Jurnal RECHTSVINDING Media Pembinaan Hukum Nasional ISSN 2089-9009
Volume 15 Nomor 1, April 2026

MEMBANGUN KESADARAN HUKUM MASYARAKAT DALAM MENINGKATKAN KEAMANAN SIBER

Edmon Makarim
Fakultas Hukum Universitas Indonesia

Abstract

The rapid development of digital technology has significantly transformed modern society while simultaneously escalating cyber security threats that affect individuals, organizations, and states. The growing dependence on digital space is not always accompanied by adequate legal awareness and cyber security literacy, making the public particularly vulnerable to cyber crimes such as personal data breaches, online fraud, and social engineering attacks. This article aims to analyze the urgency of building public legal awareness in enhancing cyber security in the digital era and to examine its relevance to the effectiveness of national regulations on information technology and personal data protection. This study employs a normative juridical approach supported by a sociological perspective of law and literature analysis. The findings indicate that cyber security should not be viewed solely as a technical issue, but rather as a multidimensional challenge strongly influenced by human behavior and public awareness. Therefore, strengthening legal awareness through educational and participatory approaches is a fundamental prerequisite for establishing a safe, inclusive, and sustainable digital ecosystem, as well as for reinforcing national cyber resilience amid ongoing digital transformation.
Keywords: cyber security, legal awareness, personal data, digital society, data protection

Abstrak

Perkembangan teknologi digital telah membawa perubahan signifikan dalam kehidupan masyarakat, sekaligus meningkatkan eskalasi ancaman keamanan siber yang berdampak pada individu, organisasi, dan negara. Tingginya ketergantungan masyarakat terhadap ruang digital tidak selalu diimbangi dengan tingkat kesadaran hukum dan literasi keamanan siber yang memadai, sehingga menjadikan masyarakat sebagai kelompok yang paling rentan terhadap kejahatan siber, seperti pencurian data pribadi, penipuan daring, dan rekayasa sosial. Artikel ini bertujuan untuk menganalisis urgensi pembangunan kesadaran hukum masyarakat dalam meningkatkan keamanan siber di era digital, serta menelaah keterkaitannya dengan efektivitas regulasi nasional di bidang teknologi informasi dan perlindungan data pribadi. Metode penulisan yang digunakan adalah pendekatan yuridis normatif dengan dukungan perspektif sosiologis hukum dan analisis literatur. Hasil kajian menunjukkan bahwa keamanan siber tidak dapat dipahami semata-mata sebagai persoalan teknis, melainkan sebagai isu multidimensional yang sangat dipengaruhi oleh faktor perilaku dan kesadaran masyarakat. Oleh karena itu, penguatan kesadaran hukum melalui pendekatan edukatif dan partisipatif menjadi prasyarat utama dalam menciptakan ekosistem digital yang aman, inklusif, dan berkelanjutan, sekaligus memperkuat ketahanan siber nasional di tengah dinamika transformasi digital.
Kata kunci: keamanan siber, kesadaran hukum, data pribadi, masyarakat digital perlindungan data

A. Latar belakang

Teknologi digital meliputi internet, media sosial, aplikasi seluler, serta beragam platform digital lainnya kini telah menyatu dalam aktivitas keseharian manusia dan membawa perubahan mendasar dalam cara individu berinteraksi, menimba pengetahuan, serta memperoleh dan mengelola informasi.[1] Kehadiran teknologi digital tidak hanya mempermudah komunikasi dengan teman dan keluarga, tetapi juga membuka ruang baru dalam mencari pekerjaan, membangun relasi sosial, menemukan pasangan hidup, menjalankan aktivitas bisnis, hingga menikmati hiburan seperti permainan daring dan belanja elektronik. Didukung oleh ketersediaan jaringan internet berkecepatan tinggi serta perangkat pintar yang semakin terjangkau, akses terhadap dunia maya menjadi semakin luas dan inklusif. Hampir setiap individu kini terhubung secara virtual dengan jutaan pengguna lain di berbagai belahan dunia, menciptakan ekosistem digital yang dinamis dan saling terhubung tanpa batas ruang dan waktu.[2]

Namun, di balik berbagai kemudahan dan manfaat tersebut, meningkatnya ketergantungan pada ruang siber juga membawa konsekuensi berupa meningkatnya kerentanan terhadap berbagai bentuk kejahatan siber. Aktivitas digital yang dilakukan tanpa kesadaran dan kehati-hatian yang memadai dapat membuka celah bagi pihak-pihak yang tidak bertanggung jawab untuk melakukan penyalahgunaan, mulai dari pencurian data pribadi, penipuan daring, peretasan akun, hingga bentuk pelecehan dan serangan digital lainnya. Kelalaian yang tampak sepele, seperti penggunaan kata sandi yang lemah, membagikan informasi pribadi secara berlebihan, atau mengakses layanan digital yang tidak aman, berpotensi menimbulkan dampak serius berupa kerugian finansial, rusaknya reputasi, serta gangguan terhadap rasa aman dan privasi individu.[3]

Oleh karena itu, kesadaran dan kewaspadaan dalam menjalani kehidupan digital menjadi suatu keharusan. Setiap individu dituntut untuk lebih berhati-hati dan bertanggung jawab dalam menggunakan teknologi, baik ketika melakukan transaksi keuangan, berinteraksi di media sosial, bermain game daring, maupun mencari dan membagikan informasi melalui internet. Sikap waspada tersebut tidak hanya berfungsi sebagai upaya perlindungan diri, tetapi juga sebagai bagian dari budaya digital yang sehat dan aman, sehingga pemanfaatan teknologi informasi dan komunikasi dapat benar-benar memberikan manfaat maksimal tanpa mengorbankan keamanan dan kenyamanan penggunanya.[4]

Berbagai kajian menunjukkan bahwa eskalasi ancaman siber tidak semata-mata disebabkan oleh kecanggihan teknologi atau kelemahan sistem, melainkan sangat dipengaruhi oleh faktor manusia (*human factor*).[5] Rendahnya

---

1 Joshi, Renu, N. Pavithra, and C. K. Singh. "Internet an integral part of human life in 21st century: a review." *Current Journal of Applied Science and Technology,* Vol. 41.issue 36 (2022). Hlm. 12-18, tersedia https://doi.org/10.9734/cjast/2022/v41i363963, diakses pada 28 Januari 2026.

2 ISO JIL INFORMATION TECHNOLOGYLIMITED, *Cyber Security Awareness Handbook*, diakses pada tanggal 28 Januari 2026. .

3 *Ibid.*

4 *Ibid.*

5 *Nabilla* Ivana Nova dkk, " Analisis Keamanan Sistem Pembayaran Digital terhadap Perlindungan Data Pengguna", *Department of Digital Business Journal of Artificial Intelligence and Digital Business (RIGGS)* , Vol. 4 No. 4 (2026), hlm. 8985-8991, tersedia https://journal.ilmudata.co.id/index.php/RIGGS diakses pada tanggal 29 Januari 2026.

kesadaran masyarakat terhadap keamanan siber menjadi titik lemah utama yang kerap dimanfaatkan oleh pelaku kejahatan digital. Praktik-praktik seperti penggunaan kata sandi yang lemah, membagikan kode autentikasi sekali pakai (OTP), mengklik tautan mencurigakan, serta penggunaan aplikasi ilegal merupakan contoh nyata bagaimana perilaku pengguna berkontribusi terhadap meningkatnya risiko keamanan siber.[6] Dengan demikian, keamanan siber harus dipahami sebagai persoalan perilaku dan kesadaran masyarakat, bukan semata-mata persoalan teknologi.

Dalam konteks ekonomi digital, data pribadi telah berkembang menjadi aset bernilai tinggi. Informasi mengenai identitas, kebiasaan, preferensi, dan aktivitas digital individu memiliki nilai ekonomi yang signifikan dan menjadi komoditas strategis dalam ekosistem digital. Namun, tingginya nilai data pribadi tersebut tidak selalu diiringi dengan kesadaran masyarakat untuk melindunginya. Banyak pengguna layanan digital yang secara sukarela memberikan data pribadi tanpa memahami risiko, tujuan pemrosesan, maupun konsekuensi hukum yang mungkin timbul akibat penyalahgunaan data tersebut. Fenomena ini menunjukkan adanya kesenjangan antara tingkat adopsi teknologi dan tingkat literasi keamanan serta kesadaran hukum masyarakat.

Di Indonesia, tantangan keamanan siber semakin mengemuka seiring dengan pesatnya pertumbuhan pengguna internet dan perluasan layanan digital, baik dalam bentuk digitalisasi pelayanan publik, sistem pembayaran elektronik, maupun platform perdagangan daring yang mendorong inklusi ekonomi masyarakat. Di balik berbagai manfaat tersebut, peningkatan aktivitas digital juga diiringi oleh lonjakan kasus kejahatan siber yang menyasar masyarakat sebagai pengguna akhir, sering kali dipicu oleh kelalaian pengguna dan rendahnya kesadaran terhadap prinsip-prinsip dasar keamanan siber.

Kondisi ini tercermin dari temuan paruh pertama tahun 2023 yang dilakukan oleh Nailul Huda dkk, menunjukkan bahwa informasi terkait Indonesia cukup banyak diperjualbelikan di *dark web*, terutama berupa pengumuman korban dan data yang terekspos, yang mencapai 53 persen dari total postingan, mengindikasikan bahwa kebocoran atau pencurian data kerap berujung pada pengungkapan identitas korban secara publik akibat serangan siber atau insiden peretasan.[7]

Lebih lanjut, sektor administrasi publik, termasuk layanan publik, tercatat sebagai sektor paling rentan dengan porsi sebesar 25,2 persen data Indonesia yang terdeteksi berada di dark web, sehingga menegaskan bahwa penguatan keamanan siber dan peningkatan kesadaran masyarakat menjadi kebutuhan mendesak dalam ekosistem digital nasional.[8] Kondisi ini mencerminkan bahwa pembangunan infrastruktur digital belum sepenuhnya diimbangi dengan pembangunan kapasitas sumber daya manusia dan budaya sadar keamanan siber

Dari perspektif hukum, Indonesia telah memiliki kerangka regulasi yang mengatur pemanfaatan teknologi informasi dan keamanan siber. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024 menegaskan

6 *Ibid*.
7 *Nailul* Huda dkk, Outlook Ekonomi Digital 205, Celios.
8 *Ibid*.

kewajiban penyelenggara sistem elektronik untuk menjamin keamanan, keandalan, dan tanggung jawab dalam penyelenggaraan sistem elektronik. Selain itu, UU ITE juga mengatur larangan dan sanksi terhadap berbagai bentuk kejahatan siber. Namun, keberadaan norma hukum tersebut belum sepenuhnya diinternalisasi oleh masyarakat sebagai pengguna teknologi digital, sehingga efektivitasnya dalam mencegah kejahatan siber masih terbatas.[9]

Penguatan regulasi di bidang perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP) menandai perubahan paradigma penting dalam hukum siber Indonesia. UU PDP menempatkan data pribadi sebagai hak asasi warga negara yang harus dilindungi, sekaligus menegaskan tanggung jawab pengendali dan prosesor data dalam mengelola data secara aman dan bertanggung jawab.[10] Namun, UU PDP juga secara implisit menuntut peran aktif masyarakat sebagai subjek data untuk menjaga keamanan datanya sendiri. Tanpa adanya kesadaran masyarakat mengenai nilai dan risiko data pribadi, perlindungan hukum yang diatur dalam UU PDP berpotensi tidak efektif dan bersifat reaktif.

Selain kerangka undang-undang, pemerintah juga telah menetapkan kebijakan strategis melalui Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Peraturan ini menegaskan bahwa keamanan siber merupakan bagian dari kepentingan nasional yang harus dijaga secara terpadu dan berkelanjutan. Salah satu pilar utama dalam strategi tersebut adalah pembangunan budaya sadar keamanan siber, yang menempatkan masyarakat sebagai aktor penting dalam menjaga ketahanan ruang siber nasional. [11] Kebijakan ini menunjukkan bahwa negara menyadari keterbatasan pendekatan teknis dan represif semata, serta pentingnya pendekatan edukatif dan preventif berbasis kesadaran masyarakat.

Dalam perspektif sosiologis hukum, kesadaran hukum masyarakat merupakan faktor penentu efektivitas suatu regulasi. Kesadaran hukum memainkan peran penting dalam membangun tata kelola pemerintahan yang baik dan masyarakat yang taat hukum.[12] Hukum tidak akan pernah benar-benar berfungsi secara nyata apabila tidak ditopang oleh kesadaran hukum yang hidup dan berkembang dalam masyarakat. Hukum sejatinya bukan sekadar kumpulan norma tertulis, melainkan cerminan dari kepercayaan bersama terhadap nilai-nilai yang dianggap penting dan layak untuk dijaga.

Ketika masyarakat tidak memiliki keterikatan moral dan partisipasi batin terhadap hukum, maka keberadaan hukum pun tereduksi

---

9 Undang-Undang tentang Informasi dan Transaksi Elektronik, UU Nomor 11 Tahun 2008, LN Tahun 2008 No.58, TLN No. 4843 sebagiaimana terkahir diubah oleh UU Nomor 1 Tahun 2024 tentang Perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, LN Tahun 2024 No. 6905 selanjutnya disebut UU ITE.

10 Undang-Undang tentang Perlindungan Data Pribadi, UU Nomor 27 Tahun 2022, LN Tahun 2022 No, 196, TLN No. 6829.

11 Peraturan Presiden tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, Perpres Nomor 47 Tahun 2023, LN Tahun 2023 No. 99.

12 Annisa Fajriyati Sadeli &Indira Irawati, "Awareness o f Personal Data Protection Law In Concern To Literacy, " *Jurnal Kajian Informasi & Perpustakaan,* Vol. 11, No. 2 (2023), tersedia pada https://jurnal.unpad.ac.id/jkip/article/view/47526, diakses pada tanggal 28 Januari 2026.

menjadi sekadar rangkaian ketentuan formal yang kehilangan makna substantif.[13] Dalam konteks keamanan siber, kesadaran hukum mencakup pemahaman masyarakat terhadap hak dan kewajiban digital, risiko hukum dari perilaku tidak aman di ruang siber, serta etika dalam menggunakan teknologi informasi. Tanpa kesadaran tersebut, hukum akan selalu tertinggal di belakang perkembangan teknologi dan hanya berfungsi sebagai alat penindakan setelah terjadinya pelanggaran.

Hasil penelitian yang dilakukan oleh Yul Ernis[14] menunjukkan adanya hubungan yang kuat antara pendidikan dan kesadaran hukum, di mana pendidikan berperan sebagai fondasi utama dalam pembangunan manusia yang berkesadaran hukum, mengingat kesadaran hukum bukanlah kondisi yang terbentuk secara alamiah, melainkan berkembang melalui pemanfaatan nalar manusia sebagai potensi dasarnya yang terwujud dalam pengetahuan, pemahaman, sikap, dan perilaku. Sejalan dengan hal tersebut, berbagai studi mengenai kesadaran hukum mengungkapkan bahwa rendahnya tingkat kepatuhan dan partisipasi masyarakat terhadap norma hukum kerap dipengaruhi oleh minimnya edukasi, kompleksitas regulasi yang sulit dipahami, serta kurangnya strategi komunikasi hukum yang efektif, sehingga semakin menegaskan pentingnya pendidikan hukum yang berkelanjutan dan kontekstual bagi masyarakat.

Hal ini juga terjadi dalam konteks keamanan siber, di mana regulasi sering dipersepsikan sebagai isu teknis atau tanggung jawab negara dan penyelenggara sistem elektronik semata. Akibatnya, masyarakat cenderung pasif dan tidak menyadari perannya sebagai subjek hukum yang memiliki tanggung jawab dalam menjaga keamanan ruang siber. Oleh karena itu, pembangunan kesadaran masyarakat dalam meningkatkan keamanan siber harus dipahami sebagai bagian integral dari pembangunan hukum nasional di era digital. Kesadaran tersebut tidak hanya mencakup literasi teknis, tetapi juga literasi hukum dan etika digital. Masyarakat perlu dibekali pemahaman mengenai pentingnya perlindungan data pribadi, risiko kejahatan siber, serta konsekuensi hukum dari perilaku digital yang tidak aman.[15] Pendekatan ini sejalan dengan praktik global yang menempatkan *cyber security awareness* sebagai fondasi utama dalam menciptakan ekosistem digital yang aman dan terpercaya.

Lebih jauh, pembangunan kesadaran keamanan siber juga memiliki implikasi strategis bagi ketahanan nasional. Ruang siber yang tidak aman dapat mengganggu stabilitas ekonomi, kepercayaan publik terhadap layanan digital, serta legitimasi negara dalam melindungi warga negaranya. Dalam konteks ini, masyarakat tidak hanya diposisikan sebagai objek perlindungan, tetapi juga sebagai subjek aktif yang berperan dalam menjaga keamanan dan ketahanan ruang siber nasional. Kesadaran masyarakat menjadi

---

13 M. Khusnul Khuluq, "Hukum dan Kesadaran Hukum: Dari Teori E. Ehrlich Hingga Habermas, " tersedia pada https://marinews.mahkamahagung.go.id/artikel/hukum-dan-kesadaran-hukum-dari-teori-e-ehrlich-0pP, diakses pada tanggal 28 Januari 2026.

14 Yul Ernis, "Implikasi Penyuluhan Hukum Langsung terhadap Peningkatan Kesadaran Hukum Masyarakat," *Jurnal Penelitian Hukum De Jure*, tersedia pada https://doi.org/10.30641/dejure.2018.V18.477-496, diakses pada tanggal 28 Januari 2026.

15 R. E. Purba et al., "Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital," *Mandub, Jurnal Politik, Sosial, Hukum dan Humaniora,* Vol 2, No. 2 (2024): 167–176.

prasyarat bagi terciptanya kolaborasi yang efektif antara pemerintah, sektor swasta, dan pengguna dalam menghadapi ancaman siber yang semakin kompleks.

Berdasarkan latar belakang tersebut, artikel ini berfokus pada analisis permasalahan utama mengenai bagaimana membangun dan memperkuat kesadaran masyarakat dalam keamanan siber di era digital? Penguatan kesadaran ini dipandang sebagai prasyarat penting bagi efektivitas regulasi nasional di bidang teknologi informasi dan perlindungan data pribadi, sekaligus sebagai fondasi dalam mewujudkan ekosistem digital yang aman, inklusif, dan berkelanjutan. Tanpa kesadaran masyarakat yang memadai, transformasi digital berpotensi menjadi sumber kerentanan baru yang justru menghambat tujuan pembangunan nasional di era digital.

B. Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan kualitatif, yang berfokus pada kajian terhadap norma hukum, asas, dan prinsip yang mengatur keamanan siber serta perlindungan data pribadi di Indonesia. Pendekatan ini digunakan untuk menganalisis kerangka regulasi yang relevan, khususnya Undang-Undang tentang Informasi dan Transaksi Elektronik, Undang-Undang tentang Perlindungan Data Pribadi, serta kebijakan nasional di bidang keamanan siber.

Selain pendekatan normatif, penelitian ini juga didukung oleh pendekatan sosiologis hukum**,** guna memahami hubungan antara ketentuan hukum dan realitas sosial masyarakat digital, khususnya terkait tingkat kesadaran hukum dan perilaku masyarakat dalam menjaga keamanan siber. Pendekatan ini memungkinkan analisis yang lebih komprehensif terhadap efektivitas hukum dalam konteks penerapannya di masyarakat.

Bahan hukum yang digunakan terdiri atas bahan hukum primer**,** berupa peraturan perundang-undangan dan kebijakan resmi yang berkaitan dengan keamanan siber dan perlindungan data pribadi; bahan hukum sekunder**,** berupa buku, jurnal ilmiah, hasil penelitian, dan publikasi akademik yang relevan; serta bahan hukum tersier sebagai bahan pendukung. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan *(library research).*

Analisis data dilakukan secara kualitatif deskriptif dengan menafsirkan dan mengaitkan ketentuan hukum yang berlaku dengan konsep kesadaran hukum, literasi keamanan siber, serta tantangan yang dihadapi masyarakat digital. Hasil analisis digunakan untuk merumuskan kesimpulan dan rekomendasi mengenai strategi penguatan kesadaran hukum masyarakat dalam meningkatkan keamanan siber di era digital.

C. Pembahasan

1) Konsep Keamanan Siber dan Kesadaran Masyarakat di Era Digital

Keamanan siber (cyber security) pada hakikatnya merupakan suatu kondisi terlindunginya sistem elektronik, jaringan, perangkat, serta data dari berbagai ancaman yang dapat mengganggu kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) informasi. Dalam perkembangan mutakhir, konsep keamanan siber tidak lagi terbatas pada perlindungan infrastruktur teknologi informasi semata, tetapi telah bergeser menjadi isu tata kelola

(governance) yang melibatkan dimensi hukum, sosial, budaya, dan perilaku manusia.[16]

Pendekatan teknis dalam keamanan siber, seperti penggunaan enkripsi, firewall, dan sistem deteksi intrusi, meskipun tetap penting, tidak akan efektif tanpa dukungan kesadaran pengguna sebagai lapisan pertahanan pertama. Berbagai studi menegaskan bahwa manusia merupakan mata rantai terlemah dalam sistem keamanan siber, sekaligus faktor penentu keberhasilan perlindungan sistem elektronik.[17] Oleh karena itu, keamanan siber harus dipahami sebagai tanggung jawab kolektif yang melibatkan negara, penyelenggara sistem elektronik, dan masyarakat sebagai pengguna akhir teknologi digital.

Dalam konteks masyarakat digital, kesadaran keamanan siber merupakan bagian integral dari kesadaran hukum dan literasi digital. Kesadaran keamanan siber dan literasi digital memiliki hubungan yang saling menguatkan dan bersifat sinergis, di mana keduanya mendorong individu untuk secara aktif menerapkan langkah-langkah keamanan siber yang preventif serta membentuk pola perilaku daring yang lebih bijak, aman, dan bertanggung jawab.[18] Tanpa kesadaran tersebut, masyarakat cenderung memandang keamanan siber sebagai persoalan teknis yang sepenuhnya menjadi tanggung jawab negara atau penyedia layanan digital. Pandangan ini berimplikasi pada rendahnya kepedulian individu terhadap perlindungan data pribadi dan keamanan aktivitas digitalnya sendiri.

Lebih lanjut, kesadaran keamanan siber juga berkaitan erat dengan pemahaman masyarakat terhadap nilai strategis data dan informasi. Dalam ekosistem digital, data pribadi tidak hanya berfungsi sebagai identitas individu, tetapi juga sebagai aset ekonomi dan sumber kekuasaan. Namun demikian, banyak pengguna layanan digital yang belum menyadari nilai tersebut, sehingga cenderung mengabaikan aspek perlindungan data dalam aktivitas sehari-hari. Fenomena ini menunjukkan bahwa rendahnya kesadaran keamanan siber tidak hanya bersumber dari keterbatasan pengetahuan teknis, tetapi juga dari lemahnya kesadaran hukum dan etika digital.[19]

Berdasarkan penelitian yang dlakukan Deny Budiyanto dan Muhammad Mabruri terhadap 500 responden masyarakat umum pengguna internet, tingkat literasi siber masyarakat di Indonesia masih menunjukkan

---

16 CISO Jil Information Technology Limited, "Cyber Security Awareness Handbook," tersedia https://www.jiit.ac.in/sites/default/files/Cyber%20Security%20Awareness%20Hand%20Book.pdf, diakses pada tanggal 29 Januari 2026.

17 Mohammad Taufik Hidayatuloh, "Kedaulatan Informasi dan Integritas Profesional: Analisis Holistik Perlindungan Rahasia Dagang dalam Industri Teknologi Informasi di Indonesia. "tersedia pada https://www.researchgate.net/publication/398870025_Kedaulatan_Informasi_dan_Integritas_Profesional_Analisis_Holistik_Perlindungan_Rahasia_Dagang_dalam_Industri_Teknologi_Informasi_di_Indonesia/link/694560810c98040d481ef02c/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19, diakses pada tanggal 29 Januasri 2026.

18 Sharma, S., et all, "Digital citizen empowerment: A systematic literature review of theories and development models. Information Technology for Development," tersedia pada https://doi.org/10.1080/02681102.2022.2046533, diakses pada tanggal 29 Januari 2026.

19 Abraham Ethan etc, "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective," I*nternational Journal of Business, Economics and Social. Development*, Vol. 2, No. 4, (2021), hlm. 43-152, tersedia pada Available online at https://journal.rescollacomm.com/index.php/ijbesd/index, diakses pada tanggal 28 Januari 2026.

kondisi yang memprihatinkan. Temuan survei mengungkapkan bahwa hanya sekitar 30 persen responden yang memiliki pemahaman yang baik mengenai ancaman siber yang umum, seperti *phishing* dan *ransomware*. Sementara itu, sekitar 40 persen responden hanya memiliki pemahaman yang terbatas, dan sisanya sekitar 30 persen mengaku tidak mengetahui secara memadai bentuk-bentuk ancaman siber tersebut.[20] Kondisi ini menunjukkan bahwa sebagian besar masyarakat masih belum memiliki bekal pengetahuan yang cukup untuk mengenali dan mengantisipasi risiko keamanan di ruang digital.

Rendahnya literasi siber tersebut tercermin pula dalam praktik keamanan digital sehari-hari. Mayoritas responden, yakni sekitar 70 persen, tidak menerapkan langkah-langkah keamanan dasar seperti penggunaan autentikasi dua faktor (*two-factor authentication/2FA*), yang seharusnya menjadi lapisan perlindungan awal terhadap akses tidak sah. Selain itu, sebanyak 60 persen responden tidak secara rutin melakukan pembaruan perangkat lunak keamanan, termasuk antivirus, sehingga perangkat yang digunakan tetap berada dalam kondisi rentan terhadap eksploitasi celah keamanan yang sebenarnya dapat dicegah.[21]

Dari aspek kesadaran terhadap serangan *phishing*, survei menunjukkan bahwa lebih dari separuh responden (55 persen) pernah menerima email atau pesan mencurigakan yang berpotensi merupakan upaya *phishing*. Namun demikian, hanya sekitar 35 persen dari responden tersebut yang mampu mengenali ciri-ciri serangan *phishing* dengan tepat. Hal ini mengindikasikan adanya kesenjangan antara pengalaman menerima ancaman siber dan kemampuan untuk mengidentifikasinya secara benar, yang berpotensi meningkatkan risiko terjadinya penipuan dan pencurian data pribadi.[22]

Kerentanan masyarakat terhadap ancaman siber juga diperparah oleh kebiasaan penggunaan kata sandi yang tidak aman. Lebih dari 65 persen responden masih menggunakan kata sandi yang lemah atau mudah ditebak, seperti deretan angka sederhana atau nama pribadi. Praktik ini membuat akun dan data pribadi mereka sangat rentan terhadap serangan *brute force* maupun *credential stuffing*. Secara keseluruhan, hasil survei ini menegaskan bahwa rendahnya tingkat literasi siber tidak hanya menjadi persoalan pengetahuan, tetapi juga berdampak langsung pada perilaku digital masyarakat, sehingga diperlukan upaya edukasi dan peningkatan kesadaran keamanan siber yang lebih sistematis dan berkelanjutan.[23]

Dalam perspektif hukum nasional, keamanan siber memiliki keterkaitan langsung dengan prinsip perlindungan hak asasi manusia, khususnya hak atas privasi dan perlindungan data pribadi. UU PDP menegaskan bahwa setiap orang berhak atas perlindungan data pribadinya dan berhak untuk menentukan penggunaan data tersebut. Namun, perlindungan hukum tersebut mensyaratkan adanya partisipasi aktif masyarakat sebagai subjek data. Tanpa kesadaran masyarakat untuk menjaga kerahasiaan data

---

20 Deny Budiyanto & Muhammad Mabruri, "Pentingnya Keamanan Siber Dalam Era Digital: Tinjauan Global Dan Kondisi Di Indonesia," *Prosiding Seminar Nasional Sains dan Teknologi Seri IIIFakultas Sains dan Teknologi, Universitas Terbuka,* Vol. 2 No. 1(2025)e, diakses pada tanggal 29 Januari 2026.

21 *Ibid.*

22 *Ibid.*

23 *Ibid.*

dan memahami risiko penyalahgunaan data, perlindungan hukum akan bersifat formalistik dan tidak efektif.[24]

Selain itu, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali menegaskan bahwa pemanfaatan teknologi informasi harus memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.[25] Norma ini menunjukkan bahwa keamanan siber bukan hanya kewajiban penyelenggara sistem elektronik, tetapi juga kewajiban setiap pengguna teknologi digital. Dengan demikian, kesadaran keamanan siber merupakan perwujudan dari kepatuhan masyarakat terhadap norma hukum yang mengatur pemanfaatan teknologi informasi.

Dari sudut pandang sosiologis, pembangunan kesadaran keamanan siber memerlukan proses yang berkelanjutan dan kontekstual. Kesadaran tidak dapat dibentuk secara instan melalui regulasi semata, melainkan melalui edukasi, sosialisasi, dan internalisasi nilai yang sesuai dengan realitas sosial masyarakat. Efektivitas hukum sangat ditentukan oleh sejauh mana hukum tersebut dipahami, diterima, dan dijalankan oleh masyarakat, karena hukum pada hakikatnya bekerja melalui pengaruhnya terhadap komunitas hukum. Suatu hukum dapat dikatakan efektif apabila mampu membentuk perilaku individu, baik dalam bentuk kepatuhan terhadap norma yang diatur maupun melalui konsekuensi yang muncul ketika terjadi ketidakpatuhan.[26] Pandangan tersebut menguatkan bahwa pembangunan keamanan siber nasional harus didukung oleh strategi peningkatan kesadaran masyarakat yang sistematis dan berkelanjutan.

Dengan demikian, konsep keamanan siber di era digital harus dipahami secara komprehensif sebagai perpaduan antara sistem teknologi yang andal, kerangka hukum yang memadai, dan kesadaran masyarakat yang tinggi. Kesadaran masyarakat bukan sekadar pelengkap, melainkan fondasi utama dalam menciptakan ruang siber yang aman, terpercaya, dan berkelanjutan. Tanpa kesadaran tersebut, berbagai kebijakan dan regulasi keamanan siber berpotensi kehilangan efektivitasnya dalam menghadapi dinamika ancaman digital yang terus berkembang.

2) Ancaman Keamanan Siber dan Kerentanan Masyarakat Digital

Transformasi digital yang masif telah menciptakan ruang interaksi baru yang sarat dengan peluang, tetapi sekaligus memunculkan spektrum ancaman keamanan siber yang semakin kompleks. Ancaman siber tidak lagi terbatas pada serangan terhadap infrastruktur teknologi informasi, melainkan telah berkembang menjadi fenomena sosial yang secara langsung memengaruhi keamanan, kesejahteraan, dan hak-hak masyarakat digital. Dalam konteks ini, masyarakat bukan hanya berperan sebagai pengguna teknologi, tetapi juga sebagai kelompok yang paling rentan terdampak oleh berbagai bentuk ancaman siber.[27]

Ancaman siber merupakan konsep kunci dalam kajian keamanan informasi karena

---

[24] UU PDP Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
[25] UU ITE, Pasal 4
[26] Judith Hahn, :Foundations of a Sociology of Canon Law."T*he Effectiveness of the Law Chapter 6*. Springer Nature Link, diakses pada 29 Januari 2026.
[27] *Cyber Security Awareness Handbook.*

mencerminkan berbagai kondisi dan peristiwa yang berpotensi menimbulkan dampak merugikan terhadap sistem informasi dan pihak-pihak yang bergantung padanya.[28] Ancaman siber dapat dipahami sebagai segala bentuk keadaan atau kejadian yang mampu mengganggu operasi organisasi termasuk misi, fungsi, citra, dan reputasi serta membahayakan aset organisasi, individu, entitas lain, bahkan negara, melalui pemanfaatan sistem informasi.[29] Dampak tersebut dapat terjadi akibat akses yang tidak sah, penghancuran data, pengungkapan informasi, perubahan informasi tanpa izin, maupun penolakan layanan (denial of service) yang menghambat ketersediaan sistem.[30] Dalam perspektif ini, ancaman siber tidak hanya berkaitan dengan aspek teknis, tetapi juga menyentuh dimensi strategis, ekonomi, dan sosial yang lebih luas.

Salah satu bentuk ancaman siber yang paling dominan adalah rekayasa sosial (social engineering), yaitu teknik manipulasi psikologis yang memanfaatkan kelemahan manusia untuk memperoleh informasi sensitif atau mengendalikan perilaku korban. Dalam konteks ini, phishing tetap menjadi ancaman yang meluas terhadap keamanan informasi, bersama dengan berbagai modus lain seperti penipuan daring dan penyamaran identitas, yang mengeksploitasi rendahnya kewaspadaan serta terbatasnya literasi keamanan digital masyarakat, sehingga mendorong individu untuk mengungkapkan data pribadi atau melakukan tindakan yang pada akhirnya merugikan kepentingan terbaik mereka, baik secara pribadi maupun institusional.[31] Ancaman ini menjadi sangat efektif karena menyerang aspek kepercayaan dan emosi manusia, yang tidak dapat sepenuhnya dilindungi oleh sistem keamanan teknis.

Selain rekayasa sosial, ancaman siber juga mencakup penyalahgunaan data pribadi, peretasan akun digital, serta serangan berbasis malware dan ransomware yang berdampak langsung pada individu. Dalam masyarakat digital yang sangat bergantung pada layanan daring, hilangnya akses akun atau kebocoran data pribadi dapat menimbulkan kerugian ekonomi, tekanan psikologis, hingga kerusakan reputasi sosial. Ancaman semacam ini menunjukkan bahwa dampak keamanan siber tidak hanya bersifat teknis, tetapi juga menyentuh dimensi sosial dan personal kehidupan masyarakat.[32]

Kerentanan masyarakat digital terhadap ancaman siber diperkuat oleh tingginya intensitas interaksi dengan teknologi digital dalam kehidupan sehari-hari. Penggunaan media sosial, aplikasi pesan instan, layanan keuangan digital, dan platform perdagangan elektronik telah menjadi bagian integral dari aktivitas masyarakat. Namun, intensitas penggunaan tersebut tidak selalu diimbangi

---

28 Kevin Matthe Caramancion et al, "The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats", tersedia pada **https://doi.org/10.3390/data7040049**, diakses pada tanggal 29 Januari 2026.

29 *Ibid.*

30 *Ibid.*

31 Ioannis Stylianou, et al, Suspicious minds: Psychological techniques correlated with online phishing, Computersin Human Behavior Reports, tersedia pada journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports , diakses pada tanggal 29 Januari 2026.

32 Yenny Aman Seah et al, "Raising Public Legal Awareness in the Digital Age*)," Journal of Law and Legal Reform,* Vol. 6 Issue 1 (2025), hlm. 209-238, tersedia pada https://doi.org/10.15294/jllr.v6i1.68129, diakses pada tanggal 29 Januari 2026.

dengan pemahaman yang memadai mengenai risiko keamanan. Ketergantungan yang tinggi terhadap teknologi digital tanpa kesadaran keamanan yang cukup menciptakan kondisi rentan (*vulnerable condition*) yang sistemik.[33]

Kerentanan yang berpusat pada manusia berakar pada bias kognitif, kesenjangan keterampilan, serta norma budaya tertentu, dan hingga kini merupakan salah satu vektor serangan yang paling banyak dieksploitasi dalam ranah keamanan siber (Papatsaroucha dkk., 2021). Praktik seperti *phishing*, penggunaan kata sandi yang lemah, dan berbagai bentuk rekayasa sosial mendominasi jenis kerentanan ini. Kondisi tersebut semakin diperparah oleh rendahnya tingkat literasi digital, yang menyebabkan individu lebih mudah dimanipulasi dan dieksploitasi dalam interaksi berbasis teknologi[34] Kondisi ini menegaskan bahwa kerentanan masyarakat digital merupakan faktor struktural dalam ekosistem keamanan siber.

Kerentanan tersebut tidak bersifat seragam di seluruh lapisan masyarakat. Berbagai studi menunjukkan bahwa kelompok masyarakat tertentu menghadapi tingkat risiko yang lebih tinggi akibat posisi sosial, aktivitas digital, atau keterbatasan akses terhadap literasi keamanan siber. Penelitian di kawasan Asia Tenggara menunjukkan bahwa aktivis masyarakat sipil, pembela hak asasi manusia, serta kelompok rentan lainnya sering menjadi sasaran serangan siber yang bertujuan membungkam ekspresi, mengganggu aktivitas, atau menimbulkan rasa takut.[35] Hal ini menunjukkan bahwa ancaman siber juga memiliki dimensi kekuasaan dan ketimpangan sosial.

Ancaman siber terhadap kelompok masyarakat tidak hanya berdampak pada individu, tetapi juga dapat melemahkan ruang partisipasi publik dan demokrasi digital. Serangan berupa doxing, peretasan akun, dan intimidasi daring dapat menciptakan efek jera (*chilling effect*) yang membatasi kebebasan berekspresi dan partisipasi masyarakat dalam ruang digital. Dalam konteks ini, keamanan siber tidak dapat dipisahkan dari perlindungan hak-hak sipil dan politik masyarakat digital.[36] Selain itu, masyarakat digital juga menghadapi ancaman berupa disinformasi dan manipulasi informasi yang tersebar melalui platform digital.

Meskipun sering tidak dikategorikan sebagai ancaman keamanan siber dalam arti teknis, disinformasi memiliki dampak signifikan terhadap keamanan sosial dan stabilitas masyarakat. Penyebaran informasi palsu dapat memicu konflik sosial, merusak kepercayaan publik, dan memengaruhi pengambilan keputusan individu maupun kolektif. Ancaman ini semakin efektif ketika masyarakat memiliki tingkat literasi digital yang rendah.

Kerentanan masyarakat terhadap disinformasi menunjukkan bahwa keamanan siber harus dipahami secara luas, mencakup keamanan informasi dan ketahanan kognitif masyarakat. Masyarakat yang tidak memiliki kemampuan kritis dalam memilah informasi

---

33 *Cyber* Security Awareness Handbook

34 *Muhammad* Wajahat Parvez, "THE IMPACT OF DIGITAL ILLITERACY ON CYBERSECURITY VULNERABILITIES: A DEMOGRAPHIC STUDY IN PAKISTAN," tersedia pada https://jyx.jyu.fi/jyx/Record/jyx_123456789_103514, diakses pada tanggal 30 Januari 2026.

35 *UN* Women and UNU, "Cybersecurity Threats, Vulnerabilities And Resilience Among Women Human Rights Defenders And Civil Society In South-East Asia," tersedia pada https://doi.org/10.17605/OSF.IO/H38WZ, diakses pada tanggal 30 Januari 2026.

36 *Ibid.*

akan lebih mudah terpapar manipulasi digital. Oleh karena itu, ancaman keamanan siber tidak hanya menyerang sistem teknologi, tetapi juga menyerang kemampuan masyarakat dalam memahami dan memproses informasi secara rasional.

Dalam perspektif hukum dan kebijakan, kerentanan masyarakat digital sering kali diperparah oleh kesenjangan antara perkembangan teknologi dan pemahaman hukum masyarakat. Meskipun kerangka regulasi telah berkembang, banyak pengguna teknologi digital yang belum memahami hak dan kewajibannya di ruang siber. Ketidaktahuan ini menjadikan masyarakat berada pada posisi lemah ketika menghadapi ancaman siber, baik sebagai korban maupun sebagai pihak yang secara tidak sadar melanggar norma hukum.

Lebih jauh, ancaman keamanan siber juga berkaitan dengan isu privasi dan perlindungan data pribadi. Dalam masyarakat digital, data pribadi menjadi sasaran utama eksploitasi oleh pelaku kejahatan siber. *Kebocoran data pribadi tidak hanya menimbulkan risiko finansial, tetapi juga mengancam hak privasi, karena data yang tersebar dapat disalahgunakan untuk pemantauan ilegal, penipuan, pemalsuan identitas, pemerasan, hingga doxing oleh pihak yang tidak berwenang.*[37] Kerentanan masyarakat dalam melindungi data pribadi menunjukkan bahwa ancaman siber memiliki sifat berlapis dan jangka panjang.

Dengan demikian, ancaman keamanan siber dan kerentanan masyarakat digital merupakan dua aspek yang saling terkait dan tidak dapat dipisahkan. Ancaman siber terus berkembang seiring dengan kemajuan teknologi, sementara kerentanan masyarakat sering kali meningkat akibat rendahnya kesadaran, literasi, dan kesiapan sosial dalam menghadapi risiko digital. Tanpa upaya sistematis untuk mengurangi kerentanan tersebut, masyarakat akan terus berada dalam posisi defensif dan reaktif terhadap ancaman siber.

Oleh karena itu, pemahaman yang komprehensif mengenai ancaman keamanan siber dan kerentanan masyarakat digital menjadi dasar penting bagi perumusan kebijakan dan strategi keamanan siber yang efektif. Pendekatan yang menempatkan masyarakat sebagai pusat perhatian tidak hanya akan meningkatkan perlindungan individu, tetapi juga memperkuat ketahanan ruang siber secara kolektif. Dalam konteks ini, keamanan siber tidak lagi sekadar isu teknis, melainkan bagian dari upaya membangun masyarakat digital yang aman, berdaya, dan berkeadilan.[38]

3) Urgensi Pendekatan Edukatif dan Partisipatif dalam Keamanan Siber

Perkembangan teknologi informasi yang semakin pesat telah membawa perubahan mendasar dalam cara organisasi mengelola, menyimpan, dan memanfaatkan informasi. Secara keseluruhan, teknologi informasi berperan strategis sebagai penggerak utama transformasi digital dan pengembangan inovasi.[39] Informasi tidak lagi sekadar berfungsi

---

37 *Hisbulloh*, M. H., "Urgensi rancangan undang-undang (RUU) perlindungan data pribadi," *Jurnal Hukum*, Volume 37 No. 2, Desember, hlm. 127, tersedia padahttps://jurnal.unissula.ac.id/index.php/jurnalhukum/article/view/16272/6156, diakses pada tanggal 30 Januari 2026.

38 *Cyber* security awareness handbook

39 *Fatarolius* Harefa & Daniel Hasanema Lase, "Pengaruh Teknologi Informasi Terhadap Transformasi Digital Dan Inovasi Dalam Organisasi. " *IDENTIK: Jurnal Ilmu Ekonomi, Pendidikan dan Teknik ISSN 3063-864X (E)* Volume 02, Nomor 01, Januari 2025.

sebagai pendukung kegiatan operasional, melainkan telah bertransformasi menjadi aset strategis yang menentukan keberlanjutan organisasi, reputasi institusional, serta daya saing di tengah kompetisi global.

Keamanan siber merupakan rangkaian upaya terencana untuk melindungi sistem, jaringan, dan data dari berbagai ancaman digital, seperti peretasan, perangkat lunak berbahaya, dan pencurian data. Urgensi keamanan siber semakin meningkat seiring dengan tingginya ketergantungan masyarakat dan organisasi terhadap teknologi digital. Tanpa sistem perlindungan yang memadai, serangan siber tidak hanya menimbulkan kerugian finansial, tetapi juga berpotensi mengganggu keberlangsungan organisasi, merusak reputasi, serta mengancam keamanan nasional.[40] Dalam konteks tersebut, keamanan siber menjadi aspek yang tidak dapat diabaikan, seiring dengan meningkatnya ancaman siber, kebocoran data, penyalahgunaan informasi, dan berbagai bentuk kejahatan berbasis teknologi digital. Oleh karena itu, strategi implementasi dan pengelolaan keamanan siber perlu dirancang secara sistematis, terstruktur, dan berkelanjutan guna melindungi aset informasi dari berbagai risiko yang mungkin timbul.

Keamanan siber harus dipahami sebagai suatu sistem yang terintegrasi, di mana kebijakan, prosedur, dan teknologi saling melengkapi untuk melindungi aset informasi dari berbagai ancaman, baik yang bersifat internal maupun eksternal.[41] Dengan demikian, pendekatan parsial atau ad hoc dalam pengelolaan keamanan siber tidak lagi memadai untuk menjawab kompleksitas risiko di era digital. Salah satu pendekatan yang secara luas diakui dalam implementasi dan pengelolaan keamanan siber adalah penerapan Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS). ISMS merupakan kerangka kerja yang membantu organisasi mengelola dan melindungi keamanan informasi serta infrastruktur bisnis dari berbagai risiko. ISMS mencakup kebijakan, prosedur, proses, dan pengendalian teknis maupun organisatoris yang diterapkan dalam lingkungan terkontrol dan ditingkatkan secara berkelanjutan, dengan melindungi seluruh elemen system baik sumber daya manusia, perangkat lunak, maupun perangkat keras dari potensi ancaman dan serangan.[42]

Standar internasional yang paling banyak dijadikan acuan dalam implementasi ISMS adalah ISO/IEC 27001.[43] Standar ini menyediakan persyaratan dan panduan bagi organisasi dalam membangun, menerapkan, memelihara, serta meningkatkan sistem manajemen keamanan informasi secara berkelanjutan. ISO/IEC 27001

---

40 *Eko* Budi, et al, "Strategi penguatan cyber securitygunamewujudkan keamanan nasional di era society 5.0. " *Prosiding Seminar Nasional SainsTeknologi Dan Inovasi Indonesia P-ISSN,*Vol. 3 Tahun 2021.

41 Bilqis Aurabillah, "Implementasi Framework Iso 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature Review)," *JATI (Jurnal Mahasiswa Teknik Informatika),* Vol. 8 No. 1, Februari 2024.

42 *Ta-Seen Junaid,* "ISO 27001: Information Security Management Systems," tersedia pada https://www.researchgate.net/profile/Ta-Seen-Junaid/publication/367166657_ISO_27001_Information_Security_Management_Systems/links/63c4e6536fe15d6a5722c964/ISO-27001-Information-Security-Management-Systems.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uRG93bmxvYWQiLCJwcmV2aW91c1BhZ2UiOiJwdWJsaWNhdGlvbiJ9fQ&__cf_chl_tk=g5nSJL1BrSlltT8zwWS_33WB8bEIvMgxk6cKocAUhpE-1769771075-1.0.1.1-VxcnsvtbMvevBz2KZmv9R7HvtO.oXA0G-NPzDdEgWQBU, diakses pada tanggal 30 Januari 2026

43 ISO/IEC, *ISO/IEC 27001: Information Security Management Systems — Requirements*, 2022.

menekankan pendekatan berbasis risiko, di mana organisasi diwajibkan memahami konteks internal dan eksternal, mengidentifikasi aset informasi yang kritis, serta menilai ancaman dan kerentanan yang berpotensi memengaruhi keamanan aset tersebut. Standar ini biasanya menggunakan siklus *Plan–Do–Check–Act* (PDCA) sebagai mekanisme utama untuk memastikan adanya perencanaan yang matang, pelaksanaan yang konsisten, pemantauan berkelanjutan, serta perbaikan terus-menerus dalam pengelolaan keamanan informasi. Siklus PDCA (pada awalnya dikembangkan untuk meningkatkan proses manufaktur, namun kini telah diterapkan secara luas pada berbagai jenis proses, termasuk proses organisasi seperti keamanan informasi. Metode ini pernah menjadi pendekatan wajib dalam penerapan ISO/IEC 27001 versi 2005. Meskipun pada versi 2013 organisasi diberikan fleksibilitas untuk memilih metode peningkatan yang digunakan, PDCA tetap menjadi pendekatan yang paling umum. Hal ini disebabkan oleh sifatnya yang sederhana, mudah dipahami, serta mudah diintegrasikan dengan upaya peningkatan berkelanjutan yang telah berjalan dalam organisasi.[44]

Pada tahap *Plan*, organisasi menetapkan kebijakan keamanan informasi, menentukan ruang lingkup ISMS, serta melakukan penilaian risiko untuk mengidentifikasi ancaman dan kerentanan yang berpotensi menimbulkan dampak signifikan. Tahap *Do* berfokus pada implementasi kebijakan dan kontrol keamanan, termasuk penerapan prosedur operasional, pengamanan teknis, serta peningkatan kesadaran keamanan bagi sumber daya manusia. Selanjutnya, tahap *Check* dilakukan melalui pemantauan dan evaluasi efektivitas ISMS, antara lain dengan audit internal, pengukuran kinerja keamanan, dan peninjauan manajemen. Adapun tahap *Act* diarahkan pada tindakan korektif dan peningkatan berkelanjutan berdasarkan hasil evaluasi dan temuan audit.[45]

Dalam keseluruhan proses implementasi ISMS, manajemen risiko memegang peranan sentral. Keamanan informasi pada hakikatnya tidak bertujuan untuk menghilangkan seluruh risiko, melainkan mengelola risiko pada tingkat yang dapat diterima oleh organisasi. Manajemen risiko keamanan informasi mencakup kegiatan identifikasi, analisis, evaluasi, serta perlakuan risiko secara sistematis. Analisis risiko dalam keamanan informasi harus mempertimbangkan tiga aspek utama, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Ketiga aspek tersebut dirangkum dalam model CIA Triad, yang merupakan kerangka kerja fundamental dalam keamanan informasi yang menjadi acuan bagi organisasi dalam melindungi data serta menjaga sistem informasi agar tetap aman, andal, dan dapat dipercaya.[46]

Selain aspek teknis dan manajerial, keberhasilan pengelolaan keamanan informasi juga sangat ditentukan oleh kebijakan keamanan informasi yang jelas dan terdokumentasi dengan baik. Kebijakan ini mencerminkan komitmen manajemen puncak terhadap perlindungan aset informasi serta menjadi landasan normatif bagi penerapan kontrol keamanan di seluruh organisasi. Kebijakan keamanan informasi yang tidak terdokumentasi dengan baik akan

---

44 Sieuwert Van Otterloo, I"nformation Security and PDCA (Plan-Do-CheckAct)," tersedia pada https://ictinstitute.nl/pdca-plan-do-check-act/, diakses pada tanggal 30 Januari 2026.

45 Peltier, T. R., *Information Security Policies, Procedures, and Standards*, CRC Press, 2016.

46 What is CIA Triad? tersedia pada https://www.geeksforgeeks.org/computer-networks/the-cia-triad-in-cryptography/, diakses pada 30 Januari 2026.

menyulitkan organisasi dalam memastikan konsistensi dan kepatuhan pelaksanaan keamanan informasi. Kebijakan tersebut kemudian diturunkan ke dalam prosedur operasional dan Standar Operasional Prosedur (SOP) yang lebih aplikatif untuk meminimalkan kesalahan manusia sebagai salah satu penyebab utama insiden keamanan informasi.

Di samping itu, pengendalian akses, praktik *secure coding*, penggunaan enkripsi data, serta pengelolaan insiden keamanan informasi merupakan bagian integral dari strategi pengelolaan keamanan informasi yang komprehensif. Seluruh kontrol keamanan tersebut idealnya diterapkan melalui pendekatan *security by design* dan *security by default*, sehingga aspek keamanan telah dipertimbangkan sejak tahap perencanaan hingga penghentian sistem.[47] Meskipun kerangka ISMS dan berbagai kontrol keamanan telah dirancang secara sistematis, tantangan keamanan siber pada level yang lebih luas menunjukkan bahwa ancaman siber tidak semata-mata bersifat teknis. Ancaman tersebut juga berkaitan erat dengan perilaku pengguna, rendahnya kesadaran keamanan digital, serta kurangnya pemahaman masyarakat terhadap risiko hukum dan sosial dari kejahatan siber. Dalam konteks ini lah urgensi pendekatan edukatif dan partisipatif dalam keamanan siber menjadi semakin nyata. Ketergantungan masyarakat terhadap sistem digital dalam berbagai aspek kehidupan menuntut pengembangan *cyber hygiene* nasional yang tidak hanya bertumpu pada regulasi dan teknologi, tetapi juga pada perubahan perilaku dan kesadaran kolektif.

Urgensi edukasi keamanan siber semakin meningkat, khususnya dalam upaya menumbuhkan kesadaran masyarakat akan pentingnya perlindungan data pribadi di tengah meningkatnya kejahatan siber.[48] Edukasi keamanan siber tidak hanya berfungsi untuk meminimalkan potensi kerugian finansial, tetapi juga untuk mencegah dampak psikologis yang kerap muncul akibat pelanggaran privasi dan penyalahgunaan identitas. Melalui pemberian pemahaman dasar mengenai langkah-langkah perlindungan data, masyarakat diharapkan mampu bersikap lebih aman dan bertanggung jawab dalam beraktivitas di ruang digita.[49]

Dengan demikian, pendekatan edukatif menjadi kunci untuk meningkatkan literasi dan kesadaran keamanan siber bagi seluruh lapisan masyarakat. Edukasi keamanan siber tidak cukup dilakukan melalui penyampaian informasi teknis semata, tetapi harus dikaitkan dengan konteks kehidupan sehari-hari, termasuk risiko hukum, perlindungan data pribadi, serta dampak sosial dari penyalahgunaan teknologi digital. Pendekatan ini bertujuan mendorong perubahan perilaku digital yang berkelanjutan, sehingga individu tidak hanya menjadi pengguna pasif teknologi, tetapi subjek yang mampu mengenali risiko, melindungi dirinya, dan bertindak secara bertanggung jawab di ruang siber.

Sejalan dengan itu, pendekatan partisipatif menempatkan masyarakat sebagai aktor

---

47 Widia Febriyani et al, Keamanan Siber, *Melindungi data di dunia digital*, PT Penamuda Media ISBN: 9786347269362, hlm. 104, diakses pada tanggal 30 Januari 2026.

48 Fajri et al, "Pembinaan Masyarakat Melalui Edukasi Bahaya Pinjaman Online Untuk Menghindari Bahaya Kejahatan Siber di Gampong Cot Keumuneng Kecamatan Sawang Kabupaten Aceh Utara," *Jurnal Solusi Masyarakat Dikara*, Vol. *2* No. 3 (2022), 158-165., tersedia pada https://jsmd.dikara.org/jsmd/article/view/47/58, diakses pada tanggal 31 Januari 2026. .

49 Sari, S. D. (2023). Privasi dan Keamanan Data Dalam Statistik Resmi: Tantangan dan Solusi Dalam Perlindungan Data Individu. *Madani: Jurnal Ilmiah Multidisiplin*, *1*(11), 71-83

aktif dalam menjaga keamanan ruang siber. Pengembangan *cyber hygiene* nasional tidak dapat dibebankan semata-mata kepada pemerintah sebagai regulator, melainkan menuntut tanggung jawab bersama yang melibatkan asosiasi industri, sektor swasta, lembaga pendidikan, dan masyarakat sipil. Keterlibatan industri memungkinkan transfer pengetahuan dan praktik terbaik yang relevan dengan perkembangan teknologi, sementara partisipasi masyarakat sipil berperan penting dalam mengartikulasikan kepentingan publik, termasuk perlindungan hak atas privasi dan keamanan informasi.[50]

Pembangunan kesadaran masyarakat melalui pendekatan edukatif dan partisipatif merupakan fondasi penting bagi ketahanan siber nasional. Pendekatan ini tidak hanya memperkuat efektivitas regulasi dan kebijakan keamanan siber, tetapi juga membentuk budaya keamanan digital yang kolektif dan berkelanjutan. Integrasi antara kerangka teknis ISMS, pendekatan berbasis risiko, serta pemberdayaan masyarakat melalui edukasi dan partisipasi aktif akan memperkuat posisi masyarakat sebagai aktor utama dalam menciptakan ruang digital yang aman, terpercaya, dan berkelanjutan.

Dalam kerangka pendekatan edukatif dan partisipatif tersebut, penguatan sumber daya manusia (SDM) keamanan siber menjadi agenda strategis yang tidak dapat ditunda. Ketahanan siber nasional pada hakikatnya sangat bergantung pada kualitas, kuantitas, dan pemerataan kapasitas SDM yang terlibat dalam pengelolaan dan pengamanan ruang digital. Oleh karena itu, diperlukan pembangunan strategi nasional penguatan SDM keamanan siber yang bersifat inklusif dan berkelanjutan. Strategi ini harus mencakup pengembangan pendidikan formal dan vokasi di bidang keamanan siber, penyediaan skema sertifikasi dan pelatihan berkelanjutan bagi aparatur negara, pelaku usaha, serta tenaga teknis, sekaligus pelaksanaan kampanye literasi dan peningkatan kesadaran keamanan siber bagi masyarakat umum secara masif dan berkesinambungan.

Lebih lanjut, strategi penguatan SDM keamanan siber tersebut perlu diperkuat melalui sinergi dan kerja sama lintas pemangku kepentingan. Keterlibatan sektor swasta dan asosiasi industri penting untuk memastikan bahwa kurikulum, pelatihan, dan sertifikasi yang dikembangkan selaras dengan kebutuhan nyata di lapangan dan perkembangan teknologi terkini. Di sisi lain, peran lembaga pendidikan menjadi krusial dalam membangun fondasi pengetahuan, keterampilan, serta etika keamanan siber sejak dini. Tidak kalah penting, kerja sama internasional dengan negara lain dan organisasi global di bidang keamanan siber dapat menjadi sarana transfer pengetahuan, peningkatan kapasitas, serta adopsi praktik terbaik (*best practices*) yang telah terbukti efektif. Melalui pendekatan kolaboratif ini, penguatan SDM keamanan siber tidak hanya berkontribusi pada peningkatan kapasitas teknis, tetapi juga memperkuat budaya keamanan digital nasional yang inklusif, adaptif, dan berdaya saing global.

D. Penutup

Berdasarkan uraian di atas, dapat disimpulkan bahwa keamanan siber tidak lagi semata-mata merupakan isu teknis, melainkan

[50] Cichonski,Paul. *Et. Al*. "NIST, Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology" NIST Special Publication 800-61 Revision 2. Tersedia pada http://dx.doi.org/10.6028/NIST.SP.800-61r2. Diakses pada tanggal 31 Januari 2026.

telah berkembang menjadi isu strategis yang mencakup dimensi manajerial, sosial, dan hukum. Penerapan Sistem Manajemen Keamanan Informasi (SMKI/ISMS) berbasis standar ISO/IEC 27001 dengan pendekatan manajemen risiko menjadi fondasi penting dalam melindungi aset informasi organisasi. Namun demikian, efektivitas perlindungan tersebut sangat ditentukan oleh tingkat kesadaran dan perilaku pengguna sebagai bagian dari ekosistem digital. Dengan demikian, penguatan keamanan siber harus diiringi dengan pembangunan kesadaran masyarakat yang komprehensif, termasuk kesadaran hukum atas hak, kewajiban, serta konsekuensi dari aktivitas di ruang siber.

Dalam konteks tersebut, pembangunan kesadaran hukum masyarakat menjadi elemen krusial untuk mendorong terciptanya budaya keamanan digital yang bertanggung jawab. Masyarakat perlu memahami bahwa setiap aktivitas di ruang digital memiliki implikasi hukum, baik terkait perlindungan data pribadi, penyebaran informasi, maupun potensi pelanggaran hukum lainnya. Kesadaran hukum ini tidak hanya berfungsi sebagai upaya preventif terhadap kejahatan siber, tetapi juga sebagai sarana pemberdayaan masyarakat agar mampu melindungi dirinya secara mandiri.

Lebih lanjut, penguatan kesadaran siber harus memberikan perhatian khusus pada kelompok rentan, khususnya anak-anak, yang merupakan pengguna aktif teknologi digital namun belum memiliki kematangan dalam memahami risiko dan konsekuensi hukum. Dalam hal ini, diperlukan pendekatan yang terintegrasi melalui pendidikan sejak dini, baik di lingkungan keluarga, sekolah, maupun masyarakat, untuk menanamkan nilai-nilai keamanan digital, etika berinternet, serta pemahaman dasar mengenai perlindungan data pribadi. Perlindungan anak di ruang siber tidak hanya menjadi tanggung jawab negara, tetapi juga memerlukan keterlibatan aktif orang tua, pendidik, serta seluruh pemangku kepentingan.

Sejalan dengan hal tersebut, beberapa saran yang dapat diajukan antara lain: Pertama, pemerintah perlu memperkuat kebijakan dan program literasi digital nasional yang secara spesifik mengintegrasikan aspek kesadaran hukum dan perlindungan anak dalam keamanan siber.

Kedua, lembaga pendidikan perlu mengembangkan kurikulum yang memasukkan materi keamanan siber dan etika digital secara sistematis dan berkelanjutan sejak pendidikan dasar. Ketiga, diperlukan kampanye publik yang masif dan berkelanjutan untuk meningkatkan kesadaran masyarakat terhadap risiko siber, dengan pendekatan yang komunikatif dan mudah dipahami oleh berbagai kelompok usia, termasuk anak-anak dan remaja.

Keempat, orang tua dan keluarga perlu didorong untuk berperan aktif dalam mendampingi anak dalam penggunaan teknologi digital, termasuk melalui pengawasan, komunikasi terbuka, dan pemberian pemahaman yang tepat mengenai risiko di ruang siber. Kelima, penguatan kolaborasi antara pemerintah, sektor swasta, lembaga pendidikan, dan masyarakat sipil perlu terus didorong untuk menciptakan ekosistem keamanan siber yang inklusif dan berkelanjutan.

Dengan demikian, integrasi antara pendekatan teknis melalui ISMS, pendekatan berbasis risiko, serta pembangunan kesadaran hukum masyarakat—khususnya bagi anak sebagai generasi digital—akan menjadi kunci dalam mewujudkan ruang siber yang aman, terpercaya, dan berkelanjutan.

Daftar Pustaka

Jurnal

Aurabillah,Bilqis. "Implementasi Framework Iso 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature Review)," *JATI (Jurnal Mahasiswa Teknik Informatika),* Vol. 8 No. 1, Februari 2024.

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

Budi, Eko*. Et al.* "Strategi penguatan cyber securitygunamewujudkan keamanan nasional di era society 5.0. " *Prosiding Seminar Nasional SainsTeknologi Dan Inovasi Indonesia P-ISSN,*Vol. 3 Tahun 2021

Budiyanto, Deny dan Muhammada Mabruri, "Pentingnya Keamanan Siber Dalam Era Digital: Tinjauan Global Dan Kondisi Di Indonesia. " *Prosiding Seminar Nasional Sains dan Teknologi Seri IIIFakultas Sains dan Teknologi, Universitas Terbuka,* Vol. 2 No. 1(2025)e. T Tersedia pada https://conference.ut.ac.id/index.php/saintek/article/view/5134#pkp_content_main, diakses pada tanggal 29 Januari 2026.

Caramancion Kevin. *Et al.* "The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. College of Emergency Preparedness, Homeland Security, and Cybersecurity," *University at Albany, State University of New York, Albany, NY 12222, US.* Tersedia pada, **https://doi.org/10.3390/data7040049**. Diakses pada tanggal 29 Januari 2026.

Cichonski,Paul. *Et. Al*. "NIST, Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology" NIST Special Publication 800-61 Revision 2. Tersedia pada http://dx.doi.org/10.6028/NIST.SP.800-61r2. Diakses pada tanggal 31 Januari 2026.

CISO JIL Information Technology limited. "Cyber Security Awareness Handbook". Tersedia pada https://www.jiit.ac.in/sites/default/files/Cyber%20Security%20Awareness%20Hand%20Book.pdf, diakses pada tanggal 28 Januari 2026.

Ernis,Yul. "Implikasi Penyuluhan Hukum Langsung terhadap Peningkatan Kesadaran Hukum Masyarakat." *Jurnal Penelitian Hukum De Jure*. Tersedia pada https://doi.org/10.30641/dejure.2018.V18.477-496. Diakses pada tanggal 28 Januari 2026.

Fajri**,** Muhammad Daud Mursalin& Muhammad Ali. Pembinaan Masyarakat Melalui Edukasi Bahaya Pinjaman Online Untuk Menghindari Bahaya Kejahatan Siber di Gampong Cot Keumuneng Kecamatan Sawang Kabupaten Aceh Utara. *Jurnal Solusi Masyarakat Dikara*. Vol 2 Nomor 3 158-165. Tersedia pada https://jsmd.dikara.org/jsmd/article/view/47/58, diakses pada tanggal 31 Januari 2026.

Harefa *Fatarolius* & Daniel Hasanema Lase, "Pengaruh Teknologi Informasi Terhadap Transformasi Digital Dan Inovasi Dalam Organisasi.**"** *IDENTIK: Jurnal Ilmu Ekonomi, Pendidikan dan Teknik ISSN 3063-864X (E)* . Volume 02, Nomor 01, Januari 2025.

Hisbulloh, M. H., "Urgensi rancangan undang-undang (RUU) perlindungan data pribadi," *Jurnal Hukum*,

Huda, Nailul Huda, Dyah Ayu dan Rani Septyarini, Outlook Ekonomi Digital 2025, Center of Economic and Law Studies (CELIOS) Jakarta, Indonesia

ISO/IEC, *ISO/IEC 27001: Information Security Management Systems — Requirements*, 2022.

Joshi, Renu. *Et al*. "Internet an integral part of human life in 21st century: a review." *Current Journal of Applied Science and Technology,* Vol. 41.issue 36 (2022). Hlm. 12-18, tersedia https://doi.org/10.9734/cjast/2022/v41i363963, diakses pada 28 Januari 2026.

Judith Hahn, "Foundations of a Sociology of Canon Law. "T*he Effectiveness of the Law Chapter 6*. Springer Nature Link, diakses pada 29 Januari 2026.

Loannis Stylianou. *Et. Al*. "Suspicious minds: Psychological techniques correlated with online phishing attacks. Contents lists available at ScienceDirect Computersin Human Behavior Reports journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports . Diakses pada tangal

M. Khusnul Khuluq, "Hukum dan Kesadaran Hukum: Dari Teori E. Ehrlich Hingga Habermas." Tersedia pada https://marinews.mahkamahagung.go.id/

artikel/hukum-dan-kesadaran-hukum-dari-teori-e-ehrlich-0pP, diakses pada tanggal 28 Januari 2026.

Marune Sahat A. E. M., Brandon Hartanto, "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective, " *International Journal of Business, Economics and Social Development,* Vol. 2, No. 4, pp. 143-152, 2021,

Mohammad Taufik Hidayatuloh, "Kedaulatan Informasi dan Integritas Profesional: Analisis Holistik Perlindungan Rahasia Dagang dalam Industri Teknologi Informasi di Indonesia." Tersedia pada https://www.researchgate.net/publication/398870025_Kedaulatan_Informasi_dan_Integritas_Profesional_Analisis_Holistik_Perlindungan_Rahasia_Dagang_dalam_Industri_Teknologi_Informasi_di_Indonesia/link/694560810c98040d481ef02c/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19. Diakses pada tanggal 29 Januasri 2026.

Nova, Nabilla Ivana Nova, Sela Nabila , Parid Rehan Paiza , Norita Sinaga "Analisis Keamanan Sistem Pembayaran Digital terhadap Perlindungan Data Pengguna", *Department of Digital Business Journal of Artificial Intelligence and Digital Business (RIGGS)* , Vol. 4 No. 4 (2026), hlm. 8985-8991, tersedia https://journal.ilmudata.co.id/index.php/RIGGS .

Parvez Muhammad Wajahat, "The Impact Of Digital Illiteracy On Cybersecurity Vulnerabilities: A Demographic Study In Pakistan." Tersedia pada https://jyx.jyu.fi/jyx/Record/jyx_123456789_103514. Diakses pada tanggal 30 Januari 2026.

Peltier, R, Thomas. "Information Security Policies, Procedures, and Standard." Tersedia pada https://doi.org/10.1201/9780849390326.

Purba, R. E., D. Maharani, M. A. A. BMY, and R. Z. Al Zahra. "Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital." *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora* 2, No. 2 (2024): 167–176

Sadeli Annisa Fajriyati &Indira Irawati. "Awareness o f Personal Data Protection Law In Concern To Literacy, " *Jurnal Kajian Informasi & Perpustakaan,* Vol. 11, No. 2 (2023), tersedia pada https://jurnal.unpad.ac.id/jkip/article/view/47526, diakses pada tanggal 28 Januari 2026.

Sari, S. D. (2023). Privasi dan Keamanan Data Dalam Statistik Resmi: Tantangan dan Solusi Dalam Perlindungan Data Individu. *Madani: Jurnal Ilmiah Multidisiplin*, *1*(11), 71-83

Sharma, Swapnil. *Et al*. "Digital citizen empowerment: A systematic literature review of theories and development models. Information Technology for Development." Tersedia pada https://doi.org/10.1080/02681102.2022.2046533. Diakses pada tanggal 29 Januari 2026.

Sieuwert Van Otterloo, "Information Security and PDCA (Plan-Do-CheckAct). " Tersedia pada https://ictinstitute.nl/pdca-plan-do-check-act/. Diakses pada tanggal 30 Januari 2026.

SO JIL INFORMATION TECHNOLOGYLIMITED, Cyber Security Awareness Handbook.

Stylianou Ioannis. *Et al* . "Suspicious minds: Psychological techniques correlated with online phishing." *Computersin Human Behavior Reports*. Tersedia pada Journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports, diakses pada tanggal 29 Januari 2026.

Ta-Seen Junaid, "ISO 27001: Information Security Management Systems." Tersedia pada https://www.researchgate.net/profile/Ta-Seen-Junaid/publication/367166657_ISO_27001_Information_Security_Management_Systems/links/63c4e6536fe15d6a5722c964/ISO-27001-Information-Security-Management-Systems.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uRG93bmxvYWQiLCJwcmV2aW91c1BhZ2UiOiJwdWJsaWNhdGlvbiJ9fQ&__cf_chl_tk=g5nSJL1BrSlltT8zwWS_33WB8bEIvMgxk6cKocAUhpE-1769771075-1.0.1.1-VxcnsvtbMvevBz2KZmv9R7HvtO.oXA0GNPzDdEgWQBU. Diakses pada tanggal 30 Januari 2026.

UN Women and UNU, "Cybersecurity Threats, Vulnerabilities And Resilience Among Women Human Rights Defenders And Civil Society In South-East Asia. " Tersedia pada https://doi.org/10.17605/OSF.IO/H38WZ. Diakses pada tanggal 30 Januari 2026.

Widia Febriyani . *Et al*. *Keamanan Siber, Melindungi data di dunia digital*, PT Penamuda Media ISBN: 9786347269362. Tersedia pada https://www.researchgate.net/

publication/395935100_KEAMANAN_SIBER_MELINDUNGI_DATA_DI_DUNIA_DIGITAL/link/68d8f714220a341aa1505a2b/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19. Diakses pada tanggal 30 Januari 2026.

Yenny Aman Seah. *Et al*. *"*Raising Public Legal Awareness in the Digital Age*)," Journal of Law and Legal Reform,* Vol. 6 Issue 1 (2025), hlm. 209-238. Tersedia pada https://doi.org/10.15294/jllr.v6i1.68129. Diakses pada tanggal 29 Januari 2026.

Peraturan Perundang-undangan

Undang-Undang tentang Informasi dan Transaksi Elektronik, UU Nomor 11 Tahun 2008, LN Tahun 2008 No.58, TLN No. 4843 sebagiaimana terkahir diubah oleh UU Nomor 1 Tahun 2024 tentang Perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, LN Tahun 2024 No. 6905 selanjutnya disebut UU ITE.

Undang-Undang tentang Perlindungan Data Pribadi, UU Nomor 27 Tahun 2022, LN Tahun 2022 No, 196, TLN No. 6829.

Peraturan Presiden tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, Perpres Nomor 47 Tahun 2023, LN Tahun 2023 No. 99.

Internet

What is CIA Triad?. Tersedia pada https://www.geeksforgeeks.org/computer-networks/the-cia-triad-in-cryptography/. diakses pada 30 Januari 2026.