CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol 1 No 5 Tahun 2023.
Prefix DOI : 10.3783/causa.v1i1.571

PERLINDUNGAN HUKUM TERHADAP SERANGAN SIBER: TINJAUAN ATAS KEBIJAKAN DAN REGULASI TERBARU

Dinda Aprilita Herera[1], Muhamad Hasan Sebyar[2]
Universitas Terbuka, Sekolah Tinggi Agama Islam Negeri Mandailing Natal
Email : aprilitadinda@yahoo.co.id

Abstrak *:* Ancaman serangan siber semakin meningkat dan menjadi kekhawatiran serius seiring dengan pesatnya perkembangan teknologi informasi. Meskipun manfaat besar diperoleh dari kemajuan teknologi ini, pintu terbuka lebar bagi para pelaku kejahatan siber yang semakin mahir dan terorganisir. Dari data pribadi hingga informasi bisnis dan infrastruktur kritis, semuanya berpotensi menghadapi ancaman yang tidak hanya berdampak pada keamanan, tetapi juga stabilitas ekonomi dan sosial. Penelitian ini bertujuan untuk melakukan tinjauan mendalam terhadap kebijakan dan peraturan terbaru yang diterapkan untuk melindungi masyarakat dari serangan siber. Dengan menganalisis langkah-langkah spesifik, kita dapat mengevaluasi efektivitas kebijakan-kebijakan tersebut dalam menghadapi tantangan serangan siber yang semakin meningkat. Metode penelitian dalam penelitian ini menggunakan jenis penelitian hukum normatif untuk menganalisis pendekatan peraturan perundang-undangan *(statute approach)* terkini terkait perlindungan hukum terhadap serangan siber. Hasil Penelitian ini menunjukkan bahwa Perubahan kebijakan dan regulasi terbaru dalam hukum siber berdampak signnifikan terhadap perlindungan hukum terhadap serangan siber. Dengan adanya kebijakan dan regulasi terbaru ini, terdapat peningkatan perlindungan terhadap data pribadi, informasi sensitif, dan infrastruktur penting. Hal ini dapat meningkatkan kemampuan pemerintah dalam merespon dan melindungi negara dari serangan siber.
Kata Kunci: Perlindungan Hukum; Siber; Peraturan Perundang-undangan

Abstract: *The threat of cyberattacks is increasing and becoming a serious concern along with the rapid development of information technology. While great benefits are derived from these technological advancements, the door is wide open for increasingly proficient and organized cyber criminals. From personal data to business information and critical infrastructure, all are potentially facing threats that not only impact security, but also economic and social stability. This research aims to conduct an in-depth review of the latest policies and regulations implemented to protect society from cyberattacks. By analyzing specific measures, we can evaluate the effectiveness of these policies in facing the increasing challenges of cyberattacks. The research method in this study uses a type of normative legal research to analyze the latest statute approach related to legal protection against cyber attacks. The*

results of this study show that the latest policy changes and regulations in cyber law have a significant impact on legal protection against cyber attacks. With these latest policies and regulations, there is an increase in the protection of personal data, sensitive information, and critical infrastructure. This can improve the government's ability to respond and protect the country from cyber attacks.
Keywords: Legal Protection; Cyber; Legislation

PENDAHULUAN

Di era digital yang terus berubah, serangan siber menjadi ancaman yang semakin nyata dan mengkhawatirkan. Pesatnya perkembangan teknologi informasi telah membawa manfaat yang sangat besar bagi masyarakat global, namun di sisi lain juga membuka pintu lebar-lebar bagi para pelaku kejahatan siber yang semakin terampil dan terorganisir. Data Pribadi, informasi bisnis, dan infrastruktur penting, semuanya menghadapi potensi ancaman yang tidak hanya membahayakan keamanan tetapi juga stabilitas ekonomi dan sosial. Russel Butarbutar (2023) menyatakan bahwa faktor manusia telah terbukti bertanggung jawab atas beberapa serangan siber terburuk yang menimpa organisasi setiap harinya. Yang paling sulit untuk dikelola adalah eksploitasi terhadap manusia, yang seiring disebut sebagai "rekayasa sosial". Indonesia adalah negara yang termasuk target serangan siber dimana menurut Kominfo setiap tahunnya data yang dicuri mencapai jutaan identitas, selain itu Indonesia juga termasuk negara yang dijadikan target dalam serangan siber, Badan Siber dan Sandi Negara (BSSN) mempublikasikan laporan tahunan monitoring keamanan siber tahun 2021. Laporan ini dipublikasikan pada situs resmi milik Direktorat Operasi Keamanan Siber BSSN tepatnya pada Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center), dari laporan tersebut dapat terlihat bahwa lebih dari 1,6 miliar atau tepatnya adalah 1.637.973.022 anomali trafik atau serangan siber (*cyber attack*) yang terjadi di seluruh wilayah Indonesia pada tahun 2021 (Tamarell Vimy, dkk, 2022). Oleh karena itu, perlindungan hukum terhadap serangan siber merupakan kebutuhan yang mendesak. Saat merinci tantangan serangan siber, kita harus memahami kompleksitas lingkungan digital saat ini. Pengelolaan data dan informasi pribadi di Indonesia dinilai sangat penting untuk diawasi dan dikelola dengan sistem keamanan yang baik dan terjamin sehingga dapat meminimalisir kejahatan pencurian atau pembobolan data dan informasi serta kejahatan jual beli data dan informasi online di Indonesia, karena dampak dari kejahatan tersebut adalah adanya penyalahgunaan data dan informasi pribadi seorang oleh pihak yang tidak bertanggungjawab (Ririn Aswandi, dkk, 2020).

Usaha untuk menjangkau kejahatan dalam bidang siber yang tidak dapat diakomodir oleh Kitab Undang-Undang Hukum Pidana, dibentuklah suatu undang-undang khusus yang mengatur bidang siber dan mengenai tindak pidana di bidang siber yakni Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik jo Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, walaupun telah diberlakukan dan diadakannya perubahan namun serangan siber yang terjadi sulit untuk di tanggulangi, dikarenakan tindakan penanggulangan serangan siber pada mulanya dilakukan secara terpisah-pisah (Hidayat, 2017). Oleh karena itu, penting untuk melakukan tinjauan menyeluruh terhadap kebijakan dan peraturan terbaru yang bertujuan melindungi masyarakat dari serangan siber. Kita harus memahami bahwa serangan siber tidak hanya menimbulkan ancaman terhadap individu atau badan usaha tertentu, tetapi juga dapat berdampak luas di tingkat nasional dan internasional. Serangan siber dapat membahayakan dan menghancurkan infrastuktur penting, serta menimbulkan kerugian besar pada sektor bisnis. Kebijakan regulasi yang efektif harus mampu mengatasi, meningkatkan skala dan kompleksitas serangan siber.

Penelitian terdahulu tentang perlindungan hukum terhadap serangan siber telah mengeksplorasi sejumlah aspek yang relevan, diantaranya:

1. Regulasi Keamanan Siber: Analisis terhadap regulasi yang ada atau diusulkan untuk melindungi organisasi dan individu dari serangan siber. Contoh Peraturan perundang-undangan yang mengatur ada dalam Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang penyelenggaraan Keamanan Informasi di Bank Indoensia (PBI Keamanan Informasi).
2. Privasi dan Perlindungan Data: Penelitian cenderung menyelidiki dampak serangan siber terhadap privasi dan perlindungan data. Hal ini termasuk meninjau perlindungan data pribadi, tanggung jawab perusahaan, dan implikasi hukum dari pelanggaran data.
3. Aspek Internasional dan Lintas Batas: Fokus pada kerja sama internasional dan regulasi lintas batas untuk memerangi serangan siber. Hal ini termasuk pertukaran informasi, penyerahan pelaku serangan, dan koordinasi tindakan antar negara.
4. Hukuman dan Penuntutan: Peninjauan mekanisme hukuman dan penuntutan bagi pelaku serangan siber. Hal ini mencakup tantangan untuk mengidentifikasi dan mengadili para pelaku serangan.
5. Kebijakan Publik dan Partisipasi Swasta: Peran kebijakan publik dalam membentuk kerangka peraturan untuk keamanan siber dari

kontribusi sektor swasta dalam menciptakan lingkungan yang lebih aman.

Banyak negara yang memahami betapa parahnya ancaman ini, negara-negara tersebut merancang kebijakan dan peraturan baru yang ditunjukan khusus untuk melindungi masyarakat dari serangan. Langkah-langkah tersebut mencakup pembentukan organisasi keamanan siber, peningkatan kerja sama internasional dalam memerangi kejahatan siber lintas negara, dan peningkatan sanksi hukum terhadap pelaku serangan. Namun keberhasilan penerapan kebijakan ini masih kontroversial. Ketidakpastian dalam menentukan sanksi yang tepat dan menerapkan proses hukum terhadap pelaku serangan siber yang beroperasi di wilayah yang sulit dijangkau secara hukum menjadi kendala utama bagi upaya pembelaan hukum ini.

Dalam konteks ini, artikel ini bertujuan untuk melakukan tinjauan mendalam terhadap kebijakan dan peraturan terbaru yang diterapkan untuk melindungi masyarakat dari serangan siber. Dengan menganalisis langkah-langkah spesifik, kita dapat mengevaluasi efektivitas kebijakan-kebijakan tersebut dalam menghadapi tantangan serangan siber yang semakin meningkat. Oleh karena itu, artikel ini berupaya memberikan pemahaman lebih dalam mengenai upaya perlindungan hukum terhadap realitas serangan siber di era digital.

METODE PENELITIAN

Studi ini menggunakan jenis penelitian hukum normatif untuk menganalisis pendekatan peraturan peundang-undangan *(statute approach)* terkini terkait perlindungan hukum terhadap serangan siber. Sumber data dikumpulkan melalui penelitian terhadap dokumen-dokumen hukum, antara lain undang-undang, peraturan, kebijakan pemerintah, dan dokumen resmi terkait perlindungan terhadap serangan siber. Teknik pengumpulan data dilakukan melalui analisis isi dokumen, identifikasi aspek hukum dan klasifikasi peraturan terkait untuk melindungi dari serangan siber. Analisis data mencakup interpretasi hukum atas kebijakan dan peraturan yang ada untuk mengidentifikasi kelemahan, kekuatan, dan dampak dalam konteks perlindungan terhadap serangan siber. Ruang lingkup kajian fokus penelitian dibatasi pada kebijakan dan peraturan terkini yang terkait langsung dengan perlindungan hukum.

HASIL DAN PEMBAHASAN

Serangan siber adalah upaya orang yang tidak berwenang untuk mengakses ke sistem atau jaringan komputer dan merusak atau mencuri informasi. Serangan ini

dapat mencakup berbagai teknik, termasuk malware, phising, dan penolakan layanan (DoS). Serangan siber dapat menimbulkan konsekuensi serius, termasuk kerugian finansial, pencurian identitas, dan rusaknya reputasi bisnis dan individu. Kelemahan keamanan siber di Indonesia memiliki dampak signifikan terhadap investasi dan pengembangan teknologi. Untuk menarik investasi dan mendorong pengembangan teknologi yang lebih baik, perlu dilakukan perbaikan dalam indeks pertahanan siber, penandatanganan regulasi keamanan siber yang memadai, dan peningkatan anggaran untuk investasi keamanan siber. Tindakan ini akan meningkatkan kepercayaan investor dan membuka peluang bagi perkembangan teknologi yang lebih maju di Indonesia. Faktor manusia menjadi kelemahan utama dalam keamanan siber. Untuk menghadapi tantangan ini, perlindungan yang efektif melibatkan pendidikan dan edukasi berkelanjutan guna meningkatkan literasi digital dan kesadaran akan keamanan siber. Sinergi antara pemangku kepentingan dalam meningkatkan literasi digital dan kesadaran akan keamanan siber sangat penting. Selain itu, strategi antisipasi yang melibatkan perencanaan ketahanan dan keamanan digital yang komprehensif juga diperlukan (Muhammad Subhan Abdullah, & Heidiani Ikasari, I, 2023).

Di Indonesia, serangan siber menjadi isu yang semakin penting. Banyaknya serangan ke sistem informasi Indonesia adalah karena kesadaran akan ancaman siber dan regulasi atau aturan belum kuat di Indonesia, hal ini karena para penentu kebijakan masih awam terhadap informasi terkait siber. Dimana tata kelola manajemen keamanan siber juga masih dibilang lemah, yang harusnya ketika timbul ancaman, tim IT langsung tanggap dan langsung melakukan upaya pertahanan pada situs-stu yang berisi data penting dengan cara pengecekan, menghubungi lembaga ahli seperti BSSN dan lebih jauh dengan melakukan takedown sementara sehingga tidak menimbulka kebocoran data ke internet (Tamarell Vimy, dkk, 2022). Lauder Siagian, dkk (2018) menyatakan bahwa Infrastruktur teknologi informasi menjadi tulang punggung berjalannya informasi berbagai lini politik, ekonomi, sosial, budaya, pertahanan dan keamanan meningkatkan potensi ancaman / gangguan pada sistem teknologi internet (Su, X., 2006).

Prabowo, W., Wibawa, S., & Azmi, F. (2020) menyatakan tujuan dari keamanan siber apabila dikaitkan dengan eksistensi informasi dalam ruang siber akan sangat memprioritaskan tiga hal yaitu Confidentiality, Integrity dan Availability. Untuk mencegah kejahatan sibers, individu dan pemerintah perlu memahami dengan jelas skema kejahatan di dunia maya dan tren serta perilaku Internet kontemporer dan berkelanjutan dari para penjahat ini. Saat ini, pencurian kartu kredit dan kasus pencucian uang online kejahatan dunia maya semakin meningkat. Pelecehan dan pencemaran nama baik melalui media sosial juga menjadi

perhatian individu. Cyber-terorisme merupakan aspek yang paling menonjol dari kejahatan dunia maya di seluruh negara. Dengan demikian keamanan dan keselamatan informasi telah menjadi tantangan utama saat ini. Dengan pertumbuhan pengguna yang pesat, kasus kejahatan dunia maya juga meningkat dan tidak dibatasi oleh batasan geografis atau batas negara di dunia. Ini merupakan masalah yang sangat memprihatinkan karena berdampak negatif langsung pada kehidupan ekonomi dan sosial masyarakat (Russel, 2023). Secara umum unsur-unsur yang dapat diidentifikasi memiliki potensi sebagai ancaman siber terdiri atas : Sumber internal dan eksternal, kegiatan intelijen, kekecewaan, investigasi, organisasi ekstremis, acktivists, grup kejahatan terorganisir, persaingan, permusuhan & konflik, teknologi.

Bentuk ancaman siber yang sering terjadi saat ini dapat berupa hal-hal sebagai berikut :

a) Serangan Advanced Persistent Threats (APT), Denial of Service (DoS) dan Distributed Denial of Service (DDoS), biasanya dilakukan dengan melakukan overloading kapasitas sistem dan mencegah pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Serangan ini bertujuan untuk mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang bisa ditangani sistem. Sehingga sistem menjadi terlalu sibuk dan crash, akibatnya menjadi tidak dapat melayani atau tidak dapat beroperasi. Permasalahan ini merupakan ancaman yang berbahaya bagi organisasi yang mengandalkan hampir sepenuhnya pada kemampuan internet guna menjalankan roda kegiatannya. Pemahaman risiko serangan siber merupakan tanggung jawab seluruh personel bukan hanya menjadi masalah bagian IT adalah hal yang perluditekankan oleh manajemen. Pintu masuk serangan siber bisa melalui akses ke situs rawan, pengunduhan file gratis, passwordyang sederhana, dan hal lainnya yang bisa dilakukan oleh semua personel yang kurang waspada (Anastasia Lana, 2021).

Jenis Kejahatan Siber terdiri dari: (1) Rekayasa Sosial dan tipu daya (social engineering and trickery); (2) Pelecehan Daring (Online Harassment); (3) Kejahatan terkait Identitas (Identify-related crimes); (4) Peretasan (Hacking); dan (5) Penolakan Layanan dan Informasi (Denial of Service and Information). Secara umum kita banyak mengenal kejahatan siber seperti phishing, malware, kejahatan identitas, penipuan online, dan pelecehan online dapat memiliki dampak serius terhadap keamanan, privasi, dan kesejahteraan individu (Russel, 2023).

Peraturan Perundang-undangan Yang Mengatur Kejahatan Siber di Indonesia:

Peraturan perundang-undangan yang mengatur kejahatan siber di Indonesia terdapat dalam Undang-Undang Dasar Negara Republik Indonesia 1945 (UUDRI 1945), Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik.

a. Perlindungan Hak Asasi dalam Pasal 28 G ayat (1) UUD 1945 menyatakan "Setiap orang berhak atas perlindungan atas perlindungan pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada dibawah kekuasannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." Hak privasi merupakan pengakuan sebagai hak asasi manusia, hak privasi pada perlindungan data yaitu suatu bagian penting untuk kebebasan diri seseorang. Perlindungan data merupakan wujud kebebasan dalam berpolitik, keagamaan, maupun aktiitas yang sifatnya pribadi. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Alenia keempat pembukaan UUD 1945 menyatakan bahwa pemerintah berkewajiban secara konstitusional memberikan perlindungan bagi seluruh warga negara, meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa, serta terlibat dalam tata tertib dunia berdasarkan kemerdekaan, perdamaian abadi, maupun keadilan sosial. Perkembangan teknologi informasi dan komunikasi dalam suatu negara yang diwujudkan dalam bentuk perlindungan data pribadi dari setiap warga negara Indonesia. Selaku konstitusi memberikan kebijakan untuk menanggulangi tindakan mencuri data pribadi dengan memberikan perlindungan atas kepemilikan pribadi dari berbagai pihak yang berupaya melakukan pembobolan atau mencuri data dari pihak lain. Kebutuhan akan perlindungan hukum data pribadi mulai menguat seiring dengan perkembangan terhadap pemanfaatan teknologi informasi pada era globalisasi saat ini yang semakin berkembang dengan pesat. Beberapa kasus khususnya yang mempunyai hubungan dengan data pribadi yang bocor berakibat ke tindakan penipuan/tindakan criminal, pornografi, menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi.

b. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah dengan Undang-undang Nomor 19Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Perlindungan data pribadi dalam UU ITE meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, serta perlindungan dari berbagai akses ilegal. Terkait penaggulangan kebocoran data pribadi yaitu dengan memberikan parlindungan kepada data pribadi dari penggunaan atau pemanfaatan tanpa izin.

1. Tindakan yang melanggar kesusilaan Dalam Pasal 27 ayat (1) UU Nomor 11 Tahun 2008 disebutkan "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan", tetapi dalam pasal tersebut tidak dijelaskan mengenai perbuatan yang (Mudadi & Barda Nawawi, Teori-teori dan Kebijakan Pidana, PT. Alumni Bandung, 2010, Hal. 157 dalam Utin Indah, 2022). memiliki muatan yang melanggar kesusilaan. Sementara dalam konteks perbuatan yang melanggar kesusilaan melalui media elektronik, terdapat beberapa tindakan yang tergolong dalam Pasal 27 ayat (1) UU Nomor 11 Tahun 2008, yaitu cyber pornografi dan prostitusi online. Tindak pidana ini akan semakin berat hukumannya apabila dilakukan terhadap anak di bawah umur. Salah satu permasalahan yang ditimbulkan dari kemajuan teknologi informasi melalui jaringan internet adalah beragamnya situs yang menampilkan adegan pornografi. Seolah-oleh sekarang ini, sulit sekali memproteksi jaringan internet dari serbuan pebisnis hiburan yang menjual pornografi.
2. Penghinaan/Pencemaran nama baik. Penghinaan/Pencemaran nama baik di cyber space diatur dalam Pasal 27 ayat (3) UU Nomor 11 Tahun 2008 yang menyatakan "Setiap orang dengan sengaja dam tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diakseskan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik". Dalam UU ITE ini, pembuat undang-undang menyetarakan antara penghinaan dengan pencemaran, pada penghinaan sendiri merupakan suatu kelompok perbuatan, sedangkan salah satu bentuk penghinaan ialah pencemaran (Utin Indah, 2022).

Pasal 26 UU ITE memberi syarat bahwa setiap penggunaan data pribadi dalam sebuah media elektronik harus terlebih dahulu mendapatkan persetujuan pemilik data bersangkutan. Para pihak yang melanggar dapat digugat atas kerugian yang ditimbulkan. Adapun isi dari Pasal 26 UU ITE, yaitu sebegai berikut:

1) Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.
2) Setiap orang yang dilanggar haknya sebagimana yang dimaksud ayat 1 dapat menagjukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang.
3) Setiap penyelenggara sistem elektronik wajib menghapus informasi elektronik dan atau/ dokumen elektronik yang tidak relevan yang

berada dibawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.

4) Setiap penyelenggaran sistem elektronik wajib menyedikan mekanisme penghapusan informasi elektronik dan/ atau dokumen elektronik yang tida relevan sesuai dengan ketentuan peraturan perundang-undangan.
5) Ketentuan mengenai tata cara penghapusan informasi elektronik dan/ atau dokumen elektronik sebagaimana demaksud pada ayat 3 dan ayat 4 diatur dalam peraturan pemerintah. (Desmon, A. ., & Angelia, R. R. O. . , 2022).

Pasal 15 UU ITE mengatur bahwa Penyelenggara Sistem Elektronik harus menyelenggarakan sistem elektroniknya secara aman, andal, dan bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. Artinya seluruh Penyelenggara Sistem Elektronik, terlepas apakah sistem itu digunakan untuk kepentingan pemerintahan, komersial, atau pribadi harus menyelenggarakan sistemnya secara andal, aman dan bertanggung jawab. PP 82/2012 memberikan pedoman bagaimana Penyelenggara Sistem Elektronik menyelenggarakan sistemnya secara andal, aman, dan bertanggung jawab sebagaimana diamanatkan oleh UU ITE. Kemudian PP 82/2012 mengatur bahwa Sistem Elektronik memiliki lima komponen, yaitu: Perangkat keras, Perangkat lunak, Tenaga ahli, Tata kelola, dan Pengamanan. PP 82/2012 membagi Penyelenggara Sistem Elektronik menjadi dua bagian besar, yaitu: Penyelenggara Sistem Elektronik untuk Pelayanan Publik; dan Penyelenggara Sistem Elektronik untuk non Pelayanan Publik.

PP 82/2012 memberikan standar yang lebih tinggi kepada Penyelenggara Sistem Elektronik untuk Pelayanan Publik dalam menyelenggarakan sistemnya secara andal, aman dan bertanggung jawab terhadap kelima komponen yang dimaksud, misalnya:

1. Wajib melakukan pendaftaran sebelum Sistem Elektronik mulai digunakan publik (Pasal 5 ayat (1) PP 82/2012)
2. Perangkat lunak yang digunakan wajib terdaftar pada Kominfo serta terjamin keamanan dan keandalan operasi-nya (Pasal 7 PP 82/2012)
3. Wajib menerapkan tata kelola yang baik dan akuntabel (Pasal 16 ayat (1) PP 82/2012)
4. Memiliki rencana keberlangsungan kegiatan untuk menanggulangi gangguan atau bencana sesuai dengan risiko dari dampak yang ditimbulkannya (Pasal 17 ayat (1) PP 82/2012)
5. Menempatkan pusat data dan pusat pemulihan bencana di wilayah hukum Indonesia (Pasal 17 ayat (2) PP 82/2012)
6. Memiliki Sertifikat Kelaikan Sistem Elektronik (Pasal 30 ayat (1) PP 82/2012)

7. Menggunakan Sertifikat Keandalan (Pasal 41 ayat (1) PP 82/2012)
8. Memiliki Sertifikat Elektronik (Pasal 59 ayat (1) PP 82/2012)
9. Memenuhi persyaratan penyelenggaraan Transaksi Elektronik

Dengan adanya pedoman tersebut, diharapkan agar secara semesta atau secara nasional, Sistem Elektronik yang ada di Indonesia dapat menjadi satu kesatuan sistem yang kokoh, andal dan aman. Hal ini selaras dengan prinsip pertahanan nasional yaitu bahwa pertahanan dilakukan secara semesta. Pertahanan negara diselenggarakan melalui usaha membangun dan membina kemampuan, daya tangkal negara dan bangsa, serta menanggulangi setiap ancaman.

Beberapa aspek perlindungan hukum dalam UU ITE meliputi:

1. **Pengaturan Tindakan Kriminal:** UU ITE menetapkan tindakan kriminal terkait dengan penggunaan teknologi informasi, seperti akses ilegal, perusakan data, dan penyebaran infomasi palsu.
2. **Perlindungan Privasi:** Undang-undang ini juga mencakup ketentuan terkait perlindungan privasi data pengguna dan pengolahan informasi pribadi.
3. **Perlindungan dari serangan:** UU ITE memberikan landasan hukum untuk memberantas serangan siber, termasuk serangan phising, malware, dan aktivitas kriminal lainnya terkait teknologi informasi.
4. **Kewajiban Penyedia Layanan:** Penyedia di ruang digital bertanggung jawab melindungi data dan informasi pengguna sesuai ketentuan yang diatur dalam UU ITE.

Berdasarkan Pasal diatas aktifitas pengumpulan dan penyebarluasan data pribadi merupakan suatu perbuatan pelanggaran terhadap privasi seseorang dikarenakan hak privasi mencakup hak menentukan memberikan atau tidak memberikan data pribadi. Dengan adanya UU ITE ini pemerintah memberikan kepada penyelenggara sistem elektronik yang melakukan pelanggaran berkaitan dengan data pribadi dapat mengajukan gugatan secara perdata kepada pengadilan.Selain untuk mencegah pelanggaran-pelanggaran penyalahgunaan berupa pencurian dan kebobolan data pribadi pemerintah melalui UU ITE memberikan perintah kepada Penyelenggara Sistem Elektronik untuk menyiapkan sebuah sistem yang dapat melakukan penyesuaian serta penghapusan pada data pribadi yang dianggap tidak sesuai berdasarkan dari pihak terkait kepada pengadilan dan putusan pengadilan (Desmon, A. ., & Angelia, R. R. O. . , 2022).

c. Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelanggaraan Sistem dan Transaksi ElektronikPeraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelanggaran Sistem dan Transaksi Elektonik ini merupakan pengaturan lebih lanjut dari Undang-Undang Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Nomor 11 tahun 2011 tentang Informasi dan Transaksi Elektronik yang

salah satu isinya terkait mengenai penyalahgunaan data pribadi. Dalam Pasal 14 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ada beberapa prinsip yang wajib oleh penyelenggara sistem elektronik dalam memberikan perlindungan data pribadi seseorang dari pencurian data pribadi yaitu :

1. Penyelenggara Sistem Elektronik wajib melaksanakan prinsip perlindungan data pribadi dalam melakukan proses pemrosesan data pribadi yang meliputi :

a. Pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik data pribadi;

b. Pemrosesan data pribadi dilakukan sesuai dengan tujuannya;

c. Pemrosesan data pribadi dilakukan dengan menjamin hak pemilik data pribadi;

d. Pemrosesan data pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan data pribadi;

e. Pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi, dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan data pribadi;

f. Pemprosesan data pribadi dilakukan dengan memberitahukantujuan pengumpulan, aktifitas pemprosesan, dan kegagalan perlindungan data pribadi;

g. Pemrosesan data pribadi dimusnahkan dan/atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan. (Desmon, A. ., & Angelia, R. R. O. . , 2022).

Secara sosiologis, masyarakat memang membutuhkan suatu peraturan tentang regulasi hukum yang konkrit tentang teknologi informasi yang sebelum dikeluarkannya UU ITE, peraturan yang ada hanya sebatas berhubungan dengan teknologi informasi, belum menjelaskan dengan secara langsung dan lebih konkrit. Dengan adanya UU ITE dimaksudkan untuk mengatur berbagai aktivitas masyarakat saat berinteraksi di cyber space. Selain memenuhi syarat sosiologis, UU ITE juga telah memenuhi syarat secara filosofis. Secara filosofis, lahirnya UU ITE ini didasarkan pada amanat yang terkandung dalam Pasal 28F Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan " Setiap orang berhak untuk mencari, memperoleh, memiliki, meyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia" (Utin Indah, 2022). Wahyu Beny (2020) menyatakan bahwa UU ITE tidak mengatur secara spesifik pemasalahan terkait *cybercrime*. Pemerintah masih menggunakan pendekatan kebijakan publik yang melibatkan kelompok lain.

Analisis Peraturan Perlindungan Terhadap Serangan Siber

Tinjauan dan kebijakan serangan siber melibatkan penilaian menyeluruh terhadap potensi risiko dan ancaman yang mungkin dihadapi. Tingkat keparahan ancaman siber yang dirasakan selaras dengan peringkat efektivitas. Perbedaan di antara kelompok peserta mungkin mencerminkan pengalaman yang beragam di dalam sektor-sektor, yang menyoroti perlunya tindakan hukum yang ditargetkan (Ramayanti , Arief Fahmi Lubis, 2023). Kebijakan serangan siber di Indonesia melibatkan berbagai aspek, antara lain :

1. Undang-undang Informasi dan Transaksi Elektronik (UU ITE)

UU ITE merupakan landasan hukum yang mengatur kegiatan perdagangan elektronik di Indonesia. UU ITE juga memuat keentuan mengenai keamanan siber dan pemberantasan kejahatan dunia maya.

2. National Cyber Security Policy (NCSP)

Kebijakan ini bertujuan untuk meningkatkan tingkat keamanan siber di Indonesia. NCSP mencakup komitmen untuk melindungi infrastruktur penting, meningkatkan kemampuan tenaga kerja keamanan siber, dan berkolaborasi dengan sektor swasta dan lembaga terkait.

3. Badan Siber dan Sandi Negara

Badan siber dan Sandi Negara merupakan lembaga pemerintah yang fokus di bidang keamanan siber. Mereka bertanggung jawab untuk mengembangkan kebijakan, standar, dan kerangka keamanan siber nasional.

4. Kerjasama dengan Sektor Swasta dan Lembaga Terkait

Pemerintah Indonesia bekerja sama dengan sektor swasta dan lembaga terkait untuk meningkatkan keamanan siber. Hal ini termasuk memberikan pelatihan keamanan siber, berbagai informasi, dan kolaborasi untuk mengatasi ancaman siber.

5. Pendidikan dan Pelatihan Keamanan Siber

Berfokus pada peningkatan kemampuan tenaga kerja keamanan siber, Pemerintah mendukung program pendidikan dan pelatihan untuk mengembangkan profesional yang dapat mengatasi tantangan keamanan siber.

6. Pengawasan dan Penegakan Hukum

Pemerintah memantau keamanan siber dan menjatuhkan hukuman atas pelanggaran. Hal ini mancakup tindakan penegakan hukum terhadap serangan siber dan kejahatan siber lainnya.

Pedoman ini membentuk kerangka komprehensif untuk melindungi Indonesia dari anccaman serangan siber dan meningkatkan kemampuannya dalam menghadapi tantangan teknologi informasi.

Poin-poin penting ketika mengembangkan kebijakan serangan siber adalah :

a. **Penilaian Resiko:** Identifikasi aset penting dan kerentanan yang dapat diekploitasi. Penilaian resiko membantu organisasi memahami tingkat resiko

yang mereka hadapi dan mengambil langkah-langkah yang tepat untuk mengurangi resiko.

b. **Perlindungan dan Pencegahan:** Menerapkan tindakan teknis seperti firewall, antivirus, dan enkripsi untuk melindungi sistem dari ancaman siber. Kebijakan ini juga mencakup penggunakan praktik keamanan seperti autentikasi dua faktor dan pembaruan perangkat lunak rutin.
c. **Deteksi dan Respons:** Membangun kemampuan untuk mendeteksi dan merespons serangan siber dengan cepat. Ini mungkin termasuk penggunaan sistem deteksi intrusi (IDS) atau sistem manajemen kejadian keamanan informasi (SIEM).
d. **Kesadaran dan Pelatihan:** Memberikan pelatihan kepada karyawan atau pengguna untuk mengenali tanda-tanda serangan siber dan mempraktikkan praktik keamanan yang baik.
e. **Pemantauan Berkelanjutan:** Memastikan sistem pemantanuan yang efektif tersedia untuk memantau aktivitas jaringan dan dengan cepat mengidentifikasi potensi ancaman.

Perubahan kebijakan dan regulasi terbaru dalam hukum siber berdampak signnifikan terhadap perlindungan hukum terhadap serangan siber. Dengan adanya kebijakan dan regulasi terbaru ini, terdapat peningkatan perlindungan terhadap data pribadi, informasi sensitif, dan infrastruktur penting. Hal ini dapat meningkatkan kemampuan pemerintah dalam merespon dan mmelindungi negara dari serangan siber. Peraturan terbaru yang ada juga dapat meningkatkan hukuman bagi pelaku serangan siber. Hal ini meningkatkan pencegahan dan meningkatkan efektivitas penegakan hukum. Regulasi baru dapat mengenai kewajiban organisasi untuk meningkatkan standar keamanan siber mereka. Ini dapat mencakup pengembangan kebijakan keamanan, pelatihan karyawann, dan penerapan teknologi keamanan terkini.

Implementasi Penerapan Kebijakan Perlindungan Hukum Terhadap Serangan Siber di Berbagai Yuridiksi:

1) Pengembangan Undang-undang Khusus: Pengembangan undang-undang yang secara khusus mengatur kejahatan siber, menetapkan hukuman, dan memberi dasar hukum untuk penanganan serangan siber
2) Pembentukan Lembaga atau Otoritas Khusus: Mendirikan lembaga atau ottoritas yang khusus menangani keamanan siber, seperti Badan Siber Nasional (BSSN) di Indonesia atau Cybersecurity and Infrastucture Security Agency (CISA) di Amerika Serikat
3) Kerjasama Internasional: Berpartisipasi dalam forum dan inisiatif internasional untuk berbagai informasi, intelejen, dan berkoordinasi dalam penanggulangan serangan siber.

4) Standarisasi Keamanan Sektor Swasta: Menetapkan standar keamanan yang harus dipatuhi oleh sektor swasta, mungkin melalui peraturan atau program sertifikasi keamanan
5) Pendidikan dan Pelatihan Keamanan Siber: Mempromosikan pendidikan dan pelatihan keamanan siber untuk meningkatkan kemampuan sumber daya manusia dalam merespon ancaman siber
6) Penggunaan Teknologi Modern: Menerapkan teknologi modern untuk mendeteksi, merespon, dan mencegah serangan siber, termasuk kebijakan mengenai penggunaan keamanan teknologi informasi
7) Persyaratan Pelaporan dan Transparansi: Menetapkan persyaratan pelaporan serangan siber dan persyaratan transparansi bagi pihak terkait untuk mempercepat respon dan mengurangi dampak serangan

Langkah-langkah ini menciptakan kerangka komprehensif untuk melindungi negara dan dunia usaha dari serangan dunia maya dan memberikan dasar hukum yang diperlukan untuk penegakan hukum.

KESIMPULAN DAN SARAN

Berdasarkan analisis mengenai Perlindungan Hukum Terhadap Serangan Siber, dapat disimpulkan bahwa di era digital, ancaman dunia maya menjadi semakin penting dan berpengaruh. Meskipun kemajuan teknologi informasi telah memberikan manfaat bagi masyarakat global, kemajuan tersebut juga meningkatkan ancaman terhadap para profesional keamanan siber. Privasi, informasi bisnis, dan infrastruktur penting semuanya berkontribusi terhadap potensi ancaman dunia maya yang berdampak tidak hanya pada keamanan tetai juga stabilitas ekonomi dan sosial. Ancaman dunia maya tidak hanya merugikan individu dan bisnis, tetapi juga dapat menyebar melintasi batas negara. Regulasi yang efektif harus bertujuan untuk mengatasi meningkatnya skala dan kompleksitas ancaman siber. Peraturan tersebut antara lain memperkuat organisasi keamanan siber, meningkatkan kerja sama internasional di bidang pertahanan siber, dan mmemperkuat perlindungan hukum terhadap penjahat siber. Dapat diketahui bahwa perlindungan hukum yang tertera dalam perturan perundang-undangan terkait serangan siber terdapat dalam Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang merupakan landasan hukum yang mengatur kegiatan perdagangan elektronik di Indonesia, National Cyber Security Policy (NCSP) yang bertujuan untuk meningkatkan tingkat keamanan siber di Indonesia, dibentuknya Badan Siber dan Sandi Negara, yang bertanggung jawab untuk mengembangkan kebijakan, standar, dan kerangka keamanan siber nasional, Kerjasama dengan sektor swasta dan lembaga terkait keamanan siber, Tersedianya pendidikan dan pelatihan keamanan siber, berfokus pada peningkatan kemampuan tenaga kerja keamanan siber, pemerintah

mendukung program pendidikan dan pelatihan untuk mengembangkan profesional yang dapat mengatasi tantangan keamanan siber, pengawasan dan penegakan hukum pemerintah juga memantau keamanan siber dan menjatuhkan hukuman atas pelanggaran.

Berdasarkan kesimpulan maka berikut saran-saran:

1. Memperkuat Kerjasama: Mendorong kerjasama lebih lanjut antara Pemerintah, sektor swasta, dan akademisi akan mengembangkan solusi bersama yang dapat mengatasi tantangan keamanan siber.
2. Pembaruan Peraturan: Mengidentifikasi dan memperbarui peraturan yang relevan untuk mengimbangi perkembangan teknologi dan mempertimbangkan hukuman yang lebih berat bagi penjahat dunia maya.
3. Meningkatkan Kesadaran Masyarakat: Melakukan kampanye pendidikan yang lebih agresif untuk meningkatkan kesadaran masrayakat mengenai risiko keamanan siber dan cara melindungi diri saat online.
4. Peningkatan Kapasitas Sumber Daya Manusia: Mengembankan keahlian keamanan siber, termasuk pakar sektor publik dan swasta. Diharapkan dengan menerapkan rekomendasi tersebut, Indonesia dapat lebih siap menghadapi ancaman siber yang semakin kompleks, menjaga integritas informasi, dan menciptakan lingkungan digital yang aman dan andal.

DAFTAR PUSTAKA

Jurnal

Aswandi, R., Muchin, P. R. N., & Sultan, M. (2020). Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (Idps). *Legislatif*, 167-190.

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal*, *2*(2), 3.

Desmon, A. ., & Angelia, R. R. O. . (2022). Perlindungan Hukum Terhadap Data Pibadi User Aplikasi Digital Akibat Serangan Siber. *Science And Research Journal Of Mai Wandeu*, *2*(1), 38–47.

Hidayat. (2017) Tinjauan Yuridis Kewenangan Badan siber dan Sandi Negara Dalam Penanggulangan Serangan Siber. *S1 thesis, Universitas Mataram.*

Lana, A. (2021). Dampak Kejahatan Siber Terhadap Teknologi Informasi dan Pengendalian Internal.

Lauder Siagian, Arief Budiarto, Simatupang Simatupang. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional.

M. Yusuf Samad , Pratama Dahlian Persadha. (2022). Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara dalam Menangkal Ancaman Siber.

Muhammad Subhan Abdullah, & Heidiani Ikasari, I. (2023). Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan . *JRIIN :Jurnal Riset Informatika Dan Inovasi*, *1*(1), 96–98.

Prabowo, W., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. *Padjadjaran Journal of International Relations*, *1*(3), 218-239.

Raharjo, S., & Ekawati, F. (2022). Optimasi Perlindungan Data Dari Serangan Siber Dengan Synology Untuk Kelangsungan Bisnis Perusahaan. *Jurnal Ilmu Komputer*, *5*(2), 39-39.

Ramayanti, Arief Fahmi Lubis. (2023). Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam.

Tamarell Vimy, Surya Wiranto, Rudiyanto Rudiyanto, Pujo Widodo, Panji Suwarno (2022). Ancaman Seangan Siber Pada Keamanan Nasional Indonesia.

Utin Indah Permatasari. (2022**).** Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia**.**

Wahyu Beny Mukti Setiawan, Erifendi Churniawan, Femmy Silaswaty Faried. (2020). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan siber (Cyber Attack) Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia.

Buku

Beridiansyah. (2023). *Kejahatan* Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia Penerbit: *Syiah Kuala University Press*

Dr. Yurizal, Sh. MH. (2018). *Penegakan* Hukum Tindak Pidana Cyber Crime di Indonesia Penerbit: *Media Nusa Creative*

Idik Saeful Bahri. (2023). *Cyber* Crime dalam Sorotan Hukum. Penerbit: *Bahasa Rakyat*

Maskun, S.H., LL.M. (2022). *Kejahatan* Siber (Cyber Crime) Penerbit: *Prenada Media*

Nudirman Munir. (2017). *Pengantar* hukum siber Indonesia Penerbit: *Rajawali Pers*

Website Resmi

Permenhan No. 82 Tahun 2014 tentang Pertahanan Siber https://www.kemhan.go.id/pothan/2016/10/25/permenhan-no-82-tahun-2014-tentang-pertahanan-siber.html