JURNAL HUKUM SEHASEN
p-ISSN : 2528-5025
e-ISSN : 2746-6485

Regulation Of Cybersecurity Technology As An Effort To Address Security Threats To Privacy In The Digital Era

Regulasi Teknologi Keamanan Siber Sebagai Upaya Mengatasi Ancaman Keamanan Bagi Privasi Di Era Digital

Agustinus Wempy[1], Zaenal Efendi[2], Marsudi Dedi Putra[3]
[1,2,3)]Pascasarjana Universitas Wisnuwardhana Malang, Malang, Indonesia
Email: [1] agustinuswempy@gmail.com, [2] zaenalefendisg@gmail.com, [3] marsudiputra1976@gmail.com

ARTICLE HISTORY
Received [23 July 2024]
Revised [30 Sept 2024]
Accepted [10 Oct 2024]

KEYWORDS
Regulation, Technology, Cybersecurity, Privacy

ABSTRAK

Cybersecurity technology regulations play a key role in ensuring adequate protection of individual data privacy in an increasingly complex digital era. In the context of the collection, use, and dissemination of personal data by various entities, these regulations provide a foundation for governing practices related to data privacy. Through regulations such as the General Data Protection Regulation (GDPR) in the European Union, stringent standards are enforced to protect personal data and grant individuals control over their data. Transparency, restrictions on data use and access, and the implementation of robust data security measures are key aspects of this regulation. Additionally, law enforcement and sanctions for data privacy violations are integral parts of effective cybersecurity regulations. Thus, cybersecurity technology regulations aim to create a safe and trustworthy digital environment where individual data privacy is respected and optimally protected.

ABSTRACT

Regulasi Teknologi Keamanan Siber memainkan peran kunci dalam memastikan perlindungan yang memadai terhadap privasi data individu di era digital yang semakin kompleks. Dalam konteks pengumpulan, penggunaan, dan penyebaran data pribadi oleh berbagai entitas, regulasi tersebut menjadi landasan untuk mengatur praktik-praktik yang berkaitan dengan privasi data. Melalui regulasi seperti General Data Protection Regulation (GDPR) di Uni Eropa, standar yang ketat ditegakkan untuk melindungi data pribadi dan memberikan hak kontrol kepada individu terkait data mereka. Transparansi, pembatasan penggunaan dan akses data, serta penerapan keamanan data yang kuat menjadi poin-poin kunci dalam regulasi ini. Selain itu, penegakan hukum dan sanksi bagi pelanggaran privasi data merupakan bagian integral dari regulasi keamanan siber yang efektif. Dengan demikian, regulasi teknologi keamanan siber bertujuan untuk menciptakan lingkungan digital yang aman dan terpercaya, di mana privasi data individu dihormati dan dilindungi secara optimal.

PENDAHULUAN

Regulasi teknologi keamanan siber haruslah menyediakan kerangka kerja yang kuat dan holistik untuk melindungi data pribadi, mencegah serangan siber, menegakkan standar keamanan yang tinggi, dan mempromosikan kerjasama internasional dalam mengatasi ancaman keamanan siber. Di era digital saat ini, teknologi telah menjadi bagian integral dari kehidupan sehari-hari. Teknologi informasi dan komunikasi (TIK) telah mengubah cara kita bekerja, berinteraksi, dan bahkan berpikir. Tatanan ideal regulasi teknologi keamanan siber harus menciptakan lingkungan yang aman dan terpercaya bagi individu, perusahaan, dan negara. Regulasi yang efektif harus memperkuat perlindungan data pribadi, mempromosikan kesadaran dan pendidikan keamanan siber, menegakkan standar keamanan yang tinggi, dan mendorong kerjasama internasional dalam mengatasi ancaman keamanan siber secara global. Dengan demikian, regulasi tersebut dapat membantu mengatasi tantangan dan risiko yang terkait dengan teknologi keamanan siber di era digital yang terus berkembang.Kondisi objektif regulasi teknologi keamanan siber saat ini sangatlah kompleks dan terus berubah seiring dengan perkembangan teknologi dan ancaman siber yang baru muncul. Beberapa hal yang dapat diidentifikasi sebagai kondisi objektif saat ini termasuk: (a) keragaman regulasi. Terdapat keragaman regulasi di berbagai negara dan yurisdiksi terkait teknologi keamanan siber. Beberapa negara telah mengadopsi kerangka kerja yang komprehensif untuk melindungi data dan infrastruktur digital, sementara yang lain masih dalam proses pengembangan regulasi yang sesuai. (b) Ketidakseimbangan antara perkembangan teknologi dan regulasi: Perkembangan teknologi cenderung lebih cepat daripada pembuatan regulasi yang relevan. Ini menciptakan ketidakseimbangan di mana teknologi baru, seperti kecerdasan buatan dan komputasi awan, dapat memiliki dampak signifikan pada keamanan siber sebelum regulasi yang sesuai dapat

diterapkan. (c) perlindungan data pribadi yang beragam. Sejumlah negara telah mengadopsi undang-undang perlindungan data pribadi yang ketat, seperti GDPR di Uni Eropa, sementara negara lain memiliki regulasi yang lebih longgar atau bahkan belum memiliki regulasi khusus mengenai perlindungan data pribadi. Dengan memahami kondisi objektif saat ini, penting bagi regulator, organisasi, dan masyarakat untuk terus memperbarui dan meningkatkan kerangka kerja regulasi teknologi keamanan siber agar dapat mengatasi ancaman dan risiko yang terus berkembang dalam dunia digital yang terus berubah.Berbagai peraturan perundang-undangan telah dibuat oleh negara Indonesia dalam mengatur teknologi keamanan siber, antara lain: (1) UU 9 Tahun 2016 tentang Informasi dan Transaksi Elektronik, (2) Peraturan Pemerintah 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan dalam bentuk undang-undang dan turunannya mempertegas perlunya keamanan siber nasional sebagai landasan bertindak bagi para pemangku kepentingan dan penyelenggara negara dalam mewujudkan stabilitas dan kapasitas terhadap keamanan siber.Namun, terdapat beberapa kelemahan pada kedua undang-undang tersebut. Salah satu kelemahan dari Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik adalah ketidakjelasan dalam definisi dan ruang lingkup yang menyebabkan tumpang tindih dengan undang-undang lain, seperti Undang-Undang Perlindungan Data Pribadi. Selain itu, UU ini juga dinilai kurang memberikan perlindungan yang memadai terhadap privasi dan keamanan data pribadi pengguna, serta belum memberikan arahan yang cukup jelas dalam mengatasi tantangan keamanan siber yang semakin kompleks. Pada Peraturan Pemerintah 71/2019, ditemukan kelemahan kurangnya ketegasan dalam penerapan standar keamanan dan privasi data. Regulasi ini juga tidak memberikan pedoman yang cukup jelas mengenai perlindungan hak privasi pengguna dan tata cara penanganan pelanggaran data. Selain itu, PP ini kurang memperhatikan aspek keterbukaan dan transparansi dalam penyelenggaraan sistem dan transaksi elektronik. Hal ini dapat mengakibatkan risiko keamanan data dan privasi yang lebih tinggi bagi pengguna.Tidak adanya tindakan untuk melakukan perubahan regulasi yang mengatur teknologi keamanan siber saat ini dapat mengakibatkan sejumlah bahaya dan konsekuensi yang serius, baik bagi individu, perusahaan, maupun masyarakat secara keseluruhan. Tanpa peraturan yang diperbarui dan diperkuat, pelaku kejahatan siber akan terus mengembangkan teknik serangan baru dan memanfaatkan kerentanan yang ada di dalam sistem. Ini dapat mengakibatkan peningkatan frekuensi dan kompleksitas serangan siber yang dapat merugikan perusahaan dan individu. Tanpa regulasi yang jelas dan diperkuat, penegakan hukum terhadap pelanggaran keamanan siber menjadi lebih sulit. Penegak hukum membutuhkan kerangka kerja hukum yang kuat untuk menindak pelaku kejahatan siber dan menjamin pertanggungjawaban mereka. Pelanggaran data yang terjadi secara terus-menerus dapat mengakibatkan kerugian kepercayaan publik terhadap organisasi dan lembaga yang tidak mampu melindungi data pengguna mereka dengan baik. Ini dapat mengganggu hubungan antara konsumen dan perusahaan serta antara warga dan pemerintah. Tidak melakukan perubahan dalam regulasi teknologi keamanan siber dapat berakibat pada konsekuensi yang serius dan merugikan bagi individu, perusahaan, dan masyarakat secara keseluruhan. Oleh karena itu, sangat penting untuk terus memperbarui dan memperkuat regulasi yang mengatur keamanan siber untuk mengatasi ancaman yang terus berkembang dalam lingkungan digital yang semakin kompleks ini.

LANDASAN TEORI

Konsep Dasar Regulasi Keamanan Siber

Regulasi keamanan siber merupakan serangkaian aturan dan pedoman yang dirancang untuk melindungi sistem informasi dari ancaman dan serangan siber. Menurut A. Alharkan dan S. Alnasseri (2020), regulasi ini mencakup berbagai aspek mulai dari pengaturan standar keamanan teknis hingga kebijakan penegakan hukum yang mengatur tanggung jawab dan hak-hak pengguna serta penyedia layanan (Alharkan & Alnasseri, 2020). Regulasi ini bertujuan untuk mengurangi risiko serangan siber, meningkatkan kesadaran akan praktik keamanan terbaik, dan memastikan perlindungan data pribadi.

Pentingnya Regulasi dalam Perlindungan Privasi

Dalam konteks privasi, regulasi berfungsi untuk melindungi data pribadi dari pengumpulan, penggunaan, dan penyebaran yang tidak sah. Regulasi seperti General Data Protection Regulation (GDPR) di Uni Eropa telah menjadi model penting dalam hal ini. Menurut A. Greenleaf (2021), GDPR dan undang-undang serupa di berbagai negara menetapkan prinsip-prinsip utama seperti transparansi, akuntabilitas, dan hak akses individu terhadap data mereka, yang memberikan perlindungan tambahan terhadap privasi di era digital (Greenleaf, 2021).

Pendekatan dalam Pengembangan Regulasi

Pengembangan regulasi keamanan siber dan perlindungan privasi sering melibatkan pendekatan berbasis risiko dan berbasis prinsip. Pendekatan berbasis risiko, seperti yang dibahas oleh A. Karami dan

M. Ayub (2022), menekankan pada identifikasi dan mitigasi risiko yang spesifik terhadap ancaman siber. Regulasi ini memerlukan evaluasi risiko yang terus-menerus dan penerapan langkah-langkah pengamanan yang sesuai untuk mengatasi ancaman yang berkembang (Karami & Ayub, 2022). Sementara itu, pendekatan berbasis prinsip, seperti diuraikan oleh S. O'Rourke (2021), berfokus pada penerapan prinsip-prinsip umum seperti perlindungan data pribadi dan hak atas privasi, yang dapat diterapkan secara luas di berbagai konteks dan situasi (O'Rourke, 2021).

Kolaborasi Internasional dan Standar Global

Kolaborasi internasional dalam regulasi keamanan siber menjadi semakin penting mengingat sifat global dari ancaman siber. Menurut H. Deibert et al. (2023), standar global dan perjanjian internasional seperti Konvensi Budapest tentang Kejahatan Siber memainkan peran penting dalam harmonisasi peraturan dan penegakan hukum di tingkat global. Kolaborasi ini membantu negara-negara untuk berbagi informasi, teknologi, dan praktik terbaik dalam mengatasi ancaman siber secara lebih efektif (Deibert et al., 2023).

Tantangan dan Arah Masa Depan

Tantangan utama dalam regulasi keamanan siber dan perlindungan privasi termasuk kecepatan perkembangan teknologi dan perbedaan antara sistem hukum di berbagai negara. K. Smith dan J. F. Johnson (2024) menyarankan bahwa regulasi harus adaptif dan responsif terhadap perubahan teknologi yang cepat, serta mempertimbangkan perbedaan budaya dan hukum dalam penerapan regulasi (Smith & Johnson, 2024). Selain itu, pendekatan proaktif yang melibatkan stakeholder dari berbagai sektor dapat meningkatkan efektivitas regulasi.

METODE PENELITIAN

Metode penelitian hukum normatif untuk judul "Regulasi Teknologi Keamanan Siber dalam Mengatasi Ancaman Keamanan dan Privasi di Era Digital" akan berfokus pada analisis dokumen hukum yang berlaku dan pengembangan argumen hukum berdasarkan norma-norma yang terkandung di dalamnya.Pendekatan perundang-undangan dipergunakan dalam penelitian ini, untuk mengidentifikasi undang-undang, peraturan pemerintah, kebijakan, dan instrumen hukum lainnya yang berkaitan dengan regulasi teknologi keamanan siber dan perlindungan privasi data di era digital. Pendekatan konsep dipergunakan untuk mendekati dan menganalisis teks dari regulasi yang relevanuntuk memahami secara mendalam ketentuan-ketentuan yang berkaitan dengan keamanan siber dan privasi data. Ini meliputi mengidentifikasi definisi, kewajiban, hak, dan prosedur yang terkandung di dalamnya. Selanjutnya dilakukan penafsiran hukum terhadap ketentuan-ketentuan dalam regulasi tersebut berdasarkan prinsip-prinsip hukum yang berlaku, doktrin hukum terkait.Analisis dilakukan melalui yuridis deskriptif. Dengan analisis yuridis deskriptif, penelitian akan memberikan pemahaman yang komprehensif tentang kerangka hukum yang mengatur teknologi keamanan siber serta memberikan pandangan yang jelas tentang upaya yang perlu dilakukan untuk meningkatkan perlindungan keamanan dan privasi di era digital.

HASIL DAN PEMBAHASAN

Peran Regulasi Teknologi Keamanan Siber Untuk Mengatasi Ancaman Keamanan Siber di Era Digital

Di era digital saat ini, ancaman keamanan siber menjadi semakin kompleks dan beragam. Dalam konteks ini, peran regulasi dalam menghadapi ancaman keamanan siber menjadi sangat penting. Regulasi memberikan kerangka kerja hukum yang memandu organisasi dan perusahaan dalam melindungi sistem dan data mereka dari serangan siber. Peran regulasi di Indonesia dalam menghadapi ancaman keamanan siber di era digital menjadi sangat penting dalam menjaga stabilitas dan keamanan ekosistem digital.Meskipun regulasi memiliki peran penting dalam menghadapi ancaman keamanan siber, namun masih ada tantangan dalam implementasinya. Perubahan teknologi yang cepat dan taktik baru yang digunakan oleh penyerang memerlukan regulasi yang terus diperbarui dan diperkuat untuk tetap relevan dan efektif. Selain itu, penegakan regulasi juga memerlukan sumber daya yang cukup dan kerjasama antara semua pemangku kepentingan terkait. Ancaman ini meliputi serangan malware, phishing, ransomware, serangan DDoS, dan banyak lagi. Tantangan tersebut semakin rumit dengan cepatnya perkembangan teknologi, kehadiran Internet of Things (IoT), dan meningkatnya konektivitas digital.Salah satu contoh serangan malware yang terkenal adalah serangan ransomware WannaCry yang terjadi pada tahun 2017. Serangan ini menginfeksi sistem komputer dengan menggunakan exploit Eternal Blue, sebuah kerentanan dalam sistem operasi Windows yang belum diperbaiki. Setelah berhasil

menginfeksi, WannaCry mengenkripsi file-file penting pada komputer korban dan meminta tebusan (ransom) dalam bentuk mata uang digital Bitcoin agar file-file tersebut dapat dikembalikan.Serangan ini sangat merugikan karena menyerang sistem-sistem kritis seperti rumah sakit, institusi keuangan, dan perusahaan besar di seluruh dunia. Banyak organisasi terpaksa menghentikan operasi mereka karena data mereka tidak dapat diakses akibat enkripsi oleh malware ini. Selain itu, serangan WannaCry juga menunjukkan kemampuan untuk menyebar secara cepat melalui jaringan yang terhubung, membuatnya menjadi salah satu serangan ransomware terbesar yang pernah terjadi. Salah satu contoh serangan DDoS (*Distributed Denial of Service*) yang terkenal adalah serangan terhadap layanan perbankan online pada tahun 2012 yang disebut serangan "Operation Ababil". Serangan ini dilakukan oleh kelompok hacker yang mengidentifikasi diri sebagai "Izz ad-Din al-Qassam Cyber Fighters".Pada saat serangan terjadi, layanan perbankan online dari beberapa bank besar di Amerika Serikat mengalami gangguan berat. Serangan dilakukan dengan cara mengirimkan lalu lintas data yang sangat besar secara bersamaan ke server-server perbankan, menyebabkan server-server tersebut menjadi kelebihan beban dan tidak mampu menangani permintaan layanan dari pengguna yang sah.Akibat dari serangan DDoS ini, layanan perbankan online menjadi tidak dapat diakses oleh pengguna yang sah selama beberapa jam atau bahkan beberapa hari, menyebabkan gangguan besar-besaran pada aktivitas perbankan dan transaksi keuangan. Selain itu, serangan ini juga menimbulkan kerugian finansial yang signifikan bagi bank-bank yang menjadi target serangan.Serangan phishing yang terjadi di Indonesia adalah serangan phishing yang menyamar sebagai layanan perbankan online. Dalam serangan ini, para penyerang akan mengirimkan email atau pesan teks yang menyerupai komunikasi resmi dari bank-bank ternama di Indonesia kepada korban potensial. Pesan tersebut mungkin berisi pemberitahuan palsu tentang masalah keamanan atau permintaan untuk memperbarui informasi akun.Alam email atau pesan teks tersebut, seringkali disertakan tautan yang mengarah ke situs web palsu yang dirancang sedemikian rupa untuk meniru tampilan situs resmi bank. Korban yang tertipu kemudian diminta untuk memasukkan informasi pribadi seperti nomor rekening, kata sandi, dan kode keamanan ke dalam formulir yang disediakan di situs palsu tersebut.Setelah mendapatkan informasi sensitif dari korban, para penyerang kemudian dapat menggunakan informasi tersebut untuk melakukan penipuan, pencurian identitas, atau akses ilegal ke akun bank korban. Serangan phishing semacam ini dapat menyebabkan kerugian finansial dan kerugian reputasi bagi korban yang terkena dampaknya.Penting bagi pengguna internet di Indonesia untuk selalu waspada terhadap serangan phishing dengan memeriksa keaslian email atau pesan teks yang mereka terima, tidak mengklik tautan yang mencurigakan, dan tidak memberikan informasi sensitif melalui email atau pesan teks tanpa verifikasi yang jelas. Selain itu, bank dan lembaga keuangan juga harus terus memberikan edukasi kepada pelanggan mereka tentang cara mengidentifikasi dan mencegah serangan phishing.

Berikut tabel 1 yang memperlihtakan ancaman dari serangan malware, DDoS, dan phishing beserta deskripsi singkat tentang masing-masing ancaman:

Tabel 1 Ancaman Dari Serangan Malware, Ddos, Dan Phishing

Jenis Serangan	Deskripsi Ancaman
Malware	Jenis serangan yang mencakup berbagai macam program jahat yang dirancang untuk merusak, mengganggu, atau mencuri data dari sistem komputer korban. Malware dapat berupa virus, worm, trojan, ransomware, dan lain sebagainya. Ancaman dari malware termasuk kehilangan data penting, kerusakan sistem, pencurian identitas, dan pemerasan.
DDoS	Serangan Denial of Service (DDoS) adalah serangan yang bertujuan untuk membuat layanan atau sistem menjadi tidak tersedia bagi pengguna yang sah dengan menghambat akses ke layanan tersebut. Penyerang menggunakan jaringan komputer yang terdistribusi untuk mengirimkan lalu lintas data yang sangat besar ke server atau infrastruktur target, menyebabkan server menjadi kelebihan beban dan tidak dapat merespons permintaan layanan dari pengguna yang sah. Ancaman dari serangan DDoS termasuk kerugian finansial, penurunan produktivitas, dan kerusakan reputasi.
Phishing	Phishing adalah serangan yang mencoba untuk memperoleh informasi sensitif seperti nama pengguna, kata sandi, atau informasi finansial dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik. Serangan phishing seringkali dilakukan melalui email, pesan teks, atau media sosial. Ancaman dari serangan phishing termasuk pencurian identitas, penipuan keuangan, dan akses ilegal ke akun pengguna.

JURNAL HUKUM SEHASEN
p-ISSN : 2528-5025
e-ISSN : 2746-6485

Tabel 1 di atas memberikan gambaran singkat tentang ancaman dari masing-masing serangan dan dampak potensial yang dapat timbul dari serangan tersebut. Penting bagi organisasi dan individu untuk memahami ancaman ini dan mengambil langkah-langkah pencegahan yang sesuai untuk melindungi diri mereka dari serangan malware, DDoS, dan phishing.

Beberapa aspek yang perlu dipertimbangkan dalam pembahasan peran regulasi dalam menghadapi ancaman keamanan siber di era digital: (a) penetapan standar keamanan: Regulasi biasanya menetapkan standar keamanan yang harus dipatuhi oleh organisasi. Standar ini mencakup berbagai aspek keamanan, seperti enkripsi data, pemantauan keamanan secara terus-menerus, manajemen akses yang ketat, dan kebijakan keamanan yang berlaku. Dengan adanya regulasi ini, organisasi memiliki panduan yang jelas tentang langkah-langkah yang harus diambil untuk melindungi sistem dan data mereka. (b) perlindungan data pribadi: Banyak regulasi teknologi keamanan siber juga mengatur perlindungan data pribadi pengguna. Misalnya, General Data Protection Regulation (GDPR) di Uni Eropa mengatur bagaimana data pribadi pengguna harus dikelola dan dilindungi oleh organisasi. Regulasi semacam ini mendorong organisasi untuk memperlakukan data pribadi dengan sangat hati-hati dan mengambil langkah-langkah yang tepat untuk melindunginya dari akses yang tidak sah. (c) pengaturan dan penegakan hukum: Regulasi juga seringkali menyertakan sanksi bagi pelanggaran keamanan siber. Ini dapat berupa denda yang signifikan atau sanksi hukum lainnya. Tujuan dari sanksi ini adalah untuk mendorong organisasi untuk mengambil keamanan siber dengan serius dan mematuhi standar keamanan yang ditetapkan oleh regulasi. (d) pengembangan kerjasama dan kolaborasi: Regulasi juga dapat mendorong kerjasama dan kolaborasi antara pemerintah, sektor swasta, dan lembaga lainnya dalam menghadapi ancaman keamanan siber. Ini menciptakan ekosistem yang lebih kuat dalam memerangi serangan siber dan berbagi informasi tentang ancaman yang muncul. Dengan adanya kerjasama ini, semua pihak dapat saling mendukung dalam upaya melindungi infrastruktur digital.

Melalui peran regulasi ini, Indonesia dapat lebih siap dan tanggap dalam menghadapi ancaman keamanan siber di era digital. Namun, penting untuk terus melakukan evaluasi dan perbaikan terhadap regulasi yang ada agar tetap relevan dengan perkembangan teknologi dan kebutuhan masyarakat. Kolaborasi antara pemerintah, sektor swasta, dan lembaga lainnya juga perlu ditingkatkan untuk memastikan bahwa upaya perlindungan keamanan siber berjalan efektif dan efisien.

Terobosan Regulasi Yang Ideal Dalam Menghadapi Penyebaran Data Pribadi di Lingkungan Digital

Dalam era digital yang terus berkembang, penyebaran data pribadi oleh berbagai entitas dalam lingkungan digital menjadi semakin kompleks dan berpotensi mengancam privasi individu. Oleh karena itu, terobosan regulasi yang ideal menjadi sangat penting untuk menghadapi tantangan ini. aspek yang harus dipertimbangkan dalam merancang regulasi yang ideal untuk masa yang akan datang dalam menghadapi penyebaran data pribadi oleh berbagai entitas dalam lingkungan digital

Dalam merancang regulasi yang ideal untuk masa yang akan datang dalam menghadapi penyebaran data pribadi oleh berbagai entitas dalam lingkungan digital, nampak pada tabel 2 di bawah ini.

Tabel 2. Rancangan Regulasi dalam Meghadapi Penyebaran Data Pribadi oleh Berbagai Entitas pada Lingkungan Digital

No.	Aspek Regulasi	Deskripsi
	Definisi Data Pribadi	Memberikan definisi yang jelas dan komprehensif tentang apa yang dimaksud dengan "data pribadi"
	Prinsip Perlindungan Data	Menetapkan prinsip-prinsip perlindungan data yang kuat, seperti keterbukaan, transparansi, pengendalian oleh pemilik data, dan hak untuk dilupakan (*right to be forgotten*)
	Penegakan Hukum	Menyertakan mekanisme penegakan hukum yang efektif, termasuk sanksi yang tegas bagi pelanggar data, audit reguler, dan kewajiban pelaporan pelanggaran data
	Keterlibatan Pihak Ketiga	Mengatur keterlibatan pihak ketiga dalam pengelolaan data pribadi dengan mendorong adopsi praktik terbaik dalam perlindungan data
	Pendekatan Berbasis Risiko	Menerapkan pendekatan berbasis risiko dalam manajemen data pribadi untuk mengevaluasi risiko dan menerapkan langkah-langkah perlindungan yang sesuai
	Kolaborasi Internasional	Mempromosikan kolaborasi internasional dalam perlindungan data pribadi melalui pertukaran informasi dan praktik terbaik antar negara

	Pendidikan dan Kesadaran Masyarakat	Menyertakan upaya pendidikan dan kesadaran masyarakat tentang pentingnya perlindungan data pribadi dan hak individu terkait data mereka
	Inovasi Teknologi yang Berkelanjutan	Mendukung inovasi teknologi yang berkelanjutan sambil memperhitungkan keamanan dan privasi data pribadi
	Keterbukaan dan Transparansi	Memastikan keterbukaan dan transparansi dalam praktik pengelolaan data pribadi, termasuk keterbukaan tentang cara data dikumpulkan, disimpan, dan digunakan
0	Evaluasi dan Revisi Rutin	Mengatur evaluasi dan revisi rutin terhadap keefektifan regulasi, dengan mempertimbangkan perkembangan teknologi dan tren ancaman keamanan

Tabel ini membantu dalam menyusun rancangan regulasi yang komprehensif dan terstruktur untuk mengatasi penyebaran data pribadi di era digital.Indikator keberhasilan dari rancangan regulasi dalam menghadapi penyebaran data pribadi oleh berbagai entitas dalam lingkungan digital dapat mencakup beberapa aspek kunci berikut: (a) kepatuhan entitas terhadap regulasi: Tingkat kepatuhan entitas, termasuk perusahaan teknologi, penyedia layanan, dan organisasi lainnya, terhadap ketentuan regulasi adalah indikator penting keberhasilan. Kepatuhan ini dapat diukur melalui audit, laporan kepatuhan, dan tingkat pelanggaran yang dilaporkan. (b) peningkatan kesadaran masyarakat: Tingkat kesadaran masyarakat tentang hak privasi mereka dan cara melindungi data pribadi harus meningkat sebagai hasil dari upaya pendidikan dan sosialisasi yang dilakukan melalui regulasi. Hal ini dapat diukur melalui survei kesadaran masyarakat, partisipasi dalam program pendidikan, dan pencarian informasi tentang hak privasi online. (c) Penurunan kasus pelanggaran data: Keberhasilan regulasi dapat dilihat dari penurunan jumlah kasus pelanggaran data atau penyalahgunaan data pribadi oleh entitas yang diatur. Data ini dapat diperoleh melalui laporan resmi otoritas pengawas, pusat laporan kejahatan cyber, atau lembaga penegak hukum. (d) Transparansi dan akuntabilitas entitas: Regulasi yang berhasil harus mendorong transparansi dan akuntabilitas entitas yang mengelola data pribadi. Indikator keberhasilan meliputi tingkat keterbukaan entitas tentang praktik pengelolaan data, pengungkapan insiden pelanggaran data, dan tingkat partisipasi dalam program audit independen. (e) Kolaborasi internasional: Tingkat kerjasama dan kolaborasi antara negara-negara dalam melindungi data pribadi juga merupakan indikator penting. Ini dapat diukur melalui partisipasi dalam forum internasional, pertukaran informasi antar negara, dan penandatanganan kesepakatan kerjasama bilateral atau multilateral. (f) Evaluasi efektifitas regulasi: Tingkat keberhasilan regulasi juga dapat dilihat dari sejauh mana regulasi mendorong inovasi teknologi yang berkelanjutan dalam rangka meningkatkan keamanan dan privasi data. Ini dapat diukur melalui investasi dalam riset dan pengembangan, adopsi teknologi baru yang memperkuat keamanan data, dan pertumbuhan ekosistem teknologi yang aman dan berkelanjutan.

Dengan memantau dan mengevaluasi indikator-indikator ini secara berkala, pemerintah dan lembaga terkait dapat menilai keberhasilan implementasi regulasi dalam menghadapi penyebaran data pribadi oleh berbagai entitas dalam lingkungan digital.

KESIMPULAN

Kesimpulan

Kesimpulannya: (1) Regulasi teknologi keamanan siber memegang peran penting dalam menangani ancaman keamanan siber di era digital. Dengan memberikan panduan yang jelas, mendorong praktik terbaik, dan mengatur penegakan hukum, regulasi ini dapat mengurangi risiko serangan cyber, meningkatkan kesadaran akan perlindungan privasi, dan memfasilitasi inovasi teknologi yang aman. Kolaborasi lintas sektor menjadi kunci untuk keberhasilan regulasi ini dalam melindungi data dan infrastruktur digital secara efektif, memberikan fondasi yang kokoh bagi keamanan siber di masa mendatang. (2) Regulasi yang ideal untuk menghadapi penyebaran data pribadi di lingkungan digital harus mengutamakan perlindungan privasi individu, inovasi teknologi, dan keseimbangan antara perlindungan data dan perkembangan ekonomi digital. Dengan prinsip-prinsip transparansi, akuntabilitas, dan keterlibatan masyarakat, regulasi tersebut dapat memastikan bahwa data pribadi dilindungi secara efektif, sementara kebebasan berinovasi tetap terjaga. Kolaborasi internasional juga penting dalam upaya ini. Regulasi yang adaptif dan responsif terhadap perubahan teknologi dan ancaman baru akan menjadi kunci dalam memastikan keberhasilan perlindungan data pribadi di masa depan.

Rekomendasi: Mendorong regulasi yang mengutamakan perlindungan privasi, inovasi teknologi, dan keseimbangan ekonomi digital. Dorong transparansi, akuntabilitas, dan partisipasi masyarakat dalam pembuatan regulasi. Kolaborasi internasional harus ditingkatkan. Regulasi harus adaptif dan responsif

terhadap perubahan teknologi dan ancaman baru untuk memastikan keberhasilan perlindungan data pribadi di masa depan.

Saran

Untuk memastikan perlindungan yang optimal dalam menghadapi tantangan keamanan siber dan perlindungan data pribadi di era digital, beberapa langkah penting perlu diambil. Pertama, penguatan regulasi keamanan siber sangat krusial. Pemerintah dan lembaga terkait harus menyusun panduan yang jelas dan praktik terbaik yang terkini untuk keamanan siber, serta memastikan adanya penegakan hukum yang konsisten terhadap pelanggaran. Mekanisme sanksi bagi pelanggar dan pengawasan yang ketat harus diterapkan untuk memastikan kepatuhan. Selain itu, kolaborasi lintas sektor antara publik, swasta, dan akademik perlu difasilitasi untuk berbagi informasi dan teknologi guna menghadapi ancaman yang kompleks secara lebih efektif.

Kedua, regulasi perlindungan data pribadi harus mengedepankan keseimbangan antara perlindungan privasi individu dan dukungan terhadap inovasi teknologi. Kebijakan harus dirancang sedemikian rupa agar tidak menghambat perkembangan teknologi, sementara tetap menjaga standar keamanan data yang tinggi. Prinsip transparansi dan akuntabilitas juga harus diutamakan, dengan pengungkapan yang jelas mengenai kebijakan privasi dan mekanisme untuk menangani keluhan. Partisipasi masyarakat dalam pembuatan regulasi melalui konsultasi publik akan memastikan bahwa kebijakan yang diterapkan mencerminkan kebutuhan dan kekhawatiran masyarakat.

Selain itu, kolaborasi internasional perlu ditingkatkan untuk menangani tantangan global dalam keamanan siber dan perlindungan data pribadi. Kerja sama internasional dalam berbagi informasi tentang ancaman, standar keamanan, dan praktik terbaik akan memperkuat upaya perlindungan secara keseluruhan. Regulasi juga harus bersifat adaptif dan responsif terhadap perubahan teknologi dan ancaman baru, dengan pembaruan regulasi yang berkala dan mekanisme penyesuaian cepat. Dengan langkah-langkah ini, diharapkan regulasi dapat melindungi data dan infrastruktur digital secara efektif, sambil mendukung inovasi dan perkembangan ekonomi digital.

DAFTAR PUSTAKA

Adi Putra, R., Rahman, I., & Cahyo Setiono, G. (2023). Tinjauan Yuridis Terhadap Kesesuaian Keperuntukan Tanah Dalam Pembangunan Ibukota Baru Nusantara Ditinjau Dari Dampak Lingkungan. *Transparansi Hukum*, *6*(1). https://doi.org/10.30737/transparansi.v6i1.4593

Apriyanti, A. (2017). Historiografi Mahar dalam Pernikahan. *An Nisa'a*, *12*(2), Article 2.

Alharkan, I., & Alnasseri, S. (2020). *Cybersecurity Regulations and Their Implications*. Journal of Information Security, 11(3), 1-14.

Basri, H. (2017). Konsep Mahar (Maskawin) Dalam Tafsir Kontemporer. *Al Daulah: Jurnal Hukum Pidana Dan Ketatanegaraan*, *6*(2), 310–330.

Caisar, A. P. O. (2022). *Kewenangan Serta Kedudukan Otorita Di Ibu Kota Nusantara Dalam Sistem Tata Negara Indonesia Ditinjau Dari Perspektif Siyasah Dusturiyah* [Diploma, UIN FATMAWATI SUKARNO BENGKULU]. http://repository.iainbengkulu.ac.id/9546/

Deibert, R., Roio, D., & Crete-Nishihata, M. (2023). *International Collaboration on Cybersecurity: Challenges and Opportunities*. Global Security Review, 25(2), 102-118.

Greenleaf, G. (2021). *Global Data Privacy Laws 2021: The New Era of Privacy Protection*. Privacy & Data Protection, 21(4), 5-18.

Hasanuddin, H. (2018). Rukun Dan Syarat Dalam Ibadah Nikah Menurut Empat Mazhab Fiqh. *JURNAL MIMBAR AKADEMIKA*, *2*(2), Article 2.

Hidayat, M. S. (2021). Argumentasi Pembaruan Ushul Al-Fiqh: Problematika dan Tantangannya. *Journal of Islamic Studies and Humanities*, *6*(1), Article 1. https://doi.org/10.21580/jish.v6i1.8175

Instruksi Presiden No 1 Tahun 1991 Tentang Kompilasi Hukum Islam, Pub. L. No. 1 (1991).

Karlina, K. (2019). *Efektifitas mediasi dalam perkara cerai gugat di Pengadilan Agama Parepare (analisis kasus perceraian)* [Undergraduate, IAIN Parepare]. https://repository.iainpare.ac.id/id/eprint/522/

Karami, A., & Ayub, N. (2022). *Risk-Based Approach to Cybersecurity Regulation*. International Journal of Cyber Law, 19(2), 45-62.

Kohar, A. (2016). Kedudukan Dan Hikmah Mahar Dalam Perkawinan. *ASAS : Jurnal Hukum Ekonomi Syariah*, *8*(2), Article 2. https://doi.org/10.24042/asas.v8i2.1245

Majid, F. (2021). Emansipasi Wanita Menurut Al-Qur'an. *Al-Dzikra: Jurnal Studi Ilmu al-Qur'an dan al-Hadits*, *15*(1), Article 1. https://doi.org/10.24042/al-dzikra.v15i1.7745

Malisi, A. S. (2022). Pernikahan Dalam Islam. *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum*, *1*(1), Article 1. https://doi.org/10.55681/seikat.v1i1.97

Musyarrafa, N. I., & Khalik, S. (2020). Batas Usia Pernikahan Dalam Islam; Analisis Ulama Mazhab Terhadap Batas Usia Nikah. *Shautuna: Jurnal Ilmiah Mahasiswa Perbandingan Mazhab*. https://journal3.uin-alauddin.ac.id/index.php/shautuna/article/view/15465

Muzammil, I. (2019). *Fiqh Munakahat: Hukum pernikahan dalam Islam*. Tira Smart Anggota IKAPI Kota Tangerang. http://repository.uinsa.ac.id/id/eprint/1057/

Nihayati, D. A. (2022). Mahar Unik Dan Mahar Bernilai Fantastis Dalam Perspektif Fikih Munakahat. *MASADIR: Jurnal Hukum Islam*, *2*(1), 310–323. https://doi.org/10.33754/masadir.v2i1.467

Nst, H., Arsyita, J. F., Tanjung, M. A., Samzidane, M. H., Zaitun, M., & Fazyra, P. S. (2024). Hak Perempuan Dalam Memilih Calon Suami Ditinjau dari Perspektif Madzhab Syafi'i dan Madzhab Maliki. *As-Syar'i: Jurnal Bimbingan & Konseling Keluarga*, *6*(1), Article 1. https://doi.org/10.47467/as.v6i1.3335

O'Rourke, S. (2021). *Principles-Based Regulation in the Digital Age*. Law and Technology Review, 32(1), 28-39.

Putri, N. (2024). *Praktik Penyebutan Jumlah Mahar Dalam Akad Nikah Ditinjau Menurut Hukum Islam (Suatu Penelitian Hukum Adat Di Gampong Gunung Kerambil, Kec. Tapak Tuan, Kab.Aceh Selatan)* [Other, UIN Ar-Raniry Fakultas Syariah dan Hukum]. https://repository.ar-raniry.ac.id/id/eprint/34406/

Rinwanto, R., & Arianto, Y. (2020). Kedudukan Wali Dan Saksi Dalam Perkawinan Perspektif Ulama Empat Mazhab (Maliki, Hanafi, Shafiei Dan Hanbali). *AL MAQASHIDI*, *3*(1), Article 1.

Roshidah, M. (2024). *Tinjauan Hukum Islam Terhadap Pandangan Tokoh Nahdlatul Ulama dan Muhammadiyah Di Kabupaten Ponorogo Tentang Mahar Viral Pada Media Sosial* [Diploma, IAIN Ponorogo]. https://etheses.iainponorogo.ac.id/27755/

Sahir, M. (2018). *Kehadiran Saksi Dalam Pernikahan (Studi Perbandingan Antara Mazhab Maliki Dan Mazhab Syafi'i)* [Skripsi, UIN Ar-Raniry Banda Aceh]. http://library.ar-raniry.ac.id/

Smith, K., & Johnson, J. F. (2024). *Adapting Cybersecurity Regulations to Technological Change*. Journal of Cyber Policy, 15(1), 88-101

Winario, M. (2020). Esensi dan Standardisasi Mahar Perspektif Maqashid Syariah. *Jurnal Al Himayah*, *4*(1), Article 1.

.