan sektor swasta dalam membangun ekosistem keamanan siber yang tangguh serta responsif terhadap perubahan ancaman yang selalu muncul. Usaha untuk meningkatkan keamanan informasi digital tidak bisa dilakukan secara terpisah atau terbatas pada satu sektor.

Dibutuhkan pendekatan nasional yang menyeluruh, mencakup pembuatan regulasi yang jelas, pengembangan kompetensi sumber daya manusia, perlindungan infrastruktur vital nasional, serta kolaborasi antar sektor dan internasional. Pembentukan lembaga seperti Badan Siber dan Sandi Negara (BSSN) adalah langkah krusial dalam menggabungkan usaha pertahanan siber nasional, termasuk perbaikan deteksi ancaman, penanganan insiden, serta pencegahan kebocoran data (Santoso et al., 2024).

Selain aspek teknis dan regulasi, pendidikan serta pengetahuan keamanan siber bagi masyarakat menjadi fokus utama. Program pendidikan, pelatihan, dan penyuluhan yang berkelanjutan sangat penting agar masyarakat dapat mengidentifikasi dan merespon berbagai ancaman siber yang ada. Kominfo secara proaktif melaksanakan pengawasan, pendidikan, dan penegakan peraturan, termasuk dalam perlindungan data pribadi serta penanganan insiden kebocoran data (Surbakti, 2024).

Oleh karena itu, penguatan perlindungan informasi digital menjadi kebutuhan yang mendesak untuk ditanggapi secara terpadu dan kolaboratif. Dengan penerapan strategi yang sesuai dan kolaborasi antara pemerintah, sektor swasta, serta masyarakat, diharapkan Indonesia dapat membangun ekosistem digital yang aman, terpercaya, serta mendukung pertumbuhan ekonomi digital yang inklusif dan kompetitif di skala global (Budiyanto & Mabruri, 2025).

LANDASAN TEORI

Pentingnya Penguatan Keamanan Siber dan Talenta Digital

Perkembangan teknologi digital yang pesat membawa dampak signifikan terhadap berbagai aspek kehidupan, mulai dari sektor pemerintahan, bisnis, hingga kehidupan masyarakat sehari-hari. Namun, kemajuan ini juga diiringi dengan meningkatnya ancaman siber yang semakin kompleks dan masif. Oleh karena itu, penguatan keamanan siber dan pengembangan talenta digital menjadi sangat krusial untuk menjaga stabilitas, pertumbuhan ekonomi, serta kedaulatan nasional (Raffi Nur Rizky et al., 2024).

Keamanan siber merupakan upaya sistematis untuk melindungi sistem, jaringan, dan data dari ancaman digital seperti peretasan, malware, dan pencurian data. Pentingnya keamanan siber sejalan dengan tingkat ketergantungan masyarakat dan organisasi terhadap teknologi digital. Tanpa sistem keamanan yang kuat, kerugian yang ditimbulkan dari serangan siber tidak hanya bersifat finansial, tetapi juga dapat mengancam keberlangsungan bisnis, reputasi, bahkan keamanan nasional (Budi et al., 2021a).

Penguatan keamanan siber tidak hanya berfokus pada perangkat keras dan perangkat lunak, tetapi juga pada pembangunan sumber daya manusia (SDM) yang kompeten. Kompetensi SDM dalam

keamanan siber meliputi pemahaman prosedur keamanan, kemampuan menggunakan perangkat keamanan, serta keterampilan dalam merespons insiden siber secara cepat dan tepat (Febrian Aska et al., 2024).

Transformasi digital di berbagai sektor menuntut ketersediaan talenta digital yang mumpuni. Talenta digital di bidang keamanan siber sangat dibutuhkan untuk mengidentifikasi, mencegah, dan menanggulangi serangan siber yang semakin canggih. Keterbatasan talenta digital menjadi salah satu tantangan utama dalam implementasi strategi keamanan siber nasional (Adma et al., 2023).

Pengembangan talenta digital dilakukan melalui berbagai program pelatihan, beasiswa, dan kolaborasi dengan perusahaan teknologi global. Pemerintah Indonesia, misalnya, telah bekerja sama dengan perusahaan seperti Google dan Microsoft untuk melahirkan puluhan ribu talenta digital yang berkontribusi di sektor keamanan siber. Selain itu, pemanfaatan teknologi seperti kecerdasan buatan (AI) dalam pelatihan juga dapat meningkatkan efektivitas pengembangan kompetensi SDM (Febrian Aska et al., 2024).

Regulasi dan Kebijakan Perlindungan Data Pribadi

Hak atas privasi merupakan bagian fundamental dari hak asasi manusia yang menjadi dasar hukum perlindungan data pribadi. Dalam Pasal 28G UUD 1945, hak atas privasi diatur sebagai hak konstitusional warga negara Indonesia. Perlindungan data pribadi merupakan manifestasi dari perlindungan hak atas privasi tersebut, yang memberikan hak kepada individu untuk mengetahui, mengakses, memperbaiki, dan menghapus data pribadinya sesuai dengan ketentuan hukum yang berlaku (Deannova Saputra et al., 2024).

Perlindungan data pribadi juga dapat dilihat dari perspektif hukum ITE dan hukum perdata, khususnya terkait perbuatan melawan hukum (PMH).

Revolusi digital membawa kemudahan sekaligus risiko penyalahgunaan data pribadi secara masif. Oleh karena itu, UU PDP yang telah disahkan menjadi instrumen hukum penting untuk mengatur pengumpulan, penyimpanan, dan pemanfaatan data pribadi secara legal dan bertanggung jawab. Regulasi ini juga menegaskan hak subjek data dan kewajiban pengendali data, serta memberikan dasar hukum bagi penyelesaian sengketa yang timbul akibat pelanggaran data (Fikri & Rusdiana, 2023).

Dalam konteks media sosial, perlindungan data pribadi melibatkan berbagai aktor seperti prosesor data, pengendali data, dan subjek data. UU PDP mengatur secara rinci hak dan kewajiban para pihak ini, termasuk mekanisme pengolahan dan penanganan data pribadi. Politik hukum pengaturan ini menunjukkan peran aktif pemerintah dalam mengatur, menyimpan, mengolah, dan melindungi data pribadi secara preventif dan represif guna menanggulangi penyalahgunaan data di era digital (Arham & Risal, 2023).

Banyak kasus kebocoran dan penyalahgunaan data pribadi yang terjadi di Indonesia menegaskan urgensi pengesahan UU Perlindungan Data Pribadi. Penelitian yuridis normatif menegaskan bahwa perlindungan data pribadi saat ini belum berjalan optimal, sehingga pengesahan UU PDP diharapkan menjadi bentuk perlindungan negara terhadap hak atas privasi masyarakat. UU ini juga menjadi jawaban atas kebutuhan perlindungan keamanan data pribadi sebagai hak fundamental warga negara (Lesmana et al., 2021).

Kasus pembocoran data pribadi yang marak terjadi akibat kemajuan teknologi menimbulkan tantangan besar bagi perlindungan data. Penelitian normatif dengan studi kasus menyoroti pentingnya UU No.27 Tahun 2022 sebagai instrumen hukum yang menjamin keamanan data pribadi dan hak atas privasi masyarakat Indonesia. Meskipun demikian, implementasi perlindungan data pribadi masih belum optimal dan memerlukan pengawasan serta penegakan hukum yang lebih ketat (Saly et al., 2023a).

Strategi Implementasi dan Pengelolaan Keamanan Informasi

Strategi implementasi dan pengelolaan keamanan informasi merupakan suatu proses sistematis yang bertujuan untuk melindungi aset informasi organisasi dari ancaman dengan menggunakan kebijakan, prosedur, dan teknologi yang tepat (Aurabillah et al., 2024). Dalam hal ini, kita dapat menerapkan Sistem Manajemen Keamanan Informasi (SMKI/ISMS), SMKI adalah kerangka kerja yang mengintegrasikan kebijakan, prosedur, dan kontrol keamanan untuk mengelola risiko keamanan informasi secara efektif. Standar internasional ISO/IEC 27001 menjadi acuan utama dalam implementasi SMKI, yang menggunakan siklus Plan- Do-Check-Act (PDCA) untuk perencanaan, pelaksanaan, pemantauan, dan perbaikan berkelanjutan sistem keamanan informasi (Putra et al., 2016).

Dalam hal ini, manajemen resiko turut andil dalam mengimplementasikan dan mengelola keamanan informasi, manajemen risiko menjadi inti dalam pengelolaan keamanan informasi. Organisasi harus mengidentifikasi, mengevaluasi, dan mengelola risiko yang mungkin terjadi pada aset informasi. Pendekatan ini melibatkan analisis ancaman, kerentanan, dan dampak terhadap kerahasiaan, integritas, dan ketersediaan informasi (prinsip CIA Triad) (A. D. Saputra et al., 2023).

Kebijakan keamanan informasi harus terdokumentasi dengan jelas dan mencakup komitmen organisasi terhadap keamanan serta arahan umum implementasi keamanan. Prosedur operasional dan Standar Operasional Prosedur (SOP) diperlukan untuk memastikan konsistensi dalam pelaksanaan keamanan (Losari Indah & Hayuhardhika Nugraha Putra, 2020a). Pengendalian akses yang ketat, praktik pengkodean aman, enkripsi data, dan pengelolaan insiden keamanan merupakan bagian penting dalam pengelolaan keamanan informasi. Kontrol ini diterapkan sepanjang siklus hidup sistem informasi untuk meminimalkan risiko keamanan

Edukasi dan Sosialisasi Keamanan Siber

Keamanan siber adalah praktik untuk melindungi komputer, jaringan, aplikasi perangkat lunak, sistem kritis, dan data dari ancaman digital yang semakin kompleks. Dalam konteks ini, edukasi dan sosialisasi keamanan siber menjadi sangat penting untuk meningkatkan kesadaran dan kemampuan masyarakat, terutama pelajar dan pengguna teknologi aktif, dalam menghadapi risiko-risiko yang ada di dunia digital (Losari Indah & Hayuhardhika Nugraha Putra, 2020b).

Keamanan siber meliputi upaya melindungi kerahasiaan, integritas, dan ketersediaan data dari akses atau serangan yang tidak sah. Konsep dasar keamanan siber mencakup perlindungan terhadap ancaman seperti phishing, malware, ransomware, dan serangan DDoS. Menurut ISACA, tiga pilar utama keamanan siber adalah confidentiality (kerahasiaan), integrity (integritas), dan availability (ketersediaan) (Marwati & Astofa, 2024).

Berbagai metode digunakan dalam edukasi keamanan siber, seperti penyuluhan, diskusi interaktif, distribusi materi edukatif, pelatihan, dan simulasi praktik keamanan digital. Pendekatan partisipatif dan kolaboratif memungkinkan peserta aktif berbagi pengalaman dan meningkatkan kesadaran kolektif terhadap risiko siber (Karim et al., 2023). Contohnya, pengabdian masyarakat di Kelurahan Tanah Merah menggunakan edukasi lisan, demonstrasi praktik, dan sesi tanya jawab untuk meningkatkan pemahaman masyarakat tentang ancaman phishing dan malware (Setyadi et al., 2024).

Sasaran utama edukasi ini adalah pelajar, masyarakat umum, serta kelompok komunitas yang rentan terhadap ancaman siber. Pelajar sebagai pengguna teknologi aktif perlu diberikan pemahaman dasar tentang keamanan siber dan perlindungan data pribadi agar dapat menjadi pengguna internet yang bijak dan bertanggung jawab (Marwati et al., 2025). Di tingkat masyarakat, edukasi berkelanjutan dapat membentuk kader pengawas keamanan data yang melaporkan potensi ancaman kepada pihak berwenang (Karim et al., 2023).

Edukasi dan sosialisasi keamanan siber bertujuan menciptakan perubahan perilaku dalam penggunaan teknologi digital secara aman, meningkatkan kesadaran kolektif, dan memperkuat perlindungan data pribadi secara menyeluruh. Hasil evaluasi kegiatan edukasi menunjukkan peningkatan pemahaman dan keterampilan praktik keamanan digital serta keinginan untuk mendapatkan edukasi berkelanjutan (Setyadi et al., 2024).

METODE PENELITIAN

Dalam penelitian ini, metode kualitatif digunakan untuk mendapatkan pemahaman mendalam tentang strategi penguatan keamanan informasi digital dalam menghadapi ancaman siber yang bersifat kontekstual dan deskriptif. Menurut Afiyanti (2005) studi literatur merupakan metode pengumpulan data dengan cara membaca, menelaah, dan menganalisis sumber-sumber tertulis yang relevan dengan topik penelitian. Tujuannya adalah untuk mencari teori-teori yang sesuai dengan masalah penelitian, memperkuat dasar teoritis, serta memberikan konteks yang lebih luas terhadap hasil penelitian.

Untuk mencapai tujuan ini, berbagai literatur dikumpulkan, dianalisis, dan disatukan, termasuk dokumen resmi Kementerian Komunikasi dan Informasi (KOMINFO). Data yang digunakan dalam penelitian ini berasal dari penelitian pustaka sebelumnya yang berfokus pada kebijakan, strategi, dan prosedur untuk meningkatkan keamanan data digital yang telah diterapkan atau diusulkan oleh KOMINFO dan entitas terkait lainnya.

Analisis data dilakukan secara deskriptif dengan menemukan tema utama, memeriksa kesesuaian strategi saat ini, dan mengevaluasi seberapa efektif metode yang digunakan untuk melawan ancaman siber. Dengan menggunakan pendekatan ini, penelitian diharapkan dapat memberikan gambaran menyeluruh tentang strategi yang tepat dan berguna untuk meningkatkan keamanan informasi digital di era digital, khususnya dalam konteks kebijakan dan implementasi.

HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis data literatur dan kebijakan yang telah dikaji, strategi penguatan keamanan informasi digital yang dilakukan oleh Kementerian Komunikasi dan Informatika (Kominfo) dapat dikategorikan ke dalam empat pendekatan utama, yakni: regulasi dan kebijakan, pembangunan kapasitas SDM, implementasi teknologi keamanan informasi, serta edukasi publik (Erikha & Hoesein, 2025).

Regulasi dan Kebijakan Perlindungan Data

Kementerian Kominfo telah mendorong pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai landasan hukum utama dalam menjaga hak atas privasi masyarakat digital (Saly et al., 2023). UU ini menjabarkan hak-hak subjek data, kewajiban pengendali data, serta mekanisme penyelesaian sengketa akibat pelanggaran data pribadi. Perlindungan data pribadi kini menjadi salah satu indikator utama keberhasilan negara dalam menjaga kedaulatan digital (Kurnianingrum, 2023).

Namun, efektivitas implementasi UU ini masih bergantung pada pengawasan dan penegakan hukum yang kuat. Penelitian normatif juga menyebutkan bahwa pelaksanaan perlindungan data di Indonesia masih belum optimal dan sering terhambat oleh tumpang tindih kewenangan antar lembaga (Aqilah et al., 2024).

Pengembangan Talenta Digital dan SDM Keamanan Siber

Kementerian Kominfo bekerja sama dengan sektor swasta dan institusi pendidikan untuk membentuk SDM yang kompeten dalam bidang keamanan siber (Aji, 2023). Program pelatihan seperti Digital Talent Scholarship bekerja sama dengan Google dan Microsoft

menunjukkan komitmen terhadap peningkatan kapasitas nasional di sektor ini (Budi et al., 2021).

Ketimpangan jumlah talenta dengan kebutuhan industri keamanan siber masih menjadi tantangan utama. Kementerian Kominfo dan Badan Siber dan Sandi Negara (BSSN) telah mengadakan diskusi untuk meningkatkan kompetensi SDM dalam keamanan siber, mengingat kebutuhan akan SDM yang berkualitas untuk menangani ancaman siber yang semakin kompleks (Rizki, 2022a).

Salah satu metode yang disarankan adalah Enskripsi asimetris. Menurut Natalia Kristanty (2024) Enkripsi asimetris adalah metode kriptografi yang menggunakan sepasang kunci, yaitu kunci publik dan kunci privat, untuk mengamankan data dalam proses komunikasi digital. Dalam konteks transaksi digital seperti QRIS, enkripsi asimetris (misalnya, algoritma RSA 2048-bit) digunakan untuk Melindungi data transaksi, yakni Data yang dikirim dari pengguna ke sistem pembayaran dienkripsi menggunakan kunci publik sehingga hanya dapat didekripsi oleh pihak yang memiliki kunci privat, Menjamin kerahasiaan dan integritas, yakni Hanya penerima yang sah yang dapat mengakses informasi sensitif, dan data tidak dapat diubah selama transmisi tanpa terdeteksi, Mencegah akses tidak sah, yakni dengan Jika data dicuri saat proses transmisi, pihak ketiga tidak dapat membacanya tanpa kunci privat. Enkripsi asimetris menjadi fondasi keamanan digital modern, terutama untuk transaksi keuangan, karena mampu mengurangi risiko pencurian data dan penipuan.

Strategi Teknologi dan Sistem Manajemen Keamanan Informasi (SMKI)

Penerapan ISO/IEC 27001 sebagai standar internasional. SO/IEC 27001 adalah standar internasional yang menetapkan persyaratan untuk membangun, menerapkan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (SMKI atau ISMS: Information Security Management System) dalam suatu organisasi. Standar ini memberikan kerangka kerja komprehensif untuk mengelola risiko keamanan informasi melalui kebijakan, prosedur, kontrol, dan audit internal yang sistematisdalam manajemen keamanan informasi telah menjadi acuan penting (Soesanto et al., 2023). Kominfo dan beberapa instansi telah mengadopsi kerangka kerja ini dalam membangun sistem yang tangguh dan adaptif terhadap serangan.

Implementasi SMKI juga menekankan pentingnya manajemen risiko informasi, di mana identifikasi kerentanan, penilaian dampak, dan mitigasi risiko dilakukan secara sistematis. Penguatan infrastruktur teknologi seperti firewall, enkripsi, dan sistem deteksi intrusi juga diterapkan secara bertahap (Musyarofah & Bisma, 2021).

Edukasi dan Sosialisasi Keamanan Siber

Program literasi digital dan kampanye kesadaran keamanan siber dilakukan untuk mencegah insiden dari sisi pengguna. Edukasi kepada masyarakat, terutama generasi muda, menjadi krusial mengingat mereka adalah pengguna internet paling aktif. Penelitian menunjukkan bahwa metode penyuluhan langsung dan simulasi praktik lebih efektif dibandingkan pendekatan teoritis semata (Rizki, 2022).

Menurut ISACA dalam (Thakur & Pathan, 2020), tiga prinsip utama keamanan siber yang harus dipahami masyarakat adalah Confidentiality, Integrity, dan Availability (CIA Triad). Prinsip ini menjadi dasar dalam membangun kesadaran kolektif untuk menjaga data pribadi dan menghindari ancaman phishing, ransomware, dan DDoS.

KESIMPULAN

Temuan penelitian ini menunjukkan bahwa penguatan keamanan informasi digital bukan sekadar kebutuhan teknis, melainkan juga tuntutan strategis di tengah meningkatnya ancaman siber, khususnya di lingkungan Kementerian Komunikasi dan Informatika. Upaya ini tidak dapat dilakukan secara parsial, melainkan membutuhkan pendekatan menyeluruh yang mencakup aspek regulasi, teknologi, sumber daya manusia, serta kesadaran kolektif akan pentingnya perlindungan data dan informasi (Cloramidine & Badaruddin, 2023).

Keberadaan regulasi seperti Undang-Undang Perlindungan Data Pribadi menjadi fondasi penting dalam membangun kepercayaan publik terhadap pengelolaan data oleh pemerintah. Di sisi lain, strategi implementasi keamanan informasi yang diterapkan oleh Kementerian Kominfo menunjukkan perlunya pengelolaan yang adaptif dan responsif terhadap dinamika ancaman siber. Hal ini mencakup perencanaan kebijakan, pelaksanaan standar keamanan, hingga evaluasi berkala atas efektivitas sistem yang digunakan. Edukasi dan sosialisasi kepada pegawai dan masyarakat umum menjadi elemen pendukung yang krusial dalam menumbuhkan budaya sadar keamanan siber. Selain itu, pengembangan talenta digital dan peningkatan kapasitas sumber daya manusia di bidang keamanan informasi menjadi investasi jangka panjang yang sangat dibutuhkan (Darmawan et al., 2025).

Dengan komitmen yang kuat dan kolaborasi lintas sektor, Kementerian Kominfo berpotensi menjadi contoh bagi institusi pemerintah lainnya dalam membangun sistem keamanan informasi digital yang andal, inklusif, dan berkelanjutan (A. Saputra, 2024).

DAFTAR PUSTAKA

Adma, A., Surbakti, Y. M., & Sari, P. (2023). Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(1), 7.

Afiyanti, Y. (2005). PENGGUNAAN LITERATUR DALAM PENELITIAN KUALITATIF. In *Jurnal Keperawatan Indonesia* (Vol. 9, Issue 1).

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238.

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5.

Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, *9*(2), 113–118.

Aqilah, R., Waryenti, D., Susanti, P., Tanggung, :, Negara, J., & Pelindungan, M. (2024). *Jurnal Ilmiah Kutei Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. *23*(2), 158–172. https://doi.org/10.33369/jik.v23i2.34476

Arham, M. R. H., & Risal, M. C. (2023). Perlindungan data pribadi bagi pengguna media sosial. *JURNAL AL TASYRI'IYYAH*, 109–119.

Aurabillah, B., Aprillia Putri, L., Citra Fadhlilla, N., & Wulansari, A. (2024). IMPLEMENTASI FRAMEWORK ISO 27001 SEBAGAI PROTEKSI KEAMANAN

INFORMASI DALAM PEMERINTAHAN (SYSTEMATIC LITERATURE REVIEW). In *Jurnal Mahasiswa Teknik Informatika* (Vol. 8, Issue 1).

Budi, E., Wira, D., & Infantono, A. (2021a). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia P-ISSN*, *2086*, 5805.

Budi, E., Wira, D., & Infantono, A. (2021b). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia P-ISSN*, *2086*, 5805.

Budiyanto, D., & Mabruri, M. (2025). PENTINGNYA KEAMANAN SIBER DALAM ERA DIGITAL: TINJAUAN GLOBAL DAN KONDISI DI INDONESIA. *Prosiding Seminar Nasional Sains Dan Teknologi Seri III Fakultas Sains Dan Teknologi*, *2*(1).

Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). *Populis: Jurnal Sosial Dan Humaniora*, *8*(1), 57–73.

Darmawan, C. K., Sebastian, E., Notokusumo, F. L., & Loprang, J. R. (2025). URGENSI PENGUATAN REGULASI PELINDUNGAN DATA DAN KEAMANAN SIBER DI INDONESIA TERHADAP ANCAMAN HACKING DALAM SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK. *Jurnal Suara Keadilan*, *26*(1), 77–102.

Deannova Saputra, C., Septiawan Saputra, G., Aprilliani, F., & Martinelli, I. (2024). Perspektif Hukum terhadap Privasi dan Perlindungan Data Pribadi di Era Digital. *JIHHP*, *5*(1). https://doi.org/10.38035/jihhp

Erikha, A., & Hoesein, Z. A. (2025). *Strategi Pencegahan Kebocoran Data Pribadi melalui Peran Kominfo dan Gerakan Siberkreasi dalam Edukasi Digital*. https://jurnal.darmaagung.ac.id/index.php/retentum

Febrian Aska, M., pratama Putta, D., & Julyana Magdalena Sinambela, C. (2024). Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital. *Journal of Information and Information Security (JIFORTY)*, *5*(2), 187–200.

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, *5*(1), 39–57.

Karim, A., Biharudin, A., Hidayat, A. R., & Arifin, M. S. (2023a). Edukasi dan Sosialisasi Cybercrime terhadap Keamanan Data bagi Kelompok Pembina Kesejahteraan Keluarga. *Jurnal Ilmiah Pengabdian Dan Inovasi*, *2*(2), 373–380.

Karim, A., Biharudin, A., Hidayat, A. R., & Arifin, M. S. (2023b). Edukasi dan Sosialisasi Cybercrime terhadap Keamanan Data bagi Kelompok Pembina Kesejahteraan Keluarga. *Jurnal Ilmiah Pengabdian Dan Inovasi*, *2*(2), 373–380.

Kurnianingrum, T. P. (2023). Urgensi pelindungan data pribadi konsumen di era ekonomi digital. *Kajian*, *25*(3), 197–216.

Lesmana, C. S. A. T., Elis, E., & Hamimah, S. (2021). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *3*(2), 1–6.

Losari Indah, D., & Hayuhardhika Nugraha Putra, W. (2020a). *Perencanaan Implementasi Keamanan Informasi menggunakan Kerangka Kerja COBIT 5 Domain Manage Security dan Manage Security Services pada DISKOMINFO Kota Batu* (Vol. 4, Issue 1). http://j- ptiik.ub.ac.id

Losari Indah, D., & Hayuhardhika Nugraha Putra, W. (2020b). *Perencanaan Implementasi Keamanan Informasi menggunakan Kerangka Kerja COBIT 5 Domain Manage Security dan Manage Security Services pada DISKOMINFO Kota Batu* (Vol. 4, Issue 1). http://j- ptiik.ub.ac.id

Marwati, F., Akrom, A., & Astofa, A. (2025). Sosialiasi Pengenalan Pentingnya Cyber Security Guna Menjaga Keamanan Data Di Era Digital Pada Siswa/I PKBM Wong Sing Gesit. *JIPM: Jurnal Inovasi Pengabdian Masyarakat*, *3*(1), 11–16.

Marwati, F., & Astofa, A. (2024). Pentingnya Edukasi Cyber Security Untuk Menjaga Keamanan Data Pribadi dari Serangan Cyber Phishing Bagi Siswa/Siswi PKBM INTAN Tangerang Selatan. *AMMA: Jurnal Pengabdian Masyarakat*, *2*(12), 1508–1514.

Musyarofah, S. R., & Bisma, R. (2021). Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001: 2013 pada institusi pemerintah. *Teknologi: Jurnal Ilmiah Sistem Informasi*, *11*(1), 1–15.

Natalia Kristanty, D. (2024). Tren dan Tantangan Keamanan Bertransaksi dengan Qris dalam Era Transformasi Sistem Pembayaran Digital. In *Syntax Admiration* (Vol. 5, Issue 10).

Putra, A. A., Nurhayati, O. D., & Windasari, I. P. (2016). Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 20071. *Jurnal Teknologi Dan Sistem Komputer*, *4*(1), 60–66.

Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(1), 43–66. https://doi.org/10.22212/jp.v13i1.2641

Rizki, M. (2022a). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi:-. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62.

Rizki, M. (2022b). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi:-. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62.

Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023a). Analisis perlindungan data pribadi terkait uu no. 27 tahun 2022. *Jurnal Serina Sosial Humaniora*, *1*(3), 145–153.

Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023b). Analisis perlindungan data pribadi terkait uu no. 27 tahun 2022. *Jurnal Serina Sosial Humaniora*, *1*(3), 145–153.

Santoso, F. B., Pujianto, R., & Ramadhan, T. (2024). 307-320 Jakarta Raya; Jl. Raya Perjuangan No. 81 Marga Mulya. *Journal of Information and Information Security (JIFORTY)*, *5*(2), 88955882. http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Saputra, A. (2024). Perlindungan Hukum Bagi Konsumen dan Pelaku Usaha Dalam Transaksi Jual Beli Online Dengan Menggunakan Metode Cash On Delievery. *Indragiri Law Review*, *2*(3), 9–16.

Saputra, A. D., Dione, F., & Uluputty, I. (2023). Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *5*(2), 159–187.

Setyadi, H. J., Masa, A. P. A., Widagdo, P. P., Irsyad, A., Aulia, S., Nugroho, M. H., & Ananda, N. T. (2024). Edukasi Keamanan Cyber Untuk Melindungi Masyarakat Dari Ancaman

Digital. *Pengabdian Kepada Masyarakat Bidang Teknologi Dan Sistem Informasi (PETISI)*, *2*(2), 40–47.

Soesanto, E., Kurniasih, F., Mutiara, P., & Afifi, S. T. (2023). Sistem manajemen keamanan informasi dengan standar ISO/IEC 27001 dan ISO/ICE 27002 pada PT Jasa Marga. *Co- Creation: Jurnal Ilmiah Ekonomi Manajemen Akuntansi Dan Bisnis*, *1*(4), 169–179.

Surbakti, F. P. S. (2024). Edukasi Keamanan Siber Berdigital dengan Aman. *Prima Abdika: Jurnal Pengabdian Masyarakat*, *4*(4), 868–878. https://doi.org/10.37478/abdika.v4i4.4967

Thakur, K., & Pathan, A.-S. K. (2020). *Cybersecurity fundamentals: A real-world perspective*.

CRC Press. Wahidin, D., & Wati, I. I. (2024). Peluang dan Tantangan Transformasi Digital di Indonesia. *Prosiding Seminar Nasional Manajemen, Ekonomi Dan Akuntansi*, *9*, 311–322.

Zulkarnaen, S. R., Wisna, N., & Asniar, A. (2024). PENGARUH TEKNOLOGI INFORMASI DAN KEAMANAN APLIKASI TERHADAP KEPUASAN PENGGUNA QRIS PADA MASYARAKAT DI KOTA BANDUNG. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, *8*(2), 2345–2354.