(2023), 1 (6): 8–20 Kultura 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

PENERAPAN HUKUM DALAM MENANGGULANGI KEJAHATAN SIBER PENEGAKAN HUKUM TERHADAP TINDAK PIDANA SIBER

Muhammad Farhan[1)], Rajasa Syaefunaldi[2)], Dhifa Ridho Dwiputra Hidayat[3)], Asmak Ul Hosnah.[4)]
Fakultas Hukum Universitas Pakuan, Jalan Pakuan No. 1 Bogor 16143, Indonesia[1234]
Alamat e-mail : mhdfarhanbgr@gmail.com [1], syaefunaldi.rajasa@gmail.com[2], littedhifa@gmail.com [3], asmak.hosnah@unpak.ac.id [4].

Submitted: 16 December 2023 Accepted: 25 December 2023 Published: 26 December 2023

ABSTRACT

This discussion focuses on changes in law, especially changes to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) in Indonesia, which shows how important law enforcement is against cyber crime. While the speed of technological progress reinforces the need for continuous review and adjustment of laws, political complexities and the varying interests of involved parties often hinder the process of revising laws. Although they face limited resources and specialized expertise, the participation of law enforcement agencies is considered essential for the fight against cybercrime. It is vital to enhance the capabilities of these institutions, with an emphasis on concrete action and cooperation across sectors and countries. Despite challenges such as differences in legal system and cultures, international cooperation is essential to combat cybercrime worldwide. A holistic approach to law enforcement emphasizes cooperation between law enforcement agencies, the private sector, and society, while increasing public awareness and ongoing training for law enforcement personnel are considered essential to preventing cybercrime. The current focus is cybersecurity technology, with new products being created to detect, prevent, and respond more quickly to cybersecurity attacks. Involving the private sector in technology development is expected to make governments, businesses and law enforcement agencies work together. Overall, this discussion emphasized how important cross-sector and cross-country cooperation is to create a safer digital environment to face increasingly complex and growing cybercrime threats.

Keywords : *technology advances, law enforcement, cyber crime*

ABSTRAK

Pembahasan ini berfokus pada perubahan undang-undang, khususnya perubahan pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Indonesia, yang menunjukkan betapa pentingnya penegakan hukum terhadap kejahatan siber. Sementara kecepatan kemajuan teknologi memperkuat kebutuhan akan peninjauan dan penyesuaian hukum yang terus-menerus, kompleksitas politik dan berbagai kepentingan pihak terlibat sering menghalangi proses revisi undang-undang. Meskipun mereka menghadapi keterbatasan sumber daya dan keahlian khusus, partisipasi lembaga penegak hukum dianggap penting untuk pemberantasan kejahatan siber. Sangat penting untuk meningkatkan kemampuan lembaga ini, dengan penekanan pada tindakan konkret dan kerja sama lintas sektor dan negara. Meskipun dihadapkan pada tantangan seperti perbedaan sistem hukum dan budaya, kerja sama internasional sangat penting untuk memerangi kejahatan siber di seluruh dunia. Pendekatan holistik dalam penegakan hukum menekankan kerja sama antara lembaga penegak hukum, sektor swasta, dan masyarakat, sementara peningkatan kesadaran publik dan pelatihan berkelanjutan bagi personel penegak hukum dianggap penting untuk mencegah kejahatan siber. Fokus saat ini adalah teknologi keamanan siber, dengan produk baru yang diciptakan untuk mendeteksi, mencegah, dan merespons serangan keamanan siber lebih cepat. Melibatkan sektor swasta dalam pengembangan teknologi diharapkan membuat pemerintah, bisnis, dan lembaga penegak hukum bekerja sama. Secara keseluruhan, diskusi ini menekankan betapa pentingnya kerja sama lintas sektor dan lintas negara untuk menciptakan lingkungan digital yang lebih aman untuk menghadapi ancaman kejahatan siber yang semakin kompleks dan terus berkembang.

Kata Kunci : kemajuan teknologi, penegakan hukum, kejahatan siber.

Pendahuluan

Dalam mengevaluasi urgensi penerapan hukum untuk menangani kejahatan siber, perubahan legislasi menjadi elemen penting. Khususnya, revisi undang-undang, seperti yang

terjadi pada Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, mencerminkan upaya proaktif pemerintah untuk mengikuti perkembangan teknologi dan kejahatan siber. Walaupun demikian, proses revisi ini seringkali terhambat oleh kompleksitas sistem politik dan beragamnya kepentingan dari pihak-pihak yang terlibat.

Revisi undang-undang menjadi suatu keharusan mengingat kecepatan perkembangan teknologi yang dapat melampaui ketentuan hukum yang sudah ada. Oleh karena itu, upaya aktif untuk memantau dan mengevaluasi efektivitas undang-undang yang ada menjadi semakin penting. Kesiapan untuk melakukan penyesuaian juga harus dikedepankan agar hukum tetap relevan dalam menghadapi dinamika perubahan di dunia siber. Partisipasi lembaga penegak hukum dalam upaya pemberantasan kejahatan siber menjadi sangat vital, meskipun mereka seringkali dihadapkan pada sejumlah tantangan. Keterbatasan sumber daya, kurangnya keahlian khusus dalam bidang keamanan siber, dan ancaman dari pelaku kejahatan siber yang seringkali dapat menjaga anonimitasnya, semuanya merupakan faktor yang mempersulit tugas lembaga penegak hukum.

Karenanya, langkah-langkah konkret untuk meningkatkan kemampuan dan kapasitas lembaga penegak hukum menjadi sebuah kebutuhan mendesak. Kerja sama dan koordinasi baik di tingkat nasional maupun internasional menjadi kunci dalam memastikan bahwa lembaga penegak hukum dapat menjalankan tugasnya secara efektif. Ini melibatkan pertukaran informasi yang lebih efisien, partisipasi dalam program pelatihan bersama, dan pengembangan strategi bersama untuk menghadapi tantangan keamanan siber yang terus berkembang.

Aspek kerja sama internasional menjadi unsur kunci dalam upaya bersama melawan kejahatan siber, mengingat sifat transnasional dari jenis kejahatan tersebut. Kerja sama internasional melibatkan pertukaran informasi dan intelijen, bantuan hukum saling menguntungkan, harmonisasi kerangka hukum, dan partisipasi dalam forum multilateral. Walaupun demikian, kerja sama internasional juga dihadapkan pada tantangan seperti perbedaan sistem hukum dan budaya, serta kompleksitas koordinasi dan komunikasi. Proses revisi undang-undang dan peraturan seringkali mengalami hambatan, terutama karena kecepatan perkembangan teknologi yang sulit diikuti oleh perangkat hukum yang ada. Ketidakpastian hukum dan peran pihak ketiga, seperti industri teknologi, juga menjadi kendala serius. Diperlukan langkah-langkah yang hati-hati dan responsif untuk meningkatkan kecepatan proses legislatif, dengan melibatkan berbagai pihak dan mengakomodasi berbagai kepentingan.

Pendekatan holistik dalam penegakan hukum terhadap kejahatan siber menekankan kolaborasi antara lembaga penegak hukum, sektor swasta, dan masyarakat. Peningkatan kesadaran masyarakat tentang keamanan siber menjadi kunci untuk mencegah kejahatan siber, dan pelatihan berkelanjutan bagi personel lembaga penegak hukum sangat diperlukan agar mereka dapat menghadapi ancaman yang semakin kompleks di dunia maya.

Inovasi teknologi keamanan siber juga perlu menjadi fokus. Pengembangan dan penerapan solusi teknologi yang canggih dapat membantu dalam mendeteksi, mencegah, dan merespons lebih cepat terhadap serangan keamanan siber. Melibatkan sektor swasta dalam pengembangan teknologi keamanan siber dapat menciptakan sinergi yang kuat antara pemerintah, bisnis, dan lembaga penegak hukum.

latar belakang pembahasan ini menyoroti kompleksitas dan urgensi penegakan hukum terhadap kejahatan siber. Selain itu, menggarisbawahi perlunya kerja sama lintas sektor dan

lintas negara untuk menciptakan lingkungan digital yang lebih aman menjadi esensial dalam menghadapi ancaman yang semakin kompleks dan terus berkembang di dunia maya.[1]

Identifikasi Masalah

Berdasarkan diatas, Masalah yang diidentifikasi dalam penitilian ini akan dibahas antara lain sebagai berikut :
1. Bagaimana penerapan hukum dalam menanggulangi kejahatan siber?
2. Seperti apa penegakan hukum terhadap tindak pidana siber?
3. Bagaimana dampak penerapan hukum terhadap keamanan masyarakat?

Tujuan Penelitian

Berdasarkan hal-hal yang disebutkan di atas, tujuan dari penelitian ini adalah sebagai berikut :
1. Mengetahui suatu penerapan hukum dalam menanggulangi kejahatan siber;
2. Menganalisis seperti apa penegakan hukum terhadap tindak pidana siber;
3. Memberi pemahaman bagaimana suatu dampak dari penerapan hukum terhadap keamanan masyarakat.

Metode Penelitian

Metode penelitian dalam menginvestigasi peran undang-undang dan lembaga penegak hukum terhadap kejahatan siber dapat dilakukan melalui pendekatan studi literatur yang menyeluruh. Tahap awal penelitian ini akan dimulai dengan mengidentifikasi dan menganalisis undang-undang terkait kejahatan siber, khususnya mengulas revisi terakhir pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Dengan melibatkan tinjauan mendalam pada literatur hukum dan keamanan siber, peneliti akan mengevaluasi dampak dari perubahan tersebut terhadap upaya penegakan hukum terhadap para pelaku kejahatan siber. Pendekatan ini juga melibatkan pemahaman menyeluruh tentang peran lembaga penegak hukum, sebagaimana diatur dalam Undang-Undang Nomor 19 Tahun 2016, dengan fokus pada identifikasi tantangan yang dihadapi oleh lembaga-lembaga tersebut dalam mengatasi kejahatan siber.

Kajian literatur juga mencakup eksplorasi kerja sama internasional dalam penegakan hukum terhadap kejahatan siber, dengan penelitian detil pada ketentuan yang diuraikan dalam Peraturan Pemerintah Nomor 82 Tahun 2012 mengenai Penyelenggaraan Sistem dan Transaksi Elektronik. Peneliti akan menghimpun informasi dari berbagai sumber literatur untuk mengevaluasi efektivitas kerja sama internasional dalam menanggapi kejahatan siber yang melibatkan insiden atau pelaku yang melewati batas negara.

Tidak hanya itu, penelitian ini juga akan menelusuri hambatan dan tantangan yang dihadapi oleh lembaga penegak hukum, termasuk kendala sumber daya dan kesulitan dalam mengumpulkan bukti digital. Data dan informasi yang relevan akan diperoleh dari jurnal ilmiah, artikel, dan literatur terkait lainnya untuk menguraikan langkah-langkah yang perlu diambil guna meningkatkan kapasitas dan kemampuan lembaga penegak hukum. Pentingnya pendekatan multistakeholder dalam menanggulangi kejahatan siber akan dijelajahi melalui literatur yang membahas kolaborasi antara lembaga penegak hukum, sektor swasta, dan masyarakat. Penelitian ini akan mencari bukti empiris dan analisis dari literatur yang

[1] Djanggih, Hardianto, and Nurul Qamar. ‘Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)’. Pandecta Research Law Journal, vol. 13, no. 1, June 2018, pp. 10–23.

mendukung kebutuhan akan kerja sama ini untuk memperkuat penegakan hukum dan keamanan siber.

Dengan merinci metodologi penelitian ini melalui kajian literatur, diharapkan penelitian ini dapat memberikan pemahaman yang komprehensif mengenai efektivitas undang-undang dan lembaga penegak hukum dalam mengatasi tantangan yang dihadapi dalam menghadapi kejahatan siber. Selain itu, penelitian ini diharapkan memberikan pandangan yang konstruktif untuk penyempurnaan kebijakan di masa depan.

Hasil dan Pembahasan

1. Penerapan hukum dalam mengatasi kejahatan siber

Revisi undang-undang, seperti yang terjadi pada Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, memiliki peranan yang sangat penting untuk memastikan penegakan hukum yang efektif terhadap pelaku kejahatan Siber. Namun, seringkali proses revisi ini terkendala oleh kompleksitas sistem politik dan berbagai kepentingan dari berbagai pihak di beberapa negara. Selain itu, perkembangan pesat dalam teknologi membuat UU ITE dan perundang-undangan serupa menjadi usang atau tidak mampu menanggapi kejahatan Siber yang terus berkembang. Oleh karena itu, pemerintah dan lembaga penegak hukum perlu secara aktif memantau dan mengevaluasi efektivitas undang-undang yang ada, serta bersiap untuk melakukan penyesuaian atau amendemen agar tetap relevan dengan dinamika perkembangan dunia Siber.

Peran lembaga penegak hukum, seperti yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas UU ITE, menjadi sangat krusial dalam upaya pemberantasan kejahatan Siber. Tanggung jawab mereka mencakup deteksi, penyelidikan, penuntutan terhadap pelaku kejahatan Siber, serta tindakan pencegahan dan respons terhadap serangan Siber. Namun, lembaga-lembaga ini sering menghadapi sejumlah tantangan, seperti keterbatasan sumber daya, kurangnya keahlian dan pelatihan, kesulitan dalam mengumpulkan dan melestarikan bukti digital, ancaman anonimitas dan mobilitas pelaku kejahatan Siber, serta masalah yurisdiksi yang kompleks. Oleh karena itu, peningkatan kemampuan dan kapasitas lembaga penegak hukum, melalui kerja sama dan koordinasi baik di tingkat nasional maupun internasional, menjadi suatu keharusan untuk secara efektif menanggulangi kejahatan Siber.[2]

Aspek kerja sama internasional, sebagaimana diatur dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, menjadi elemen kunci dalam upaya bersama melawan kejahatan Siber, terutama ketika melibatkan insiden atau pelaku yang melintasi batas negara. Kejahatan Siber merupakan fenomena global tanpa batas negara, dan dampaknya melibatkan keamanan serta kepentingan banyak negara. Oleh karena itu, satu negara tidak dapat menangani kejahatan Siber sendiri, dan kerja sama serta bantuan dari negara-negara lain diperlukan. Kerja sama internasional melibatkan pertukaran informasi dan intelijen, bantuan hukum mutual, harmonisasi kerangka hukum, pengembangan standar dan praktik terbaik bersama, serta partisipasi dalam forum dan inisiatif multilateral. Meskipun demikian, kerja sama internasional juga dihadapkan pada tantangan, seperti perbedaan sistem hukum dan budaya, kurangnya kepercayaan politik, serta kompleksitas koordinasi dan

[2] Hosnah, A. U., Antoni, H., & Yofany, R. (2023). Law Enforcement Against Perpetrators of Defamation Through Social Media Based on the ITE Law. International Journal of Multicultural and Multireligious Understanding, 10(4), 362–372.

komunikasi.[3] Oleh karena itu, negara-negara perlu mengatasi hambatan ini dan membangun semangat saling menghormati dan bekerja sama untuk efektif menangani kejahatan Siber.

Dalam konteks undang-undang dan peraturan terkait kejahatan Siber, Undang-Undang ITE, seperti yang diatur dalam UU ITE dan Peraturan Kepolisian Negara Republik Indonesia Nomor 9 Tahun 2012 tentang Penyidikan Tindak Pidana di Bidang Teknologi Informasi dan Elektronika, menjadi landasan hukum utama yang mencakup kejahatan Siber. ITE memberikan dasar hukum bagi penuntutan pelaku kejahatan Siber dan menetapkan sanksi yang tegas. Perlindungan data pribadi juga menjadi pokok hukum penting, dengan undang-undang yang mengatur pengumpulan, penyimpanan, dan penggunaan data pribadi untuk melindungi warga negara dari penyalahgunaan oleh pihak yang tidak berwenang. Terdapat juga undang-undang yang menangani kejahatan Siber terkait dengan tindakan terorisme, mencakup serangan siber yang dapat merusak infrastruktur kritis atau menimbulkan ketakutan di masyarakat.

Namun, proses revisi undang-undang dan peraturan seringkali tidak berjalan lancar. Tantangan utama mencakup kecepatan perkembangan teknologi yang sulit diikuti oleh undang-undang, ketidakpastian hukum akibat interpretasi yang berbeda, serta peran pihak ketiga seperti industri teknologi, organisasi hak asasi manusia, dan kelompok advokasi yang dapat mempersulit mencapai keseimbangan yang tepat dalam revisi undang-undang.[4]

Untuk memperkuat peran lembaga penegak hukum, seperti yang diatur dalam Pedoman Pengamanan Siber Nasional 2017, peningkatan sumber daya menjadi hal yang sangat penting. Ini melibatkan pemberian sumber daya yang memadai, termasuk personel yang terlatih dan teknologi yang canggih, agar dapat menghadapi kejahatan Siber yang semakin kompleks. Pelatihan berkelanjutan menjadi kunci dalam menjaga pengetahuan yang terkini bagi personel lembaga penegak hukum, mengingat perkembangan teknologi yang terus berlangsung.

Kerja sama antar lembaga penegak hukum, badan intelijen, dan sektor swasta, seperti yang diatur dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Penanganan Situs Elektronik Bermuatan Negatif, menjadi elemen vital dalam upaya menanggulangi kejahatan Siber. Informasi yang saling dibagikan antara lembaga.

2. Penegakan Hukum terhadap Tindak Pidana Siber

Seiring dengan kemajuan teknologi informasi dan komunikasi, penegakan hukum terhadap tindak pidana siber menjadi semakin sulit. Untuk mengatasi tantangan ini, masyarakat harus dilindungi dari ancaman keamanan siber yang semakin beragam dan serius. Pemerintah, lembaga penegak hukum, dan sektor swasta harus bekerja sama untuk mengembangkan strategi tindak pidana siber yang efektif. Sifat lintas batas dari serangan siber merupakan salah satu tantangan utama bagi penegakan hukum terhadap kejahatan siber. Pelaku kejahatan siber dapat beroperasi dari negara mana pun dan menggunakan teknologi untuk menyembunyikan

[3] Ibid.

[4] Alameka, Dimas. SYSTEMATIC LITERATURE REVIEW: SEKTOR SERANGAN SIBER DAN METODE PENDETEKSI SERANGAN SIBER PADA WEBSITE PELAYANAN PUBLIK DI KALIMANTAN TIMUR. 2023.

identitas mereka, membuatnya lebih sulit untuk diidentifikasi dan ditangkap. Akibatnya, kolaborasi internasional sangat penting untuk penegakan hukum di ranah kejahatan siber.[5]

Banyak negara telah mengadopsi hukum dan regulasi yang mengkriminalkan tindak pidana siber, serta meningkatkan hukuman dan sanksi untuk memberikan efek jera kepada pelaku kejahatan siber. Selain itu, negara-negara ini juga memperkuat kerja sama internasional dalam hal pertukaran informasi, bukti, dan bantuan hukum untuk mendukung penegakan hukum terhadap tindak pidana siber.[6]

Untuk menangani kejahatan siber, lembaga penegak hukum di berbagai negara telah membentuk unit khusus yang terdiri dari ahli-ahli teknologi informasi, analis kejahatan siber, dan investigator yang dilatih khusus untuk menangani serangan keamanan siber. Unit-unit ini bekerja sama dengan sektor swasta, organisasi internasional, dan lembaga lainnya untuk mendeteksi, menyelidiki, dan menindak pelaku kejahatan siber. Selain itu, beberapa negara telah mengembangkan kebijakan dan strategi keamanan siber nasional untuk menghadapi ancaman kejahatan siber. Kebijakan ini mencakup perlindungan infrastruktur kritis, pencegahan serangan, dan respons cepat terhadap insiden keamanan siber. Strategi ini juga berfokus pada peningkatan kesadaran masyarakat tentang keamanan siber karena melibatkan partisipasi aktif masyarakat dalam melindungi diri mereka sendiri dan melaporkan kejadian yang terjadi.

Meskipun telah dilakukan banyak upaya dalam penegakan hukum terhadap tindak pidana siber, masih ada beberapa hambatan yang perlu diatasi. Salah satunya adalah tidak adanya peraturan internasional yang sama tentang kejahatan siber. Beberapa negara mungkin memiliki definisi, sanksi, dan proses penuntutan yang berbeda, yang dapat menyulitkan proses penegakan hukum lintas batas. Selain itu, peningkatan kapasitas dan keterampilan lembaga penegak hukum diperlukan karena ancaman keamanan siber yang terus meningkat. Penyidik dan ahli keamanan siber memerlukan pelatihan terus-menerus untuk mempertahankan keterampilan dan pengetahuan terbaru. Selain itu, penting untuk diingat bahwa penegakan hukum tidak boleh melanggar hak asasi manusia atau privasi orang; ini terutama berlaku untuk investigasi di dunia maya, yang dapat melibatkan pengawasan komunikasi dan akses ke data pribadi.

Secara keseluruhan, penegakan hukum tindak pidana siber adalah pekerjaan yang rumit dan dinamis. Untuk menciptakan lingkungan digital yang lebih aman, diperlukan pendekatan yang holistik yang melibatkan kerja sama antara pemerintah, lembaga penegak hukum, sektor swasta, dan masyarakat umum. Untuk menghadapi tantangan ini dan melindungi masyarakat dari ancaman kejahatan siber, kita perlu bekerja sama dan investasi yang berkelanjutan dalam kapasitas dan teknologi keamanan siber.

Sektor swasta harus bekerja sama untuk meningkatkan penegakan hukum terhadap tindak pidana siber. Banyak serangan keamanan siber dilakukan oleh kelompok kriminal dengan motivasi finansial. Oleh karena itu, kolaborasi dengan perusahaan teknologi, institusi keuangan, dan penyedia layanan online lainnya sangat penting. Perusahaan-perusahaan ini memiliki akses ke data yang dapat membantu penyelidikan dan memberi lembaga penegak hukum informasi penting. Pendidikan dan pelatihan sangat penting untuk penegakan hukum

[5] Jonimandala, Gian Wiatma, et al. ‘Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskim Polri Dalam Melakukan Penegakan Hukum Terhadap Kejahatan Pencurian Dan Penyalahgunaan Data Pribadi’. Innovative: Journal Of Social Science Research, vol. 3, no. 4

[6] RUSDI, ANTO. PENERAPAN PRINSIP EXTRATERRITORIAL JURISDICTION DALAM MEMERANGI TINDAK PIDANA SIBER. 2023. Universitas Mataram, skripsi. eprints.unram.ac.id

kejahatan siber. Penyidik dan ahli keamanan siber harus terus berlatih karena kemajuan teknologi yang cepat. Program pelatihan yang baik memastikan bahwa lembaga penegak hukum memiliki staf yang terampil dan siap menghadapi strategi yang terus berkembang dari pelaku kejahatan siber.

Sementara itu, mekanisme untuk melaporkan kejahatan siber dan kolaborasi pemerintah-swasta juga sangat penting. Inisiatif seperti memberikan insentif kepada bisnis yang melaporkan ancaman keamanan siber atau berbagi informasi dapat mendorong sektor swasta untuk berpartisipasi lebih aktif, yang dapat mempercepat deteksi dan penanganan kejadian keamanan siber. Seiring dengan itu, kebijakan yang berkaitan dengan privasi dan perlindungan data menjadi fokus utama dalam penegakan hukum kejahatan siber. Sangat penting untuk memastikan bahwa upaya penegakan hukum tidak mengganggu privasi orang. Oleh karena itu, ada peraturan yang jelas dan adil yang mengatur pengumpulan, penggunaan, dan penyimpanan data sesuai dengan hukum.

Selain itu, penggunaan teknologi keamanan siber yang canggih sangat penting dalam memerangi kejahatan siber.[7] Alat analisis keamanan, misalnya, yang dapat mendeteksi ancaman secara real-time, dan sistem keamanan yang tangguh dapat membantu memperkuat pertahanan terhadap serangan siber. Pemerintah dan perusahaan swasta harus menginvestasikan uang dalam penelitian dan pengembangan teknologi ini agar para pelaku kejahatan siber tetap berada di belakang mereka. Pertahanan terhadap serangan negara atau kelompok yang menggunakan kejahatan siber sebagai instrumen kebijakan luar negeri harus mendapat perhatian khusus. Ini dapat mencakup serangan terhadap infrastruktur vital, pencurian data rahasia, atau tindakan siber lainnya yang dapat mengancam keamanan negara. Di tingkat internasional, strategi penegakan hukum mempertimbangkan mekanisme respons dan detterance terhadap serangan jenis ini.

Hakim, jaksa, dan advokat perlu memahami kompleksitas teknis kejahatan siber untuk memastikan proses peradilan yang adil dan efektif. Lembaga penegak hukum dan sistem peradilan pidana keduanya membutuhkan peningkatan kemampuan penyelidikan kejahatan siber.

Selain itu, masyarakat harus dididik tentang keamanan siber, yang harus menjadi bagian integral dari kurikulum pendidikan. Ini akan membantu siswa memahami risiko dan langkah-langkah yang dapat diambil untuk melindungi diri mereka saat berada di internet. Tidak dapat diabaikan betapa pentingnya membuat hukum yang dapat menyesuaikan diri dengan cepat dengan kemajuan teknologi. Untuk memerangi kejahatan siber yang berkembang pesat, proses legislatif yang cepat dan responsif diperlukan. Ini membutuhkan kerja sama pemerintah, lembaga penegak hukum, pakar hukum, dan teknologi. Dalam situasi seperti ini, kerja sama antara sektor swasta dan pemerintah untuk membuat kebijakan dan regulasi yang sesuai dengan kemajuan teknologi merupakan kemajuan yang baik. Dengan bekerja sama, penegakan hukum terhadap kejahatan siber dapat menjadi lebih efisien, responsif, dan sesuai dengan zaman sambil memastikan hak asasi manusia dan privasi dilindungi.

1. Kolaborasi dengan Sektor Swasta

Lembaga penegak hukum dapat memperoleh informasi penting dari kolaborasi dengan perusahaan teknologi, lembaga keuangan, dan penyedia layanan online. Untuk mendeteksi,

[7] adminprodi. Meningkatkan Keamanan Siber: Pentingnya Perlindungan Data Di Era Digital - Fakultas Ilmu Komputer. 6 Mar. 2023, https://fasilkom.esaunggul.ac.id/meningkatkan-keamanan-siber-pentingnya-perlindungan-data-di-era-digital/.

melacak, dan menindak pelaku kejahatan siber, kerja sama ini dapat melibatkan pertukaran data dan informasi.

2. Pendidikan dan Pelatihan

Keterampilan penyidik dan ahli keamanan siber harus ditingkatkan melalui pelatihan terus-menerus karena teknologi terus berkembang. Ini memastikan bahwa lembaga penegak hukum memiliki staf yang terampil yang dapat menangani strategi baru pelaku kejahatan siber.

3. Mekanisme Pelaporan dan Kerjasama

Mekanisme pelaporan dan kerjasama yang efektif antara sektor swasta dan pemerintah dapat mempercepat deteksi dan penanganan kejadian keamanan siber. Inisiatif insentif untuk perusahaan yang melaporkan ancaman keamanan siber atau berbagi data juga dapat mendorong partisipasi aktif.

4. Kebijakan Privasi dan Perlindungan Data

Dalam proses penegakan hukum, privasi dan data harus dilindungi. Peraturan yang jelas dan adil diperlukan untuk mengatur penggunaan data dalam proses penegakan hukum, memastikan bahwa hak asasi manusia dan privasi individu tetap dilindungi.\

5. Teknologi Keamanan Siber

Investasi dalam alat analisis keamanan real-time dan sistem keamanan yang kuat dapat membantu melawan serangan siber dan mendeteksi ancaman dengan lebih baik.

6. Pertahanan Terhadap Serangan Negara

Mekanisme untuk menanggapi dan menangkal serangan siber dari negara atau kelompok tertentu sangat penting. Untuk melindungi keamanan nasional dari ancaman ini, diperlukan strategi tingkat internasional dan kerja sama.

7. Peningkatan Kapasitas dalam Sistem Peradilan Pidana

Untuk memastikan bahwa proses peradilan berjalan dengan adil dan efektif, hakim, jaksa, dan advokat harus memahami kompleksitas teknis kejahatan siber.

8. Pemberdayaan Masyarakat

Pendidikan siber yang melibatkan masyarakat dapat membantu orang melindungi diri dari ancaman keamanan siber. Peningkatan kesadaran akan ancaman dan langkah-langkah penting untuk melindungi diri saat berinteraksi di internet sangat penting.

9. Responsif terhadap Perkembangan Teknologi

Percepatan proses legislatif diperlukan untuk memerangi kejahatan siber yang berkembang pesat. Ini membutuhkan pemerintah, lembaga penegak hukum, pakar hukum, dan teknologi untuk bekerja sama.

10. Kerjasama Internasional

Kerja sama di seluruh dunia untuk berbagi informasi, bukti, dan bantuan hukum sangat penting untuk menangani tindak pidana siber internasional. Proses penegakan hukum dapat difasilitasi dengan harmonisasi hukum internasional.

11. Regulasi dan Standarisasi

Peraturan dan standarisasi yang lebih baik tentang keamanan siber dapat membantu penegakan hukum di tingkat nasional dan internasional. Negara-negara dan sektor-sektor yang berbeda dapat memperoleh lebih banyak informasi melalui penerapan standar yang seragam

untuk keamanan siber, yang menciptakan kerangka kerja yang lebih kuat untuk melawan serangan siber.

12. Respons Publik dan Keterlibatan Aktif

Reaksi publik yang aktif terhadap kejahatan siber dapat membantu dalam deteksi dan laporan serangan. Dengan mengenali perilaku mencurigakan atau serangan yang mungkin, masyarakat yang telah kehilangan pengetahuan tentang tindakan keamanan siber dapat menjadi mitra yang efektif dalam upaya penegakan hukum. Akibatnya, upaya pendidikan dan kampanye kesadaran publik harus ditingkatkan untuk mendorong partisipasi masyarakat.

13. Riset dan Inovasi Teknologi

Sangat penting bagi pemerintah dan sektor swasta untuk terlibat aktif dalam riset dan inovasi teknologi keamanan siber. Investasi dalam proyek riset yang mendukung pengembangan teknologi keamanan siber terdepan dapat memberikan keuntungan strategis dalam menghadapi ancaman siber yang terus berkembang. Dengan keterlibatan industri, universitas, dan lembaga penelitian dalam ekosistem inovasi ini, solusi yang lebih efisien dapat diadopsi secara luas dalam penegakan hukum.

14. Pemantauan dan Analisis Terus Menerus

Untuk memahami strategi kejahatan siber yang berkembang, unit keamanan siber di lembaga penegak hukum harus dapat memantau dan menganalisis tren keamanan siber secara terus menerus. Ini berarti mereka harus dapat memantau ancaman secara real-time, menganalisis pola serangan, dan mengambil tindakan cepat. Kapasitas untuk memantau dan menganalisis data ini dapat ditingkatkan dengan penggunaan AI dan analisis big data.

15. Kerjasama dengan Lembaga Internasional

Kerjasama dengan lembaga seperti Interpol dan Europol dapat membantu memperkuat jaringan penegakan hukum di seluruh dunia. Ini termasuk penyelenggaraan operasi bersama, pelatihan bersama, dan komunikasi informasi yang lebih efektif. Membangun hubungan yang erat dengan lembaga-lembaga ini dapat membantu negara mengatasi ancaman siber dengan lebih baik.

16. Membangun Tim Ahli Multidisiplin

Suatu keharusan untuk membentuk tim yang terdiri dari ahli hukum, teknologi informasi, dan keamanan siber. Jenis tim ini dapat bekerja sama untuk memaksimalkan penyelidikan dan pengejaran pelaku kejahatan siber. Selain itu, kerja sama antardisiplin ini dapat meningkatkan pemahaman tentang elemen teknis dan hukum yang terlibat dalam penanganan tindak pidana siber.

Penegakan hukum terhadap tindak pidana siber dapat menjadi lebih luas, fleksibel, dan efektif jika semua komponen ini digabungkan. Semua pihak, mulai dari lembaga pemerintah dan penegak hukum hingga sektor swasta, komunitas, dan lembaga internasional, harus terlibat dalam pendekatan yang menyeluruh ini.

3. Penerapan hukum terhadap kejahatan siber memiliki dampak signifikan pada keamanan masyarakat

Penerapan hukum terhadap kejahatan siber berdampak besar pada keamanan masyarakat.[8] Kejahatan ini, yang mencakup aktivitas ilegal menggunakan komputer, jaringan, atau sistem informasi, muncul dalam berbagai bentuk seperti peretasan, phishing, pencurian identitas, cyberbullying, terorisme siber, dan perang siber. Dampaknya dapat merugikan individu, organisasi, dan negara, termasuk kerugian finansial, kerusakan reputasi, tekanan psikologis, kekerasan fisik, dan ancaman terhadap keamanan nasional.[9]

Memiliki kerangka hukum yang efektif dan mekanisme penegakan hukum menjadi penting untuk mencegah, menghambat, dan menghukum kejahatan dunia maya. Namun, penerapan hukum dalam bidang ini dihadapkan pada beberapa tantangan, seperti:

1. Sifat Transnasional Kejahatan Siber

Kejahatan siber sering melibatkan beberapa negara, membuat sulit menentukan yurisdiksi, kedaulatan, dan hukum yang berlaku di berbagai negara yang terlibat.

2. Anonimitas dan Enkripsi Pelaku

Kesulitan dalam mengidentifikasi, melacak, dan mengumpulkan bukti karena pelaku kejahatan siber sering bersifat anonim dan menggunakan enkripsi.

3. Perkembangan Cepat Teknologi

Teknologi berkembang pesat, menciptakan bentuk kejahatan baru yang melampaui regulasi dan hukum yang ada.

4. Kurangnya Kesadaran dan Kerja Sama

Kurangnya kesadaran dan kerja sama antara pemerintah, lembaga penegak hukum, sektor swasta, masyarakat sipil, dan organisasi internasional.

Untuk mengatasi tantangan ini, beberapa solusi yang dapat diimplementasikan meliputi:

1. Konvensi dan Perjanjian Universal atau Regional

Membangun dan mengadopsi konvensi dan perjanjian universal atau regional tentang kejahatan dunia maya, sejalan dengan Konvensi Dewan Eropa tentang Kejahatan Dunia Maya.

2. Peningkatan Kapasitas Penegakan Hukum

Meningkatkan kapasitas dan kemampuan lembaga penegak hukum untuk menyelidiki dan menuntut kejahatan siber melalui pelatihan, peralatan, dan pembentukan unit khusus.

3. Kerja Sama Antar-Sektor

Mempromosikan kerja sama antara pemerintah, lembaga swasta, dan masyarakat sipil melalui platform berbagi informasi, gugus tugas, dan perjanjian bantuan hukum timbal balik.

4. Pendidikan dan Kesadaran Publik

[8] Pengertian Cyber Crime dan Cyber Law – BAPENDA JABAR. https://bapenda.jabarprov.go.id/2017/11/07/pengertian-cyber-crime-dan-cyber-law/.

[9] Aptika, Admin. “Kebijakan Keamanan Dan Pertahanan Siber.” Ditjen Aptika, 10 Mar. 2016, https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/.

Meningkatkan kesadaran dan pendidikan publik tentang risiko kejahatan siber melalui kampanye, lokakarya, dan pengembangan pedoman keamanan siber.

5. Penguatan Hukum Nasional

Meninjau dan memperbarui undang-undang nasional untuk mencakup aspek baru kejahatan siber dan beradaptasi dengan perkembangan teknologi.

Melalui langkah-langkah ini, diharapkan dapat dibangun fondasi hukum yang kuat untuk melawan kejahatan siber. Pentingnya kerja sama internasional juga perlu ditekankan, dengan perjanjian bilateral dan forum internasional seperti INTERPOL dan UNODC menjadi kunci. Tantangan anonimitas dan enkripsi dapat diatasi melalui penelitian dan pengembangan teknologi keamanan siber, melibatkan sektor swasta dan pemerintah. Pembaruan regulasi yang cepat juga diperlukan untuk mengikuti perkembangan teknologi.

Pendekatan holistik dalam pendidikan dan kesadaran masyarakat harus diterapkan sejak dini. Kampanye kesadaran publik harus melibatkan semua lapisan masyarakat untuk memastikan pemahaman luas tentang ancaman kejahatan siber. Keterlibatan aktif dan dukungan dari berbagai pihak, termasuk sektor swasta, akademisi, dan masyarakat sipil, sangat penting dalam mengatasi tantangan ini. Dengan bersama-sama menghadapi tantangan global, kita dapat membangun fondasi yang lebih kokoh untuk melindungi masyarakat dari dampak merugikan kejahatan siber. Sebagai kesimpulan, penerapan hukum terhadap kejahatan siber memerlukan pendekatan holistik dan terkoordinasi. Dengan kerja sama internasional, pembaruan regulasi yang cepat, peningkatan kapasitas lembaga penegak hukum, dan edukasi masyarakat, kita dapat menuju dunia maya yang lebih aman dan terlindungi.

Kesimpulan

Untuk melindungi masyarakat dari ancaman kejahatan siber, penerapan hukum yang kuat dan penegakan hukum yang tepat sangat penting. Dengan berkembangnya teknologi digital, diperlukan perhatian serius terhadap aspek hukum untuk melindungi orang dan organisasi dari ancaman dunia maya. Oleh karena itu, diperlukan upaya terus-menerus dalam mengembangkan strategi dan kerja sama lintas batas untuk menjaga keamanan dunia maya di masa depan. Kejahatan siber telah berkembang menjadi ancaman global yang tidak mengenal batas. Oleh karena itu, kerja sama yang kuat antar negara diperlukan untuk mengatasi masalah ini. Penting untuk memahami bahwa masalah keamanan siber bersifat internasional dan nasional. Jurnal ini bertujuan untuk memberikan wawasan mendalam tentang fungsi hukum dalam menangani kejahatan siber dalam konteks ini dan menggarisbawahi pentingnya penegakan hukum yang efektif untuk melindungi masyarakat.

Pembuatan undang-undang yang kuat dan relevan merupakan komponen penting dalam menanggulangi kejahatan siber. Untuk mengikuti perkembangan teknologi yang cepat, undang-undang harus mampu menetapkan hukuman yang sebanding dengan tingkat kejahatan. Pengembangan undang-undang seperti ini membutuhkan pemahaman yang mendalam tentang teknologi informasi. Selain itu, ahli hukum, pakar teknologi, dan pihak berkepentingan lainnya harus terlibat dalam proses tersebut. Jurnal ini menekankan betapa pentingnya mengkaji dan memperbarui undang-undang saat ini untuk menanggapi perubahan dalam lanskap keamanan siber.[10] Namun, legislasi saja tidak cukup. Untuk menjaga dunia digital aman, penegakan

[10] Peran Penting Cyber Security Dalam Melindungi Data Dan Privasi. https://www.deltadatamandiri.com/post/peran-penting-cyber-security-dalam-melindungi-data-dan-privasi. Accessed 10 Nov. 2023.

hukum yang kuat juga penting. Dalam banyak negara, menegakkan hukum terkait kejahatan siber sulit karena kekurangan sumber daya manusia yang memadai dan kurangnya pemahaman tentang kompleksitas kejahatan tersebut. Akibatnya, perlu ada pembiayaan yang signifikan dalam pelatihan penegak hukum dan tenaga hukum yang memiliki pemahaman yang mendalam tentang lingkungan kejahatan siber.

Kerjasama internasional juga menjadi penting dalam menangani kejahatan siber karena kejahatan siber sering melibatkan pelaku yang beroperasi dari berbagai wilayah, sehingga kerjasama internasional sangat penting untuk mengidentifikasi, mengejar, dan mengadili pelaku kejahatan tersebut. Jurnal ini menunjukkan betapa pentingnya bekerja sama dengan negara lain lebih banyak dalam hal berbagi informasi, pelatihan, dan koordinasi tindakan penegakan hukum. Selain elemen penegakan hukum, upaya preventif juga sangat penting dalam memerangi kejahatan siber. Pendidikan masyarakat tentang ancaman keamanan siber, promosi keamanan digital, dan peningkatan kesadaran tentang tindakan preventif dapat membantu mengurangi jumlah kejahatan siber yang terjadi. Jurnal ini mendorong peningkatan upaya pencegahan, seperti kampanye kesadaran masyarakat dan program pendidikan keamanan siber di tingkat nasional.

hukum tidak boleh diabaikan dalam menangani kejahatan siber. Untuk menjaga dunia digital aman, undang-undang yang kuat dan penegakan hukum yang baik sangat penting. Untuk menghadapi ancaman yang tersebar di seluruh dunia, kerja sama internasional sangat penting. Jurnal ini diharapkan dapat meningkatkan pemahaman kita tentang bagaimana hukum dapat berfungsi sebagai alat yang efektif untuk melindungi masyarakat dari ancaman kejahatan siber di era komputer dan internet saat ini.

Referensi

Perundang-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Peraturan Pemerintah Nomor 82 Tahun 2012 mengenai Penyelenggaraan Sistem dan Transaksi Elektronik

Lain-lain

Alameka, Dimas. "SYSTEMATIC LITERATURE REVIEW: SEKTOR SERANGAN SIBER DAN METODE PENDETEKSI SERANGAN SIBER PADA WEBSITE PELAYANAN PUBLIK DI KALIMANTAN TIMUR." 2023. Institut Pemerintahan Dalam Negeri, other. eprints.ipdn.ac.id, http://eprints.ipdn.ac.id/14989/.

adminprodi. "Meningkatkan Keamanan Siber: Pentingnya Perlindungan Data Di Era Digital - Fakultas Ilmu Komputer." 6 Mar. 2023, https://fasilkom.esaunggul.ac.id/meningkatkan-keamanan-siber-pentingnya-perlindungan-data-di-era-digital/.

Aptika, Admin. “Kebijakan Keamanan Dan Pertahanan Siber.” Ditjen Aptika, 10 Mar. 2016, https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/.

Djanggih, Hardianto, and Nurul Qamar. ‘Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)’. Pandecta Research Law Journal, vol. 13, no. 1, June 2018, pp. 10–23. journal.unnes.ac.id, https://doi.org/10.15294/pandecta.v13i1.14020.

Hosnah, A. U., Antoni, H., & Yofany, R. (2023). "Law Enforcement Against Perpetrators of Defamation Through Social Media Based on the ITE Law." International Journal of Multicultural and Multireligious Understanding, 10(4), 362–372. Retrieved 6 November 2023 from https://doi.org/10.18415/ijmmu.v10i4.4643.

Jonimandala, Gian Wiatma, et al. 'Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskim Polri Dalam Melakukan Penegakan Hukum Terhadap Kejahatan Pencurian Dan Penyalahgunaan Data Pribadi'. Innovative: Journal Of Social Science Research, vol. 3, no. 4, Aug. 2023, pp. 680–92. j-innovative.org, https://doi.org/10.31004/innovative.v3i4.2874.

Pengertian Cyber Crime dan Cyber Law – BAPENDA JABAR. https://bapenda.jabarprov.go.id/2017/11/07/pengertian-cyber-crime-dan-cyber-law/.

Peran Penting Cyber Security Dalam Melindungi Data Dan Privasi. https://www.deltadatamandiri.com/post/peran-penting-cyber-security-dalam-melindungi-data-dan-privasi. Accessed 10 Nov. 2023.

RUSDI, ANTO. "PENERAPAN PRINSIP EXTRATERRITORIAL JURISDICTION DALAM MEMERANGI TINDAK PIDANA SIBER." 2023. Universitas Mataram, skripsi. eprints.unram.ac.id, http://eprints.unram.ac.id/34376/.