Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia

Rahma Agri Firdaus
UIN Sunan Kalijaga Yogyakarta
E-mail: *23103040159@student.uin-suka.ac.id*

Abstract: *This research discusses aspects of legal protection and prevention of cybercrime in the digital era in the Indonesian legal system. The purpose of the research is to evaluate the effectiveness of criminal provisions in the Electronic Information and Transaction Law (ITE Law) and the role of the Personal Data Protection Law (PDP Law) as a preventive instrument. The research method used is a normative research model with a statutory approach to examine the text of the law and a philosophical approach to outline the urgency of legal protection related to cybercrime, as well as a conceptual approach to assess the suitability of norms against the legal objectives of justice, legal certainty, and expediency in the context of cyber resilience. The data analysis technique is carried out using a descriptive-qualitative model. The results show that the development of the digital world through technology and information has had an impact on the development of data security issues and the orderly use of internet technology. In Indonesia, the ITE Law has established various cyber offences with criminal sanctions, there are still overlapping norms, cross-border jurisdictional constraints, and still faced with limited digital forensic capacity of law enforcement officials. Meanwhile, the PDP Law provides a foundation for institutions and risk mitigation mechanisms through data protection, but has not been systemically integrated with criminal instruments. Thus, the main challenge of legal protection against cyber crime in the digital era is the synchronisation and optimisation of regulations and supporting tools in order to achieve cyber resilience and security*.
Keywords: *Cyber Crime; Digitalization; Legal Protection; Criminal.*

Abstrak
Penelitian ini membahas aspek perlindungan hukum dan pencegahan kejahatan siber di era digital dalam sistem hukum di Indonesia. Tujuan penelitian adalah mengevaluasi efektivitas ketentuan pidana dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta peran Undang-Undang Perlindungan Data Pribadi (UU PDP) sebagai instrumen preventif. Metode penelitian yang digunakan adalah model penelitian normatif dengan pendekatan perundang-undangan (*statute approach*) untuk menelaah teks undang-undang dan pendekatan filosofis (*philosophical approach*) untuk menguraikan urgensi perlindungan hukum terkait cybercrime, serta pendekatan konseptual untuk menilai kesesuaian norma terhadap tujuan hukum keadilan, kepastian hukum, dan kemanfaatan dalam konteks ketahanan

siber. Teknik analisis data dilakukan menggunakan model deskriptif-kualitatif. Hasil penelitian menunjukkan bahwa perkembangan dunia digital melalui teknologi dan informasi telah berdampak pada berkembangnya masalah keamanan data dan tata tertib penggunaan teknologi internet. Di Indonesia telah ada UU ITE telah menetapkan berbagai delik maya dengan sanksi pidana, masih terdapat tumpang tindih norma, kendala yurisdiksi lintas negara, dan masih dihadapkan keterbatasan kapasitas forensik digital aparat penegak hukum. Sementara itu, UU PDP memberikan landasan tentang kelembagaan dan mekanisme mitigasi risiko melalui perlindungan data, namun belum terintegrasi secara sistemik dengan instrumen pidana. Degan demikian tantangan utama perlindungan hukum terhadap kejahatan cyber di era digital adalah sinkronisasi serta optimalisasi regulasi dan perangkat pendukung yang mumpuni dalam rangka mencapai ketahanan dan keamanan cyber.

Kata kunci: *Cyber Crime; Digitalisasi; Perlindungan Hukum; Pidana.*

Pendahuluan

Hukum pidana siber adalah cabang dari hukum pidana yang khusus mengatur tentang tindak pidana yang dilakukan dengan menggunakan teknologi informasi dan komunikasi (TIK), terutama internet. Kejahatan siber, juga dikenal sebagai kejahatan dunia maya atau *cybercrime*, mencakup berbagai kegiatan ilegal yang memanfaatkan komputer, jaringan komputer, dan perangkat digital lainnya. Ruang lingkup hukum pidana siber meliputi berbagai aspek yang berkaitan dengan pengaturan, pencegahan, penyelidikan, dan penindakan terhadap Kejahatan Siber.[1]

Cyber Crime sering disebut sebagai pelanggaran komputer. Hamzah mendefinisikan cyber crime sebagai "*kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal*"[2], sedangkan Wisnubroto dalam bukunya mendefinisikan kejahatan komputer sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan komputer sebagai sarana atau alat atau komputer

[1] Muhammad Anthony Aldriano dan Mas Agus Priyambodo, "Cyber Crime Dalam Sudut Pandang Hukum Pidana," *Jurnal Kewarganegaraan* 6, no. 1 (2022).

[2] Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer* (Jakarta: Sinar Grafika, 1989).

sebagai objek, baik untuk keuntungan atau tidak, dengan merugikan pihak lain.[3]

Era digital yang terus berkembang pesat saat ini, yaitu berupa internet dan teknologi informasi telah menjadi bagian penting dari kehidupan sehari-hari. Namun, perkembangan tersebut juga tidak terlepas dari munculnya kejahatan dunia maya dikenal sebagai Kejahatan Siber muncul sebagai masalah baru seiring perkembangan teknologi dan memiliki akibat yang serius baik pada tingkat individu maupun kolektif.[4] Penipuan online, pencurian identitas, serangan *malware*, peretasan, dan penyalahgunaan data pribadi adalah contoh kejahatan dunia maya yang dilakukan melalui jaringan komputer dan Internet.[5] Kejahatan dunia maya menjadi semakin kompleks dan meluas, berdampak pada individu, organisasi, dan negara karena perkembangan pesat teknologi informasi dan komunikasi. Berbagai aspek kehidupan, seperti ekonomi, pendidikan, dan kesehatan, telah sangat berubah selama era digital. Kejahatan siber memiliki dampak negatif pada ekonomi, keamanan, dan privasi individu, dan dapat menyebabkan kerugian finansial besar. Mereka juga dapat merusak reputasi, menimbulkan ketidakamanan, dan menimbulkan ketakutan di masyarakat. Oleh karena itu, penanganan kejahatan siber sangat penting.

Kejahatan di masa sekarang ini tidak lagi sama dengan kejahatan secara konvensional, yaitu kejahatan yang perbuatannya dilakukan secara langsung di depan manusia, akan tetapi kejahatan digital memakai teknologi yang sedang berkembang saat ini yang dapat dilakukan dimana saja menggunakan teknologi – teknologi masa sekarang seperti Laptop, Komputer, Handphone, dan lain-lainnya selama terdapat akses Internet dan fasilitas gadget yang memadai, sehingga kejahatan tersebut dapat di lakukan pelaku kejahatan siber dengan mudah. Internet sendiri pada awal mula adalah suatu jaringan

---

[3] Aloysius Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer* (Penerbitan Universitas Atma Jaya Yogyakarta, 1999), https://books.google.co.id/books?id=aigRAgAACAAJ.

[4] Unair News, "Analisis Ancaman dan Respon Keamanan Siber di Indonesia," 2024, https://unair.ac.id/analisis-ancaman-dan-respon-keamanan-siber-di-indonesia/.

[5] Kadek Rima Anggen Suari dan I Made Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (25 April 2023): 132–42, https://doi.org/10.38043/jah.v6i1.4484.

komunikasi digital yang sampai saat ini telah menghubungkan hampir seluruh dunia melalui jaringan, oleh karenanya terasa tidak ada jarak antara satu negara dengan negara lainnya.

Perkembangan Kejahatan Siber atau *Cyber Crime* telah menjadi masalah besar di era komputer dan internet saat ini. Dalam hal ini, masalah utama yang muncul mencakup beberapa elemen penting. Pertama, kejahatan siber menyebabkan kerugian ekonomi yang sangat besar. Banyak kasus penipuan online yang merugikan orang dan bisnis secara finansial, seperti *phishing*, pencurian identitas, dan penipuan kartu kredit, yang sering kali melibatkan skema rumit dan sulit dilacak. Kedua, masalah keamanan dan privasi menjadi perhatian utama. Semakin banyak pelanggaran data pribadi dan perusahaan yang terjadi, lebih banyak orang yang dapat mengakses informasi sensitif, yang mengancam privasi individu dan keamanan perusahaan. Ketiga, regulasi dan hukum yang rumit membuatnya sulit.

Cyber Crime apabila ditinjau aspek realitas hukum yang ada seringkali tidak dapat mengikuti perkembangan teknologi yang cepat, yang menyebabkan kesenjangan dalam regulasi dan penegakan hukum kejahatan siber. Selain itu, berbagai lembaga penegak hukum harus bekerja sama dengan baik untuk menangani kejahatan siber. Selain itu, terdapat aspek berkaitan dengan kesadaran masyarakat akan teknologi masih rendah. Banyak masyarakat tidak menyadari sepenuhnya bahaya kejahatan siber dan cara melindungi diri, yang membuat mereka rentan terhadap serangan siber. Literasi digital masih rendah juga menghambat orang dan organisasi untuk mengambil langkah-langkah pencegahan yang efektif terhadap ancaman siber.[6]

Beberapa faktor tersebut mempengaruhi bagaimana penanganan kejahatan siber menghadapi kendala teknis di mana metode serangan siber yang semakin canggih tidak dapat diatasi oleh teknologi keamanan siber yang ada, membuat celah yang dapat dieksploitasi oleh pelaku kejahatan. Selain itu, ada kekurangan tenaga kerja yang terlatih dalam keamanan siber dan teknologi informasi. Keenam, kejahatan siber sangat menantang bagi penegakan hukum disebabkan pelaku kejahatan siber dapat bekerja dari berbagai tempat dan menggunakan teknik yang

[6] Indonet, "Faktor yang menyebabkan Kejahatan Siber Mudah Terjadi," t.t., https://indonet.co.id/id/12-faktor-penyebab-kejahatan-siber-mudah-terjadi/.

menyulitkan pelacakan, identifikasi dan penangkapan mereka sering kali sulit.

Kajian literatur terkait dengan perkembangan kejahatan *cyber* ditinjau dari aspek hukum, khususnya hukum pidana telah menunjukkan bahwa persoalan tersebut sangat krusial untuk diatasi secara efektif. Kajian pertama berkaitan dengan tindak pidana cyber dan penegakannya menunjukkan hasil masih adanya celah kekosongan hukum terutama model kejahatan yang bentuknya tidak lagi secara konvensional, melainkan sudah berbasis digital, sehingga aturan seperti KUHP dan UU ITE saat ini belum mumpuni mengatasi masalah tersebut.[7] Kajian berikutnya terkait dengan kasus peretasan data nasional di Pusat Data Nasional oleh Hacker menunjukkan aspek perlindungan yang lemah terhadap keamanan data digital di Indonesia. Instrumen hukum mampu memberikan landasan tentang kepastian dan efektivitas dalam hal perlindungan data pribadi dari kejahatan *cyber*.[8] Kajian terkait yang terakhir menunjukkan adanya urgensi terhadap paradigma hukum pidana modern yang harus lebih adaptif terhadap munculnya kejahatan model baru, dimana tantangan terkait pembuktian serta penentuan subjek akan semakin rumit, sehingga sistem hukum pidana di Indonesia khususnya perlu dikembangkan kembali.[9]

Melalui berbagai telaah pustaka diatas, serta berbagai uraian pendukung lainnya, penelitian ini akan berfokus pada kajian bagaimana penerapan hukum pidana dalam menghadapi serta pencegahan Kejahatan Siber di era digital serta bagaimana dimensi tujuan hukum terhadap perlindungan dan penegakan hukum siber di Indonesia dalam kerangka hukum positif mengenai ketahanan siber. Urgensi penelitian ini terletak pada Gambaran bahwa kejahatan siber (*cybercrime*) terus mengalami eskalasi atau perkembangan model serta dampak seiring

[7] Rafi Septia Budianto Pansariadi dan Noenik Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya," *Binamulia Hukum* 12, no. 2 (20 Desember 2023): 287–98, https://doi.org/10.37893/jbh.v12i2.605.

[8] Annisa Nadya Putri, "Upaya Hukum dalam Strategi Perlindungan Data pada Penggunaan Internet Studi Kasus : Hacker Bjorka," *Jurnal Hukum dan Pembangunan Ekonomi* 12, no. 1 (31 Juli 2024): 52, https://doi.org/10.20961/hpe.v12i1.81910.

[9] Miftakhur Rokhman Habibi dan Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23, no. 2 (19 Desember 2020): 400–426, https://doi.org/10.15642/alqanun.2020.23.2.400-426.

dengan ketergantungan masyarakat terhadap teknologi informasi. Fenomena tersebut tidak hanya menimbulkan kerugian ekonomi dan pelanggaran privasi, tetapi juga berpotensi mengancam ketertiban umum dan keamanan nasional. Dalam konteks hukum pidana, cybercrime telah diakui sebagai bentuk tindak pidana di dunia maya (delik maya) yang membutuhkan pendekatan hukum yang berbeda dari kejahatan konvensional, baik dari segi pembuktian, yurisdiksi, hingga penegakan hukumnya. Perkembangan jenis dan modus kejahatan digital yang kompleks dan lintas batas menuntut sistem hukum pidana yang responsif, adaptif, serta mampu memberikan efek jera melalui instrumen hukum yang tepat sasaran. Oleh karena itu, analisis terhadap strategi menghadapi dan mencegah kejahatan siber menjadi penting, guna mendukung upaya penegakan hukum pidana siber secara efektif dalam melindungi hak-hak masyarakat di era digital.

Menggunakan model penelitian normatif, dengan metode pengumpulan data melalui studi kepustakaan, serta teknik analisis deskriptif-kualitatif, penelitian ini menelusuri latar belakang peraturan terkait pemanfaatan dan perlindungan akses digital atau bidang Siber sebagai urgensi dari cita hukum di kemudian hari. Penelitian ini diharapkan mengungkap faktor-faktor politik yang mendasari pemilihan norma, strategi pencegahan, dan instrumen penegakan hukum yang diusulkan oleh legislator dan pemangku kepentingan lainnya mengenai tantangan *cyber crime* sebagai ancaman tidak terlihat yang berpotensi menimbulkan gangguan ketertiban dan keamanan umum bagi semua bangsa-bangsa di dunia.

Hasil dan Pembahasan

Cybercrime Dalam Konteks Hukum Positif di Indonesia

Kejahatan Siber merupakan bentuk kejahatan modern yang berkembang seiring dengan kemajuan teknologi informasi. Kejahatan siber ini berhubungan erat dengan komputer dalam penerapannya. Kejahatan siber dapat membahayakan privasi, integritas, dan eksistensi data masyarakat dan negara. Karena kejahatan siber ini memiliki karakteristik yang berbeda dari penjahat biasa, sangat penting bagi pemerintah untuk memberikan perhatian khusus kepada mereka. Banyak kejahatan siber sering terjadi dan menyebabkan kerugian bagi masyarakat. Hal ini salah satunya disebabkan dinamika masyarakat yang belum memahami teknologi secara komprehensif dan terlalu

bergantung pada teknologi yang semakin berkembang. Ruang lingkup Undang-undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau disingkat dengan UU ITE sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024 mencakup berbagai aspek mulai dari keamanan informasi, perlindungan data pribadi, transaksi elektronik, dan pencegahan kejahatan siber. UU ITE juga mengatur tentang penyebaran informasi yang dapat dianggap merugikan, menipu, atau melanggar kesusilaan. Hukum ini memberikan definisi jelas tentang apa yang dianggap sebagai tindakan kriminal dalam ruang siber, seperti penipuan online, pencurian identitas, dan penyebaran konten ilegal. UU ITE merupakan pilar utama dalam kerangka hukum keamanan siber Indonesia. UU ITE memainkan peran krusial dalam menangani isu-isu terkait dengan transaksi elektronik dan distribusi informasi di ranah digital.

Undang-Undang ITE tersebut tidak hanya berfokus pada aspek legal transaksi online, namun juga secara ekstensif mengatur tentang bagaimana informasi disebarkan di internet, memberikan kerangka untuk melindungi data pribadi warga, dan menetapkan standar untuk menangani kejahatan siber yang berkembang pesat. Secara umum, landasan hukum penanganan kejahatan siber di Indonesia berpusat pada UUU ITE. Peraturan tersebut mengatur berbagai mekanisme transaksi dan aktivitas yang dilakukan melalui sistem elektronik, termasuk mengatur isu penyebaran konten ilegal, penipuan online, pencurian data, dan peretasan. UU ini menargetkan berbagai bentuk pelanggaran siber, mulai dari penyebaran konten illegal hingga penipuan dan peretasan.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai respons terhadap meningkatnya kejahatan siber yang melibatkan penyalahgunaan informasi pribadi. UU ini menegaskan bahwa perlindungan data pribadi merupakan hak konstitusional yang wajib dijaga, serta memberikan kerangka hukum yang kuat melalui pembentukan Lembaga Perlindungan Data Pribadi, mekanisme pengawasan administratif, dan ketentuan pidana yang tegas. Pelanggaran seperti pengambilan, penyebaran, atau pemalsuan data pribadi tanpa izin diancam dengan sanksi pidana penjara dan/atau denda miliaran rupiah, serta pidana tambahan berupa ganti rugi kepada korban. UU PDP juga mengatur tanggung jawab korporasi dalam

perlindungan data, termasuk sanksi denda yang lebih besar dan kemungkinan pembekuan atau pembubaran usaha.[10]

UU PDP bersinergi dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang lebih dulu mengatur aspek kriminalitas digital, seperti akses ilegal dan penyebaran informasi elektronik tanpa hak. Sementara UU ITE menekankan aspek teknologi dari kejahatan siber, UU PDP memberikan fokus khusus pada hak-hak subjek data dan mekanisme perlindungannya, baik secara elektronik maupun non-elektronik. Kombinasi keduanya memperkuat sistem hukum pidana siber di Indonesia dalam melindungi privasi, mendorong akuntabilitas penyelenggara sistem elektronik, serta memberikan kejelasan hukum dan kepastian perlindungan bagi masyarakat yang menjadi korban kejahatan digital.

Perkembangan teknologi informasi telah mengubah hampir semua aspek kehidupan. Di satu sisi, teknologi komputer memberikan keuntungan seperti kesempatan untuk mendapatkan informasi, pekerjaan, berpartisipasi dalam politik dan kehidupan demokrasi, serta keuntungan lainnya. Kejahatan siber menjadi ancaman serius dalam kehidupan manusia, yang menghadirkan tantangan bagi organisasi pemerintah dalam mengatasi kejahatan yang terjadi dalam lingkungan teknologi komputer. Dampak buruk dari kejahatan siber ini dirasakan oleh masyarakat secara luas. Hal ini disebabkan oleh kurangnya pemahaman tentang jenis kejahatan yang terjadi di ruang internet dan kekurangan perlindungan serta keamanan data pribadi yang tidak lagi efektif. *Cyber Crime* memiliki beberapa karakteristik, yaitu antara lain:[11]

Tabel. Karakteristik Kejahatan *Cyber*

No.	Faktor
1	Kejahatan dilakukan secara ilegal, tanpa hak, atau tidak etis di ruang/wilayah maya (*cyberspace.*
2	Pelaku menggunakan peralatan apa pun yang terhubung dengan internet untuk melakukan kejahatan.

[10] Yusuf Daeng dkk., "Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi," *Innovative: Journal Of Social Science Research* 3, no. 6 (30 November 2023): 2898–2905.

[11] Admin, "Cyber Law dan Karakteristik Kejahatannya," *SIP Law Firm* (blog), t.t., https://siplawfirm.id/__trashed-3/?lang=id.

No.	Faktor
3	Kejahatan siber tidak menimbulkan kekacauan fisik yang mudah terlihat sehingga ketakutan publik seringkali tidak muncul meski kerugiannya besar.
4	Akibat kejahatan mencakup kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi).
5	Pelaku adalah individu yang menguasai penggunaan internet dan aplikasinya.
6	Kejahatan seringkali dilakukan secara transnasional atau melintasi batas negara.

Sumber: SIP Law Firm, 2023.

Dalam lanskap keamanan siber Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan revisinya pada tahun 2016, menduduki posisi sentral. UU ITE lahir dari kebutuhan untuk mengatur ruang siber yang berkembang cepat. Ruang lingkup UU ITE mencakup berbagai aspek mulai dari keamanan informasi, perlindungan data pribadi, transaksi elektronik, dan pencegahan kejahatan siber. UU ITE juga mengatur tentang penyebaran informasi yang dapat dianggap merugikan, menipu, atau melanggar kesusilaan. Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan muatan materi terkait *Cybercrime* ke dalam UU ITE yang diharapkan dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.

Berdasarkan materi muatan Kejahatan Siber di Indonesia yang terletak pada UU ITE yang mengatur tentang *Cybercrime* yaitu pada pasal Pasal 29 UU ITE: Mengatur tentang ancaman kekerasan melalui media elektronik, yaitu mengirimkan informasi elektronik atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti secara pribadi. Pasal 34 UU ITE: Mengatur tentang tindakan kriminal, seperti memproduksi, menjual, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras ,Pasal 30 jo. Pasal 46 UU ITE: Mengatur tentang pencurian dalam kasus carding. Pasal 34 ayat (1) jo. Pasal 50 UU ITE: Mengatur tentang pencurian melalui kerja sama dalam kasus

carding, Pasal 35 Jo Pasal 51 ayat (1) atau Pasal 32. Pasal 48 UU ITE: Mengatur tentang penipuan dalam kasus carding, khususnya melalui perolehan data kartu kredit orang lain dan transaksi Online. Pasal 362, 363, dan 378 KUHP: Mengatur tentang pencurian dan penipuan yang terkait dengan *Cyber Crime*.

Kejahatan siber memerlukan penindakan dan perhatian khusus dari pemerintah sebab kejahatan tersebut bisa terjadi dari wilayah atau negara manapun. Adanya ketergantungan dan kurangnya pengetahuan terhadap fungsi teknologi membuat masyarakat khususnya menjadi pihak yang paling rentan atau mudah menjadi korban kejahatan siber yang dapat merugikan mereka baik secara materiil maupun moriil.[12] Banyak kejahatan siber yang sering terjadi dan merugikan masyarakat. Hal ini disebabkan besarnya ketergantungan masyarakat terhadap teknologi yang semakin berkembang serta kurangnya pengetahuan tentang teknologi. Ketergantungan dan kurang pengetahuan inilah yang membuat masyarakat mudah untuk dijadikan korban kejahatan siber yang merugikan.

Dari berbagai telaah regulasi tersebut, maka dapat teramati dengan jelas bahwasanya perlindungan dunia digital di Indonesia masih bersifat parsial dan belum terintegrasi secara optimal. Faktor tersebut pada akhirnya memunculkan tantangan berkaitan dengan sumber daya manusia yang berkualitas dapat menciptakan cara berpikir yang positif terhadap perubahan lingkungan global serta meningkatkan kesadaran terhadap perkembangan teknologi dan informasi. Selain itu, Indonesia juga perlu memiliki fasilitas atau perangkat pengamanan negara yang lebih memadai. Fasilitas tersebut mencakup infrastruktur dan teknologi yang diperlukan untuk mendeteksi, mencegah, dan menanggulangi serangan siber. Investasi dalam pengembangan fasilitas pengamanan negara yang mutakhir dan efektif menjadi penting guna menghadapi

[12] Kristiani Virgi Kusuma Putri, "Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime," *Rewang Rencang: Jurnal Hukum Lex Generalis* 2, no. 7 (2021), https://jhlg.rewangrencang.com/.

ancaman kejahatan siber yang semakin kompleks dan terus berkembang.[13]

Urgensi Ketahanan dan Keamanan Cyber

Tindak Pidana Siber di Indonesia telah menjadi ancaman serius, terutama di sektor ekonomi yang rentan, di tengah perkembangan terus-menerus era digital. Kejahatan siber seperti pencurian data nasabah, penipuan online, perdagangan ilegal, dan serangan terhadap sistem perbankan terus meningkat.[14] Tren tersebut menimbulkan kerugian finansial bagi masyarakat dan mengancam stabilitas keamanan nasional dan pertumbuhan ekonomi. Upaya penegakan hukum perlu disesuaikan dan diperkuat untuk mengatasi tantangan yang dihadapi dalam lingkungan digital yang terus berubah dan berkembang pesat ini, karena penegakan hukum menghadapi berbagai masalah, terutama dalam upaya untuk mengharmonisasikan regulasi yang berkaitan dengan penggunaan internet.

Sebagaimana dapat teramati, perkembangan pola transaksi, pembelian, investasi, dan operasional bisnis telah mengalami perubahan besar sebagai akibat dari kemajuan terus-menerus dalam bidang teknologi informasi dan komunikasi.[15] Perkembangan tersebut juga memungkinkan sejumlah besar kejahatan siber, seperti pencurian data, serangan terhadap sektor perbankan, dan perdagangan ilegal. Oleh karena itu, diperlukan langkah-langkah konkret untuk melindungi sistem komputer, jaringan, perangkat elektronik, serta data dari berbagai ancaman siber yang ada. Untuk menghadapi tantangan baru yang muncul seiring dengan perkembangan teknologi, terdapat kebutuhan sistem hukum yang lebih sinkron harus terus diperbarui dan

[13] Handrini Ardiyanti, "Cyber-Security Dan Tantangan Pengembangannya di Indonesia," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 5, no. 1 (2024), https://doi.org/10.22212/jp.v5i1.336.

[14] Nabila Aulia Agustin dan Refania Meilani Firdos, "Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital," *Jurnal Mahasiswa Teknik Informatika* 3, no. 1 (1 April 2024): 126–31, https://doi.org/10.35473/jamastika.v3i1.2841.

[15] Alifia Fisilmi Kaffah dan Siti Malikhatun Badriyah, "Aspek Hukum Dalam Perlindungan Bisnis Era Digital Di Indonesia," *Lex Renaissance* 9, no. 1 (8 Oktober 2024): 203–28, https://doi.org/10.20885/JLR.vol9.iss1.art10.

disesuaikan agar sesuai dengan kebutuhan dan tantangan zaman yang terus berubah.[16]

Lembaga penegak hukum di berbagai negara telah membentuk tim khusus di bawah naungan Kementerian Informatika yang saat ini telah berganti nama menjadi Kementerian Komunikasi dan Digital (KOMDIGI) untuk menangani kejahatan siber yang terdiri dari ahli teknologi informasi, analis kejahatan siber, dan investigator yang dilatih khusus untuk menangani serangan keamanan siber.[17] Tim tersebut bekerja sama dengan sektor swasta, organisasi internasional, dan lembaga lainnya untuk mendeteksi, menyelidiki, dan menindak pelaku kejahatan siber.[18] Selain itu, beberapa negara telah berkoordinasi melalui berbagai kebijakan dan strategi keamanan siber untuk menghadapi ancaman kejahatan siber baik ditingkat nasional maupun regional. Kebijakan tersebut mencakup perlindungan infrastruktur kritis, pencegahan serangan, dan respons cepat terhadap insiden keamanan siber.[19] Strategi-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.[20]

Pemerintah Indonesia telah memberikan respons yang tegas terhadap meningkatnya ancaman kejahatan siber dengan mengadopsi kebijakan dan regulasi yang bertujuan untuk meningkatkan keamanan

---

[16] Firdi Gunawan, Ahmad Fadhilah, dan Essy Malays Sari, "Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime," *Tekinfo* 25, no. 1 (2024), https://doi.org/10.37817/tekinfo.v25i1.

[17] "Badan Cyber Nasional Demi Indonesia Digital," *Komdigi* (blog), 2020, https://www.komdigi.go.id/berita/sorotan-media/detail/badan-cyber-nasional-demi-indonesia-digital.

[18] Serly Sintia Saramuke, Vianna Antoneta Putri, dan Agnes Marianti Sormin, "Ancaman Keamanan Siber dan Peran Aktor Non-Negara di Dunia Digital," *Syntax Idea* 6, no. 2 (2025).

[19] Kristiani Virgi Kusuma Putri, "Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime," *Lex Generalis* 2, no. 7 (2021).

[20] Afifah Fidina Rosy, "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber: Indonesia's International Cooperation: Strengthening National Security in the Field of Cyber Security," *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan* 1, no. 2 (22 Juli 2020): 118–29, https://doi.org/10.54144/govsci.v1i2.12.

siber serta melindungi infrastruktur informasi yang kritis. Salah satu langkah konkret yang diambil adalah pendirian Badan Siber dan Sandi Negara (BSSN), sebuah lembaga yang dibentuk secara khusus untuk menghadapi berbagai ancaman dalam ranah digital.[21] Meskipun demikian, tantangan yang dihadapi tetap signifikan, dan upaya pembaruan terus-menerus dalam regulasi serta peningkatan kapabilitas dalam penegakan hukum menjadi sangat penting.[22] Hal tersebut diperlukan untuk menjaga keamanan nasional serta meminimalkan risiko kejahatan siber yang dapat mengganggu stabilitas dan keamanan di Indonesia. Dari analisis ini, perlunya penanganan serius terhadap berbagai jenis kejahatan siber seperti pencurian data, penipuan online, dan ancaman siber lainnya menjadi semakin mendesak. Penegakan hukum, khususnya dalam konteks perlindungan digital melalui aturan pidana cyber, menjadi sangat penting guna memastikan bahwa ketertiban dan keadilan tetap terjaga di tengah pesatnya perkembangan teknologi.

Berkembangnya teknologi informasi dan teknologi komunikasi seperti komputer, tablet, laptop, *smartphone* serta merambahnya provider internet dengan harga yang murah menimbulkan suatu peluang baru untuk berbuat kejahatan yang bernama Cyber Crime. *Cyber Crime* sendiri dapat dikatakan suatu dampak dari efek globalisasi, banyak orang yang terinspirasi menjadi pelaku kejahatan di dalam dunia maya atau memanfaatkan internet untuk menemukan cara cara untuk melakukan kejahatan lain dengan cara menonton video video yang ada dalam cyberspace terlebih semuanya itu diberikan secara gratis.

Keamanan siber telah menjadi isu prioritas seluruh negara di dunia semenjak teknologi informasi dan komunikasi dimanfaatkan dalam berbagai aspek kehidupan, baik dalam aspek sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan, dan lain sebagainya. Berbanding lurus dengan

---

[21] Yusep Ginanjar, "Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime melalui Badan Siber dan Sandi Negara," *Dinamika Global : Jurnal Ilmu Hubungan Internasional* 7, no. 02 (15 Desember 2022), https://doi.org/10.36859/jdg.v7i02.1187.

[22] Milla Mudzalifah dan Pujiyono Pujiyono, "The Politics of Criminal Law in Cybercrime: An Effort to Combat Information Technology Crimes in Indonesia," *Jurnal Pembaharuan Hukum* 10, no. 1 (13 April 2023): 77, https://doi.org/10.26532/jph.v10i1.26707.

tingginya tingkat pemanfaatan teknologi informasi dan komunikasi tersebut, tingkat risiko dan ancaman penyalahgunaan teknologi informasi dan komunikasi juga semakin tinggi dan semakin kompleks. [23] Indonesia, sebagai negara dengan pertumbuhan pengguna internet terbesar keempat di dunia, menghadapi peluang sekaligus ancaman besar dari perkembangan teknologi digital dan internet dalam bidang sosial, politik, dan ekonomi. Ancaman termasuk provokasi politik, hoaks, SARA, ujaran kebencian, ideologi radikalisme, terorisme, hacking, pencurian data, penipuan online, dan tindak kejahatan lainnya di internet. Untuk menjamin keamanan siber, hal-hal ini harus dapat diantisipasi, dicegah, dan ditangani.

Ketahanan dan keamanan siber sejatinya merupakan wujud perlindungan hak asasi manusia di era digital, karena akses yang aman dan andal ke dunia maya merupakan prasyarat bagi kebebasan berekspresi, hak atas privasi, hak memperoleh informasi, dan hak atas pendidikan. Tanpa jaminan keamanan siber, ruang publik digital bisa dipenuhi teror peretasan, penyebaran disinformasi, dan pelanggaran data pribadi yang pada gilirannya meredam kebebasan individu untuk bersuara atau mengakses konten tanpa rasa takut.[24] Ketika seseorang kehilangan kendali atas data pribadinya mulai dari riwayat penelusuran hingga percakapan pribadi maka hak atas privasi yang dijamin oleh konstitusi dan instrumen HAM internasional terancam hilang. Oleh karena itu, memperkuat ketahanan siber bukan sekadar persoalan teknologi atau infrastruktur, melainkan soal menjamin hak setiap warga negara untuk hidup bermartabat di ranah digital tanpa intimidasi atau pelanggaran privasi.[25]

Lebih lanjut, kerentanan sistem informasi dapat berdampak langsung pada hak atas pekerjaan, hak atas kesehatan, dan hak atas pendidikan. Misalnya, serangan siber terhadap institusi pendidikan daring dapat membatasi akses siswa terhadap materi pembelajaran; peretasan sistem rumah sakit mengancam keselamatan pasien; sementara gangguan pada layanan perbankan digital mempengaruhi

[23] Rosadi Sinta Dewi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional,* (Refika Aditama, 2018).

[24] Daeng dkk., "Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi."

[25] Denda Ginanjar dkk., "Perlindungan HAM dalam Era Digital: Tantangan dan Solusi Hukum," *Journal on Education* 4, no. 4 (2020).

hak masyarakat untuk mengelola aset dan menjalankan kegiatan ekonomi.[26] Jika hak-hak dasar tersebut tidak dilindungi melalui kerangka hukum dan kebijakan siber yang kuat, keberlangsungan pemenuhan hak asasi manusia akan terganggu secara sistemik. Dengan demikian, keamanan dan ketahanan siber sejajar dengan kewajiban negara untuk melindungi, menghormati, dan memenuhi HAM bagi seluruh rakyatnya baik di dunia nyata maupun maya.

Dalam kerangka RUU Ketahanan Siber, aspek HAM harus dijadikan landasan normatif sehingga setiap pasal dan mekanisme penegakan hukum menempatkan perlindungan individu di garis depan. Misalnya, prosedur penanganan insiden siber wajib memperhatikan prinsip proporsionalitas dan transparansi, menjamin bahwa tindakan investigasi tidak berlebihan hingga melanggar privasi tanpa dasar hukum yang jelas. Hak atas kebebasan berekspresi juga harus dijaga dengan membatasi ruang sensor atau pemblokiran konten hanya pada konten yang benar-benar membahayakan keamanan nasional atau menimbulkan pelanggaran HAM. Dengan menegakkan prinsip-prinsip HAM dalam setiap kebijakan siber, negara menunjukkan komitmennya untuk melindungi warganya seutuhnya, termasuk dalam ranah digital.[27]

Strategi Kebijakan Perlindungan dan Penegakan Hukum Pidana *Cyber*

Strategi kebijakan perlindungan dan penegakan hukum siber di Indonesia dimulai dengan upaya harmonisasi regulasi agar seluruh aspek kejahatan dunia maya berada di bawah payung hukum yang komprehensif. Pemerintah berupaya menyinkronkan RUU Ketahanan Siber dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta berbagai regulasi sektoral lainnya. Dengan demikian, tidak hanya definisi tindakan siber ilegal menjadi lebih jelas, tetapi juga alur pelaporan, prosedur penyelidikan, hingga jenis sanksi—baik administratif maupun pidana terbuka tanpa celah yurisdiksi. Langkah ini diharapkan menutup potensi tumpang tindih kewenangan antar lembaga dan mempercepat respons terhadap insiden siber, sehingga

[26] Nabila Aulia Agustin dan Refania Meilani Firdos, "Studi Literatur."
[27] Anggen Suari dan Sarjana, "Menjaga Privasi di Era Digital."

kebijakan nasional bisa lebih adaptif terhadap kecepatan perkembangan teknologi.

Dalam hal institusional, Badan Siber dan Sandi Negara (BSSN) diposisikan sebagai pusat koordinasi nasional yang menyediakan dukungan teknis forensik digital bagi aparat penegak hukum. Laboratorium forensik digital di BSSN diperkuat dengan tenaga ahli yang tersertifikasi, sehingga bukti elektronik dapat dianalisis secara cepat dan akurat. Kepolisian dan Kejaksaan RI pun didorong untuk membentuk satuan tugas khusus kejahatan siber, lengkap dengan laboratorium regional dan pelatihan berkelanjutan. Dengan modal kapasitas teknis ini, aparat tidak hanya mampu mendeteksi dan menangani serangan siber secara lebih efektif, tetapi juga menuntut pertanggungjawaban pelaku di pengadilan dengan bukti digital yang sah.

Pengembangan sumber daya manusia menjadi pilar berikutnya dalam strategi ini. Aparat penegak hukum wajib mengikuti pelatihan digital forensik, sertifikasi keamanan jaringan, dan program kolaborasi dengan akademisi serta industri teknologi. Lewat kerja sama dengan perguruan tinggi dan perusahaan termasuk magang dan riset bersama pengetahuan praktis dan pemahaman regulasi akan saling melengkapi. Selain itu, adopsi sertifikat internasional seperti CISSP atau CISA diutamakan untuk memastikan standar profesionalisme global, sehingga ketika penanganan kasus melibatkan aktor lintas negara, kualitas penyidikan tetap terjaga.

Tak kalah penting, pemerintah mendorong kemitraan publik–swasta melalui pembentukan *Information Sharing and Analysis Center* (ISAC) untuk sektor-sektor kritis seperti telekomunikasi, keuangan, dan energi. Melalui ISAC, ancaman terbaru dapat segera diidentifikasi dan direspons bersama, mengurangi waktu deteksi dan mitigasi. Di sisi lain, program edukasi "Cyber Aware" digulirkan di sekolah, universitas, dan masyarakat umum, menanamkan kesadaran akan keamanan siber dan praktik perlindungan data pribadi. Dengan demikian, masyarakat tidak hanya menjadi korban pasif, tetapi turut berperan dalam mencegah dan melaporkan insiden.[28]

[28] "Information Sharing and Analysis Centers (ISACs)," 2025, https://www.nationalisacs.org/about-isacs.

Agar respons insiden berjalan optimal, RUU Ketahanan Siber juga mengatur pembentukan *Computer Emergency Response* Team (CERT) di tingkat nasional dan sektoral, lengkap dengan standar operasional prosedur yang mewajibkan pelaporan insiden dalam batas waktu tertentu. Jalur komunikasi yang terstruktur antara lembaga pemerintahan, swasta, dan CERT memastikan koordinasi darurat berjalan lancar, serta mendukung langkah mitigasi dan pemulihan pasca-insiden.[29] Dengan rangkaian kebijakan terpadu ini, Indonesia berupaya memperkuat ketahanan siber nasional, membangun kepercayaan publik, dan menciptakan ekosistem digital yang aman bagi pertumbuhan ekonomi digital.

Dinamika globalisasi yang semakin erat dan tingginya tingkat konektivitas, kerja sama Internasional menjadi suatu keharusan dalam menangani ancaman kejahatan siber. Reformasi penegakan hukum kejahatan siber mencapai beberapa aspek penting. Pertama, peningkatan dalam bidang keamanan teknologi informasi menjadi sangat penting. Ini memerlukan penguatan sistem keamanan siber untuk melindungi infrastruktur yang penting dan data sensitif dari serangan digital. Kedua, sangat penting untuk meningkatkan pengetahuan masyarakat tentang keamanan siber untuk meningkatkan kesadaran masyarakat tentang ancaman digital dan cara menghindarinya. Penegakan hukum terhadap tindak pidana siber di Indonesia melibatkan berbagai lembaga, antara lain Kepolisian Republik Indonesia (POLRI), Kejaksaan Agung, dan Komisi Pemberantasan Korupsi (KPK). POLRI memiliki satuan khusus yang fokus menangani kejahatan dunia maya, yaitu Direktorat Tindak Pidana Siber Bareskrim Polri. Selain itu, Kejaksaan Agung juga memiliki peran penting dalam penuntutan pelaku kejahatan siber. Tantangan lain dalam penyempurnaan kebijakan keamanan siber adalah sifat ancaman siber yang multidimensi. Hal ini mengakibatkan penanggulangannya tidak hanya menjadi tanggung jawab TNI atau Polri, tetapi melibatkan berbagai kementerian seperti Kementerian Pertahanan dan Kementerian Komunikasi dan Informatika.

Digitalisasi yang berkembang dengan cepat, Indonesia menghadapi masalah besar karena peningkatan kejahatan siber,

[29] Admin, "Indonesia Computer Emergency Response Team," 2024, https://www.cert.or.id/tentang-kami/en/.

terutama di sektor ekonomi. Berbagai jenis ancaman ini termasuk serangan terhadap infrastruktur perbankan, pencurian data nasabah, penipuan online, dan perdagangan ilegal di internet. Kejahatan siber ini menjadi pusat perhatian nasional. Kejahatan siber dapat sangat merugikan masyarakat secara keseluruhan, mengancam stabilitas keamanan nasional, dan mengancam pertumbuhan ekonomi negara. Oleh karena itu, sangat penting untuk melindungi masyarakat dan infrastruktur nasional dari ancaman kejahatan siber.[30] Untuk melaksanakan penegakan hukum terhadap kejahatan siber, banyak masalah muncul,[31] Isu krusial dalam hal ini adalah bagaimana peraturan yang telah ada khususnya terkait dengan Tindak Pidana Cyber dalam UU ITE misalnya lebih konsisten untuk mengatasi kejahatan menggunakan internet. Meskipun pada praktiknya bagaimana orang bertransaksi, berbelanja, berinvestasi, dan menjalankan bisnis telah berubah karena perkembangan teknologi komunikasi dan informasi, memungkinkan pertumbuhan dan penyebaran kejahatan siber menjadi semakin masif apabila tidak diantisipasi dengan secara sistemik baik dalam bentuk regulasi maupun infrastruktur pendukungnya.[32]

Dalam menegakkan hukum siber, terdapat tantangan yang dihadapi penegak hukum dalam menegakkan hukum. Keterbatasan sumber daya dan kapasitas merupakan tantangan utama dalam penegakan hukum siber di Indonesia.[33] Di era transformasi digital saat ini, hukum pidana siber sangat penting karena membutuhkan sistem penegakan hukum yang efektif dan responsif untuk menangani berbagai jenis kejahatan siber.[34] Memiliki hukum pidana yang mengatur

[30] Regner Sabillon dkk., "Cybercrime and Cybercriminals: A Comprehensive Study," *International Journal of Computer Networks and Communications Security* 4, no. 6 (2016).

[31] Aditya Yuli Sulistyawan, "Urgensi Harmonisasi Hukum Terhadap Perkembangan Hukum Global Akibat Globalisasi," *Jurnal Hukum Progresif* 7, no. 2 (31 Oktober 2019): 171, https://doi.org/10.14710/hp.7.2.171-181.

[32] Sherly Nelsa Fitri, "Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia," *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial* 7, no. 1 (26 Juni 2022): 104, https://doi.org/10.22373/justisia.v7i1.12719.

[33] Paschal Uchenna Chinedu dkk., "Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models," t.t.

[34] Pansariadi dan Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya."

dunia maya sangat penting untuk melindungi orang dan organisasi dari ancaman berbagai kejahatan digital, seperti pencurian data, penipuan daring, dan serangan siber lainnya. Untuk memastikan bahwa keadilan dan ketertiban tetap ada di era digital ini, penegakan hukum harus tetap konsisten di tengah perkembangan teknologi yang terus berkembang.[35] Menghadapi tantangan yang semakin kompleks di era digital, muncul kebutuhan mendesak untuk merekonstruksi konsep penegakan hukum terhadap tindak pidana siber di Indonesia. Seiring dengan perkembangan teknologi yang terus maju, kejahatan siber berkembang secara cepat dan menghadirkan risiko baru yang mengancam baik masyarakat maupun pemerintah.

Dalam usaha merekonstruksi konsep penegakan hukum ini, diperlukan langkah-langkah yang progresif untuk meningkatkan kapasitas hukum dalam mengantisipasi serta menanggapi berbagai bentuk kejahatan siber yang terus berkembang. Upaya ini harus didasarkan pada kerjasama yang erat antara berbagai lembaga penegak hukum, sektor swasta, dan pihak-pihak terkait lainnya. Hal ini untuk menciptakan lingkungan digital yang lebih aman dan terpercaya bagi semua pihak yang terlibat. Dengan melakukan rekonstruksi ini, diharapkan penegakan hukum terhadap tindak pidana siber dapat menjadi lebih efektif, adaptif, dan mampu menjawab tantangan yang muncul seiring perkembangan teknologi. Upaya ini bertujuan untuk menjaga stabilitas dan keamanan dalam lingkup digital di Indonesia dengan mengakomodasi berbagai perubahan dan inovasi yang terjadi dalam ranah kejahatan siber. Konsep penegakan hukum terhadap kejahatan siber di Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016, yang merupakan hasil dari revisi terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Melalui UU ITE tersebut, penegakan hukum dapat lebih terfokus pada berbagai bentuk pelanggaran di dunia maya, serta memberikan kerangka perlindungan hukum dan sanksi pidana bagi para pelaku kejahatan siber.[36]

---

[35] Habibi dan Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia."

[36] Adwi Mulyana Hadi, "Cyber Crime in Renewing The ITE Law to Realize The Goals of Legal Justice," *Journal of Law, Society, Adn Islamic Civilisation* 12, no. 1 (2024).

Penegakan hukum kejahatan siber di Indonesia saat ini menghadapi masalah yang semakin kompleks. Oleh karena itu, untuk meningkatkan efektivitas penegakan hukum di dunia maya, pemerintah, sektor swasta, dan masyarakat harus bekerja sama. Di era digital ini, peningkatan kapasitas hukum, pembuatan regulasi yang lebih tepat dan fleksibel, dan penguatan melalui pendidikan dan pelatihan keamanan siber adalah kunci untuk menjaga stabilitas dan kedaulatan negara. Dengan merekonstruksi konsep penegakan hukum, Indonesia diharapkan dapat menangani kejahatan siber dengan lebih baik. Diharapkan tindakan ini akan memberikan perlindungan yang lebih baik terhadap infrastruktur digital dan masyarakat negara.[37] Pelaku tindak pidana siber di Indonesia saat ini menjadi ancaman serius, khususnya dalam bidang ekonomi, memerlukan perhatian dan kewaspadaan nasional.

Dampak dari digitalisasi terhadap ekonomi Indonesia yang semakin rentan terhadap serangan tindak pidana siber, seperti perbankan, pencurian data nasabah, penipuan online, dan perdagangan ilegal. Dampak dari serangan tersebut dapat merugikan masyarakat secara luas, mengancam keamanan nasional, dan membawa risiko signifikan pada pertumbuhan ekonomi.[38] Maka upaya terpenting adalah menciptakan peraturan yang selaras dengan penggunaan atau internet. Ketentuan yang tercantum dalam KUHP masih digunakan dalam pengendalian tindak pidana penipuan, perjudian, dan pornografi. Meskipun demikian, kemajuan terus-menerus dalam teknologi informasi dan komunikasi mengubah cara orang bertransaksi, berbelanja, berinvestasi, dan menjalankan bisnis. Namun, kemajuan ini juga memungkinkan kejahatan siber seperti serangan terhadap perbankan, pencurian data, dan perdagangan ilegal untuk berkembang. Sangat penting untuk mengambil tindakan nyata untuk melindungi

[37] Adinda Lola Sariani Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia," *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 2 (18 Juli 2024): 69–77, https://doi.org/10.58707/aldalil.v2i2.777.

[38] Institute of Police Science, People's Police Academy, Hanoi, Vietnam dkk., "Cybercrime in the Digital Age: Challenges and Implication for Prevention," *International Journal of Social Science And Human Research* 05, no. 11 (21 November 2022), https://doi.org/10.47191/ijsshr/v5-i11-36.

sistem komputer, jaringan, perangkat elektronik, dan data dari ancaman siber. [39]

Keamanan siber melindungi kerahasiaan, integritas, dan ketersediaan data sensitif serta infrastruktur teknologi informasi dari serangan yang dapat merusak sistem atau menyebabkan kerugian yang besar. Kolaborasi antara pemerintah, bisnis, dan individu di seluruh masyarakat semakin diperkuat untuk melindungi keamanan dan kedaulatan negara dari segala macam ancaman dan gangguan. Program pendidikan dan pelatihan keamanan siber ditingkatkan untuk meningkatkan kesadaran dan keterampilan dalam menghadapi ancaman siber. Meskipun demikian, tingkat kejahatan siber terus berkembang dan semakin kompleks.[40]

Dari berbagai pemaparan dan analisis tersebut, urgensi hukum pidana siber mencakup perlunya penegakan hukum yang efektif dan responsif terhadap kejahatan siber di tengah transformasi digital. Untuk melindungi masyarakat dan lembaga dari ancaman kejahatan di dunia maya saat ini, hukum pidana siber mencakup penanganan serius pencurian data, penipuan online, dan ancaman siber lainnya yang dapat merugikan orang dan organisasi serta mengancam keamanan nasional. Untuk menjaga ketertiban dan keadilan di tengah dinamika teknologi yang terus berkembang, penegakan hukum yang konsisten dalam konteks digital sangat penting. Peningkatan kapasitas hukum dan penyusunan regulasi yang lebih tepat dan fleksibel untuk menangani dinamika kejahatan siber diperlukan untuk menjaga keamanan siber dan melindungi masyarakat. Dalam konteks ini, untuk menghadapi tantangan di era digital dan memastikan bahwa sistem hukum mampu mengatasi masalah baru dan menjaga keamanan nasional dan melindungi masyarakat, diperlukan rekonstruksi konsep penegakan hukum terhadap Tindak Pidana Siber.

---

[39] Imelda Martinelli, Fricila Anggitha Sugiawan, dan Renita Zulianty, "Perlindungan Hak Privasi Dalam Era Digital: Harmonisasi Undang Undang Informasi dan Teknologi Elektronik Dengan Prinsip-Prinsip Filosofi Hukum Roscoe Pound Dalam Hukum Perikatan," *MOTEKAR: Jurnal Multidisiplin Teknologi dan Arsitektur* 1, no. 2 (2023).

[40] Muhammad Fahli Saputra dan Aji Prasetya Wibawa, "Peran dan Tantangan Cyber Security di Era Society 5.0," 2022.

Penutup

Dari berbagai uraian yang telah penulis paparkan pada pembahasan, maka dapat disimpulkan bahwa penerapan hukum pidana dalam menghadapi serta pencegahan kejahatan siber di era digital, dan dimensi tujuan hukum terhadap perlindungan dan penegakan hukum siber di Indonesia dihadapkan pada aspek efektivitas penanggulangan *cybercrime* yang sangat ditentukan oleh keselarasan antara instrumen pidana dan nilai-nilai fundamental tujuan hukum. Pertama, penerapan hukum pidana siber memerlukan peningkatan kapasitas norma dan teknis aparat penegak serta sinergi antar-institusi, sehingga norma yang ada dapat diaktualisasikan dalam tindakan preventif dan represif yang konkret. Kedua, dimensi tujuan hukum meliputi keadilan, kepastian hukum, dan kemanfaatan harus menjadi pijakan dalam merumuskan ancaman dan sanksi pidana sehingga tidak hanya menjerakan pelaku, tetapi juga menjaga hak asasi dan keterbukaan teknologi informasi. Ketiga, kerangka hukum positif tentang ketahanan siber perlu di sinkronisasi agar selaras dengan prinsip tujuan hukum: memberikan perlindungan menyeluruh bagi masyarakat digital, menjamin kepastian hukum bagi penyelenggara teknologi, dan mendorong kemanfaatan melalui pencegahan serta mitigasi risiko. Dengan demikian, integrasi antara penerapan hukum pidana yang adaptif dan orientasi tujuan hukum yang holistik menjadi fondasi strategis untuk memperkuat ketahanan siber nasional dan memastikan penegakan hukum siber di Indonesia berjalan efektif dan berkeadilan.

Daftar Pustaka

Admin. "Cyber Law dan Karakteristik Kejahatannya." *SIP Law Firm* (blog), t.t. https://siplawfirm.id/__trashed-3/?lang=id.

———. "Indonesia Computer Emergency Response Team," 2024. https://www.cert.or.id/tentang-kami/en/.

Aldriano, Muhammad Anthony, dan Mas Agus Priyambodo. "Cyber Crime Dalam Sudut Pandang Hukum Pidana." *Jurnal Kewarganegaraan* 6, no. 1 (2022).

Alifia Fisilmi Kaffah dan Siti Malikhatun Badriyah. "Aspek Hukum Dalam Perlindungan Bisnis Era Digital Di Indonesia." *Lex*

Renaissance 9, no. 1 (8 Oktober 2024): 203–28. https://doi.org/10.20885/JLR.vol9.iss1.art10.

Anggen Suari, Kadek Rima, dan I Made Sarjana. "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (25 April 2023): 132–42. https://doi.org/10.38043/jah.v6i1.4484.

Ardiyanti, Handrini. "Cyber-Security Dan Tantangan Pengembangannya di Indonesia." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 5, no. 1 (2024). https://doi.org/10.22212/jp.v5i1.336.

Chinedu, Paschal Uchenna, Wilson Nwankwo, Florence U Masajuwa, dan Simon Imoisi. "Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models," t.t.

Daeng, Yusuf, Nasri Linra, Atan Darham, Derry Handrianto, Risky Risandy Sianturi, Denny Martin, Rendy Pratama Putra, dan Hendi Saputra. "Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi." *Innovative: Journal Of Social Science Research* 3, no. 6 (30 November 2023): 2898–2905.

Dewi, Rosadi Sinta. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional,*. Refika Aditama, 2018.

Dinda, Adinda Lola Sariani. "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia." *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 2 (18 Juli 2024): 69–77. https://doi.org/10.58707/aldalil.v2i2.777.

Fitri, Sherly Nelsa. "Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia." *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial* 7, no. 1 (26 Juni 2022): 104. https://doi.org/10.22373/justisia.v7i1.12719.

Ginanjar, Denda, Muhammad Fajar Firdausyi, Sobali Suswandy, dan Novita Tresna Andini. "Perlindungan HAM dalam Era Digital: Tantangan dan Solusi Hukum." *Journal on Education* 4, no. 4 (2020).

Gunawan, Firdi, Ahmad Fadhilah, dan Essy Malays Sari. "Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime." *Tekinfo* 25, no. 1 (2024). https://doi.org/10.37817/tekinfo.v25i1.

Habibi, Miftakhur Rokhman, dan Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23, no. 2 (19 Desember 2020): 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426.

Hadi, Adwi Mulyana. "Cyber Crime in Renewing The ITE Law to Realize The Goals of Legal Justice." *Journal of Law, Society, Adn Islamic Civilisation* 12, no. 1 (2024).

Hamzah, Andi. *Aspek-aspek Pidana di Bidang Komputer*. Jakarta: Sinar Grafika, 1989.

Indonet. "Faktor yang menyebabkan Kejahatan Siber Mudah Terjadi," t.t. https://indonet.co.id/id/12-faktor-penyebab-kejahatan-siber-mudah-terjadi/.

"Information Sharing and Analysis Centers (ISACs)," 2025. https://www.nationalisacs.org/about-isacs.

Institute of Police Science, People's Police Academy, Hanoi, Vietnam, Nguyen The Sang, Bui Bao Trung, dan Institute of Police Science, People's Police Academy, Hanoi, Vietnam. "Cybercrime in the Digital Age: Challenges and Implication for Prevention." *International Journal of Social Science And Human Research* 05, no. 11 (21 November 2022). https://doi.org/10.47191/ijsshr/v5-i11-36.

Komdigi. "Badan Cyber Nasional Demi Indonesia Digital," 2020. https://www.komdigi.go.id/berita/sorotan-media/detail/badan-cyber-nasional-demi-indonesia-digital.

Martinelli, Imelda, Fricila Anggitha Sugiawan, dan Renita Zulianty. "Perlindungan Hak Privasi Dalam Era Digital: Harmonisasi Undang Undang Informasi dan Teknologi Elektronik Dengan Prinsip-Prinsip Filosofi Hukum Roscoe Pound Dalam Hukum

Perikatan." *MOTEKAR: Jurnal Multidisiplin Teknologi dan Arsitektur* 1, no. 2 (2023).

Mudzalifah, Milla, dan Pujiyono Pujiyono. "The Politics of Criminal Law in Cybercrime: An Effort to Combat Information Technology Crimes in Indonesia." *Jurnal Pembaharuan Hukum* 10, no. 1 (13 April 2023): 77. https://doi.org/10.26532/jph.v10i1.26707.

Nabila Aulia Agustin dan Refania Meilani Firdos. "Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital." *Jurnal Mahasiswa Teknik Informatika* 3, no. 1 (1 April 2024): 126–31. https://doi.org/10.35473/jamastika.v3i1.2841.

Pansariadi, Rafi Septia Budianto, dan Noenik Soekorini. "Tindak Pidana Cyber Crime dan Penegakan Hukumnya." *Binamulia Hukum* 12, no. 2 (20 Desember 2023): 287–98. https://doi.org/10.37893/jbh.v12i2.605.

Putri, Annisa Nadya. "Upaya Hukum dalam Strategi Perlindungan Data pada Penggunaan Internet Studi Kasus : Hacker Bjorka." *Jurnal Hukum dan Pembangunan Ekonomi* 12, no. 1 (31 Juli 2024): 52. https://doi.org/10.20961/hpe.v12i1.81910.

Putri, Kristiani Virgi Kusuma. "Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime." *Rewang Rencang : Jurnal Hukum Lex Generalis* 2, no. 7 (2021). https://jhlg.rewangrencang.com/.

———. "Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime." *Lex Generalis* 2, no. 7 (2021).

Rosy, Afifah Fidina. "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber: Indonesia's International Cooperation: Strengthening National Security in the Field of Cyber Security." *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan* 1, no. 2 (22 Juli 2020): 118–29. https://doi.org/10.54144/govsci.v1i2.12.

Sabillon, Regner, Jeimy Cano, Victor Cavaller, dan Jordi Serra. "Cybercrime and Cybercriminals: A Comprehensive Study."

International Journal of Computer Networks and Communications Security 4, no. 6 (2016).

Saputra, Muhammad Fahli, dan Aji Prasetya Wibawa. "Peran dan Tantangan Cyber Security di Era Society 5.0," 2022.

Saramuke, Serly Sintia, Vianna Antoneta Putri, dan Agnes Marianti Sormin. "Ancaman Keamanan Siber dan Peran Aktor Non-Negara di Dunia Digital." *Syntax Idea* 6, no. 2 (2025).

Sulistyawan, Aditya Yuli. "Urgensi Harmonisasi Hukum Terhadap Perkembangan Hukum Global Akibat Globalisasi." *Jurnal Hukum Progresif* 7, no. 2 (31 Oktober 2019): 171. https://doi.org/10.14710/hp.7.2.171-181.

Unair News. "Analisis Ancaman dan Respon Keamanan Siber di Indonesia," 2024. https://unair.ac.id/analisis-ancaman-dan-respon-keamanan-siber-di-indonesia/.

Wisnubroto, Aloysius. *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*. Penerbitan Universitas Atma Jaya Yogyakarta, 1999. https://books.google.co.id/books?id=aigRAgAACAAJ.

Yusep Ginanjar. "Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime melalui Badan Siber dan Sandi Negara." *Dinamika Global: Jurnal Ilmu Hubungan Internasional* 7, no. 02 (15 Desember 2022). https://doi.org/10.36859/jdg.v7i02.1187.