Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital

Risma Siti Maesaroh
UIN Sunan Kalijaga Yogyakarta
E-mail: *23103040121@student.uin.suka.ac.id*

Abstract: *The advancement of information and communication technology in the digital era has brought both significant benefits and serious challenges, particularly in the realm of cybersecurity. Indonesia is currently facing a range of cybercrimes, including data theft, hacking, online fraud, and the dissemination of illegal content. Although Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) serves as the primary legal foundation, it remains insufficient in addressing the growing complexity of cyber threats. This study aims to evaluate the effectiveness of existing regulations, identify key challenges, and propose strategic measures to strengthen cybersecurity governance in Indonesia. The research employs a descriptive-analytical method with a qualitative approach, relying on secondary data from legal literature, government policies, and recent case studies. The findings indicate that the implementation of the ITE Law faces several limitations, including narrow legal scope, limited enforcement capacity, low public awareness of digital security, and the transnational nature of cybercrime. Moreover, increasing threats to national critical infrastructure and sensitive data highlight the urgent need for a more adaptive and comprehensive legal framework. Moving forward, Indonesia must enhance its national legal instruments, improve human resource capacity in the field of cybersecurity, foster international cooperation, and promote public education on digital safety. These steps are essential to ensure state digital sovereignty and build a robust and sustainable cybersecurity system*

Keywords: *security, challenges, law enforcement*

Abstrak: Perkembangan teknologi informasi dan komunikasi di era digital telah memberikan manfaat besar, namun juga menghadirkan tantangan serius dalam bentuk ancaman kejahatan siber. Indonesia menghadapi berbagai bentuk kejahatan digital seperti pencurian data pribadi, peretasan, penipuan daring, dan penyebaran konten ilegal. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah dijadikan sebagai dasar hukum utama dalam menghadapi permasalahan ini. Penelitian ini bertujuan untuk mengevaluasi efektivitas UU ITE, mengidentifikasi tantangan dalam implementasinya, serta merumuskan langkah strategis untuk

memperkuat keamanan siber di Indonesia. Metode yang digunakan adalah deskriptif-analitis dengan pendekatan kualitatif berdasarkan data sekunder dari literatur hukum, kebijakan pemerintah, dan studi kasus. Hasil penelitian menunjukkan bahwa implementasi UU ITE masih menghadapi berbagai kendala, seperti cakupan hukum yang terbatas, lemahnya kapasitas penegakan hukum, rendahnya kesadaran masyarakat akan keamanan digital, serta karakteristik kejahatan siber yang lintas batas negara. Selain itu, meningkatnya ancaman terhadap infrastruktur vital dan data sensitif negara menunjukkan perlunya penguatan kerangka hukum yang lebih adaptif dan komprehensif. Strategi yang direkomendasikan meliputi pembaruan regulasi nasional, peningkatan kualitas sumber daya manusia di bidang keamanan siber, kerja sama internasional, serta edukasi publik secara masif mengenai pentingnya perlindungan data pribadi dan keamanan digital. Upaya ini penting untuk mewujudkan kedaulatan digital dan sistem pertahanan siber yang berkelanjutan di Indonesia.

Kata kunci: *keamanan, tantangan, implikasi hukum*

Pendahuluan

Saat ini dunia tengah sekarang berada di era informasi, tahap lanjutan dari era prasejarah, agraris, dan industri. Pada era informasi, informasi sangat penting dan penting bagi semua aspek kehidupan, dan sangat dibutuhkan oleh semua orang, baik individu maupun organisasi. Dengan kata lain, informasi telah menjadi sumber kehidupan bagi masyarakat informasi.[1] Seiring dengan berkembangnya penggunaan media elektronik di Indonesia, diperlukan dukungan perangkat hukum yang relevan. Istilah "hukum siber" sering digunakan sebagai padanan dari cyberlaw, mengikuti pendapat Mariam Darus Badrulzaman (2001: 271). Hukum siber mengacu pada aturan hukum yang berhubungan dengan pemanfaatan teknologi informasi dan komunikasi. Istilah lain yang kerap digunakan mencakup hukum teknologi informasi (law of information technology), hukum dunia maya (virtual world law), dan hukum mayantara. Kemajuan teknologi ini telah mengubah struktur masyarakat dari yang awalnya bersifat lokal menjadi masyarakat berstruktur global, perubahan yang didorong oleh kehadiran teknologi

[1] Anne W. Brascomb (ed), Toward A Law of Global Communication Network, New York: Lognman, 1986, hal.1

informasi. Perkembangan teknologi informasi ini, yang terintegrasi dengan media dan komputer, akhirnya melahirkan sebuah inovasi baru yang dikenal sebagai internet.[2]

Perkembangan teknologi internet telah memunculkan jenis kejahatan baru yang dikenal sebagai cybercrime atau kejahatan yang dilakukan melalui jaringan internet. Beberapa kasus cybercrime di Indonesia meliputi pencurian data kartu kredit, peretasan (hacking) situs web, penyadapan data seperti email, serta manipulasi data dengan menyisipkan instruksi yang tidak diinginkan ke dalam program komputer. Dalam kejahatan berbasis komputer, dikenal dua jenis delik, yaitu delik formil dan delik materil. Delik formil terjadi ketika seseorang mengakses komputer orang lain tanpa izin, sedangkan delik materil adalah tindakan yang menyebabkan kerugian bagi pihak lain. Fenomena cybercrime ini menjadi ancaman serius terhadap stabilitas, sementara pemerintah menghadapi tantangan dalam mengimbangi teknik-teknik kejahatan yang semakin canggih dengan pemanfaatan teknologi komputer, khususnya yang melibatkan jaringan internet dan intranet.[3]

Jonathan Rosenoer (1997) mengelompokkan ruang lingkup cyber law ke dalam beberapa aspek, antara lain: hak cipta (copyright), hak merek dagang (trademark), pencemaran nama baik (defamation), ujaran kebencian (hate speech, termasuk penghinaan dan fitnah), peretasan (hacking), penyebaran virus, akses ilegal (serangan terhadap komputer atau perangkat optik lainnya), pengaturan sumber daya internet (regulation of internet resources), privasi, kewajiban kehati-hatian (duty of care), tanggung jawab pidana dalam kejahatan yang melibatkan teknologi informasi, serta isu prosedural seperti yurisdiksi, pembuktian, dan penyelidikan. Selain itu, cyber law juga mencakup kontrak elektronik, transaksi pornografi, pencurian melalui internet, perlindungan konsumen, serta penggunaan internet dalam kegiatan e-commerce dan e-government.[4]

---

[2] Muhammad Prima Ersya, "Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia", 1 (1) 2017, hlm. 51.

[3] Eliasta Ketaren, "CYBERCRIME, CYBER SPACE, DAN CYBETLAW", Vol. V, No. 2, 2016, hlm. 35.

[4] Riko Nugraha, PERSPEKTIF HUKUM INDONESIA (CYBERLAW) PENANGANAN KASUS CYBER DI INDONESI, Vol. 11, no. 2, (Maret 2021), hlm. 46.

Definisi tentang keamanan siber masih belum memiliki kesepakatan yang pasti. Hal ini serupa dengan pandangan Buzan yang menyatakan bahwa konsep "keamanan" tidak memiliki definisi yang tegas (Buzan, 1998). Meskipun demikian, sejumlah literatur mencoba memberikan penjelasan mengenai keamanan siber. Roxana Radu mendefinisikan keamanan siber sebagai kumpulan kebijakan, alat, instrumen, dan pengelolaan risiko yang dirancang untuk mencegah ancaman dari dunia maya (Radu dalam Kremer & Muller, 2014). Sementara itu, Madeline Carr, dalam jurnalnya yang berjudul *Crossed Wires: International Cooperation on Cyber Security*, menggambarkan keamanan siber sebagai isu *post-state*. Ini berarti bahwa keamanan siber merupakan ancaman yang tidak dapat ditangani dengan pendekatan tradisional Westphalia, seperti penggunaan instrumen negara termasuk militer. Carr menekankan bahwa ancaman dari dunia maya bersifat tanpa batas (*borderless*) dan tidak kasat mata, namun dampaknya sangat nyata dan signifikan (Carr, 2015).[5]

Hasil dan Pembahasan

Perkembangan Hukum Cyber di Indonesia

Dalam konteks keamanan siber di Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta revisinya pada tahun 2016 memiliki peran yang sangat penting. UU ITE muncul sebagai respons terhadap kebutuhan untuk mengatur ruang siber yang berkembang dengan pesat. Sejak diberlakukan, UU ini menjadi dasar dalam penanganan berbagai kasus terkait dunia maya. Cakupan UU ITE meliputi berbagai aspek, seperti keamanan informasi, perlindungan data pribadi, transaksi elektronik, serta pencegahan kejahatan siber. Selain itu, UU ini juga mengatur tentang penyebaran informasi yang dapat dianggap menipu, merugikan, atau melanggar norma kesusilaan. UU ITE memberikan definisi yang jelas mengenai tindakan kriminal di ruang siber, seperti penipuan daring, pencurian identitas, dan distribusi konten ilegal (Ramadhani,

[5] Iqbal Ramadhan, "Stategi Keamanan Cyber Security di Kawasan Asia Tenggara: Self-Help atau Multilateralism", Vol. 3, No. 2, July-Desemver 2019, hlm. 182.

2023).[6]

Hubungan yang kompleks antara keamanan siber dan keamanan nasional menekankan pentingnya langkah-langkah hukum yang efektif. Serangan siber memiliki potensi untuk merusak infrastruktur vital, mengganggu operasi pemerintah, serta membahayakan data sensitif, sehingga menjadi ancaman langsung terhadap kedaulatan negara. Dengan semakin eratnya integrasi teknologi digital ke dalam layanan-layanan krusial, kebutuhan akan kerangka hukum yang kokoh menjadi semakin mendesak (Chik, 2013; Greenleaf, 2012; Romansky & Noninska, 2020; Shrivastava et al., 2021; Trautman, 2021).[7]

Hubungan yang kompleks antara keamanan siber dan keamanan nasional menunjukkan perlunya langkah-langkah hukum yang efektif. Serangan siber dapat mengancam infrastruktur vital, mengganggu fungsi pemerintah, dan mengekspos data sensitif, sehingga menimbulkan risiko langsung terhadap kedaulatan negara. Di Indonesia, yang tengah mengalami digitalisasi pesat dan konektivitas yang semakin luas, tantangan di bidang keamanan siber menjadi semakin kompleks. UU ITE, yang disahkan pada tahun 2008, berfungsi sebagai dasar hukum utama dalam menangani isu ini. Namun, kritik muncul terkait dengan kecukupan dan kemampuannya untuk menghadapi ancaman siber yang terus berkembang. Oleh karena itu, memahami keunggulan dan kelemahan kerangka hukum Indonesia sangat penting untuk merumuskan rekomendasi yang sesuai dengan konteks nasional (Natamiharja et al., 2022; Rosadi, 2018; Yuniarti, 2019).[8]

Hukum siber, yang juga dikenal sebagai Hukum Teknologi Informasi, adalah kumpulan prinsip dan aturan hukum yang mengatur penggunaan serta akses terhadap teknologi informasi dan komunikasi. Di tengah perkembangan era digital, hukum ini memiliki peran penting

[6] Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukuk Siber di Indonesia", Vol. 2, No. 1, April 2024, hlm. 11.

[7] Herni Rahmayanti, "Peran Hukum dalam Mengatakan Serangan Cyber yang Mengancam Keamanan Nasional", Vol. 02, No. 9, September 2023, hlm. 906.

[8] Herni Rahmayanti, "Peran Hukum dalam Mengatakan Serangan Cyber yang Mengancam Keamanan Nasional", Vol. 02, No. 9, September 2023, hlm. 907.

dalam menangani berbagai isu terkait internet, teknologi digital, perangkat lunak, komputer, dan data (Abdukhalil & Dostonbek, 2024). Aspek-aspek yang diatur meliputi keamanan data, privasi online, hak kekayaan intelektual, transaksi elektronik, kejahatan siber, serta tanggung jawab penyedia layanan internet. Tujuan utamanya adalah melindungi hak serta keamanan pengguna di dunia maya, sekaligus mendukung pertumbuhan dan inovasi dalam bidang teknologi (Sunde, 2022).

Perkembangan hukum siber di Indonesia ditandai oleh berbagai upaya legislatif dan kebijakan pemerintah yang dirancang untuk merespons tantangan yang muncul akibat evolusi teknologi informasi dan komunikasi. Salah satu pencapaian penting dalam perjalanan ini adalah pengesahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016 (MANUILOV, 2023). UU ITE menetapkan kerangka hukum untuk transaksi elektronik, mengatur hak dan kewajiban pengguna serta penyedia layanan internet, dan memberikan regulasi terkait tindak pidana di dunia maya, termasuk penyebaran konten ilegal dan pencemaran nama baik (Turns, 2021).[9]

Tantangaan Keamanan dan Hukum Cyber

Tantangan utama dalam dunia siber saat ini adalah kompleksitas yang terkait dengan keamanan siber. Keamanan siber sangat penting mengingat munculnya ancaman seperti peretasan, serangan malware, dan upaya pencurian data, yang dapat menimbulkan dampak besar bagi individu, perusahaan, dan bahkan negara. Ancaman ini tidak hanya menyebabkan kerugian finansial akibat pencurian informasi keuangan atau data bisnis, tetapi juga dapat mengakibatkan pencurian identitas yang merugikan secara pribadi. Lebih jauh lagi, kelemahan dalam keamanan infrastruktur digital dapat menimbulkan ancaman serius terhadap keamanan nasional, membuka celah bagi serangan siber yang dapat merusak integritas dan kelangsungan hidup suatu negara.[10]

Untuk menghadapi kompleksitas tersebut, upaya

[9] H. Ajamalus, "Perkembangan Hukum Cyber di Indonesia: Tantangan dan Peluang", Vol. 4, No. 3, Desember 2024, hlm. 110 - 111.

[10] CyberHub. Current Cybersecurity Trend and Future Challenges -Cloud Computing Indonesia.

mengamankan dunia siber memerlukan pendekatan yang menyeluruh. Pengembangan sistem keamanan yang solid menjadi kunci dalam melawan ancaman yang semakin canggih dan berkembang. Hal ini mencakup penerapan teknologi keamanan terbaru, pemantauan yang aktif terhadap ancaman yang mungkin muncul, serta peningkatan kemampuan untuk mendeteksi dan merespons insiden keamanan. Di samping itu, pelatihan keamanan siber tidak hanya diperlukan bagi individu, tetapi juga untuk organisasi secara keseluruhan, agar dapat lebih efektif dalam memahami dan mengelola risiko keamanan.

Dalam penegakan hukum siber, terdapat berbagai tantangan yang dihadapi oleh penegak hukum. Salah satu tantangan utama adalah keterbatasan sumber daya dan kapasitas yang dimiliki. Berdasarkan survei yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN), kurang dari setengah lembaga pemerintah di Indonesia memiliki kebijakan keamanan siber yang memadai, yang menunjukkan adanya kesenjangan signifikan dalam infrastruktur keamanan digital negara. Masalah ini semakin terasa ketika mengingat kasus-kasus seperti serangan siber terhadap database pemerintah atau kebocoran data besar, seperti insiden kebocoran data pengguna platform e-commerce besar di Indonesia pada tahun 2020.[11]

Selain itu, kesulitan dalam mengidentifikasi pelaku kejahatan siber semakin bertambah rumit dengan adanya teknologi enkripsi dan penggunaan jaringan pribadi virtual (VPN) atau server proxy. Teknologi enkripsi yang canggih memungkinkan pelaku untuk melindungi komunikasi dan data mereka, sehingga sulit bagi penegak hukum untuk mencegat atau mengaksesnya. Penggunaan VPN dan server proxy menambah lapisan kesulitan lainnya, karena teknologi ini memungkinkan pelaku untuk menyembunyikan lokasi fisik mereka dan membuat jejak digital mereka lebih sulit dilacak. Hal ini mempersulit penegak hukum dalam menentukan asal serangan siber atau aktivitas ilegal lainnya, karena pelaku bisa terlihat seolaholah beroperasi dari negara yang berbeda, atau bahkan dari beberapa negara, sehingga investigasi menjadi lebih kompleks dan sering kali membutuhkan

[11] Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukuk Siber di Indonesia", Vol. 2, No. 1, April 2024, hlm. 12.

kerjasama antar negara.

Pembangunan dan pengaturan lembaga keamanan siber nasional yang kuat merupakan syarat utama untuk mencapai sistem keamanan siber yang efektif. Penanganan keamanan siber perlu dilakukan secara terintegrasi, melibatkan berbagai lembaga terkait seperti intelijen, penegak hukum, kementerian pertahanan, TNI, serta pemerintah sebagai regulator, diwakili oleh Kominfo, ISSIRTI, dan Lembaga Sandi Negara. Meskipun Indonesia telah membentuk berbagai lembaga dan undang-undang untuk menangani isu keamanan siber, masih terdapat beberapa tantangan yang menghambat pencapaian tujuan tersebut. Menurut ABC News, pada tahun 2013, Indonesia tercatat sebagai sumber serangan siber terbanyak di dunia, dengan serangan peretasan yang merugikan berbagai situs web. Meskipun pemerintah telah memprioritaskan masalah keamanan siber, keberlanjutan kejahatan siber selama beberapa tahun terakhir disebabkan oleh belum adanya lembaga dan peraturan yang memadai. Untuk menghadapi tingginya tingkat kejahatan siber, salah satu alternatif kebijakan adalah memasukkan keamanan siber dalam konteks pertahanan, yang memerlukan pembangunan infrastruktur pendukung, seperti satelit khusus untuk pertahanan dan penanggulangan ancaman siber, mengingat banyak penyedia telekomunikasi yang dimiliki oleh modal asing.

Tantangan utama dalam penegakan keamanan siber di Indonesia dalam beberapa tahun terakhir melibatkan beberapa faktor penting. Pertama, tingkat pemahaman masyarakat Indonesia mengenai keamanan siber masih rendah, sehingga kesadaran akan pentingnya perlindungan siber bagi pengguna internet masih terbatas (Maulia, 2017). Meskipun Standar Kompetensi Kerja Nasional Indonesia (SKKNI) telah menetapkan sektor Keamanan Informasi sebagai standar untuk keamanan informasi di tempat kerja, sosialisasi mengenai hal ini masih sangat terbatas. Kurangnya promosi yang intensif dan kesulitan dalam memperbarui unit kompetensi dalam SKKNI menghambat upaya sosialisasi, apalagi dengan pesatnya perkembangan teknologi. Kedua, kebijakan pemerintah yang masih minim dan kurang spesifik mengenai keamanan informasi menjadi hambatan, terutama karena UU ITE tidak memberikan rincian mendalam mengenai ancaman siber di era modern. UU No.19/2016 tentang Perubahan UU

ITE No.11/2008 hanya memberikan gambaran umum tentang penegakan hukum siber, tanpa menyediakan langkah-langkah konkret yang dapat diambil pemerintah. Pembatalan RUU KKS pada 2019 semakin mempertegas kurangnya dasar hukum untuk menegakkan keamanan siber. Ketiga, kurangnya alokasi kebijakan dan sumber daya yang memadai oleh pemerintah untuk penegakan keamanan siber di seluruh Indonesia menjadi masalah serius. Data dari Badan Pusat Statistik (BPS) tahun 2017 menunjukkan bahwa pembangunan infrastruktur digital di Indonesia masih tidak merata, yang menjadi semakin penting karena sebagian besar pengguna internet berada di daerah perkotaan besar.

Untuk membangun keamanan siber di Indonesia di masa depan, ada empat elemen penting yang perlu dipenuhi untuk mendukung perkembangan teknologi informasi. Ini mencakup pengembangan perangkat lunak seperti sistem dan aplikasi, kemajuan alat keras (hardware), infrastruktur teknologi informasi, manajemen konten, telekomunikasi dan jaringan, serta pengembangan internet dan e-commerce. Selain itu, menurut Ardiyanti (2014) dalam tulisannya Cyber Security dan Tantangan Pengembangannya di Indonesia, langkah penting lainnya adalah pengorganisasian terkait dengan penggunaan sistem teknologi informasi, yang mencakup aspek-aspek seperti sistem informasi, kompetisi organisasi, pengambilan keputusan organisasi, serta penerapan sistem informasi dalam organisasi. Oleh karena itu, penguatan keamanan siber di masa depan harus dibangun berdasarkan lima pilar utama, yaitu kepastian hukum melalui undang-undang cybercrime, langkah-langkah teknis dan prosedural untuk pengguna akhir, bisnis, penyedia layanan, dan perusahaan perangkat lunak. Selain itu, struktur organisasi yang berkembang harus menghindari tumpang tindih, meningkatkan kapasitas dan pendidikan pengguna melalui kampanye publik serta komunikasi terbuka mengenai ancaman terbaru dari kejahatan siber, dan memperkuat kerjasama internasional, termasuk kerja sama timbal balik untuk menangani ancaman siber (Ardiyanti, 2014).[12]

1. Tantangan Cyber Securityatau Keamanan Siberdi EraSociety

[12] Yustika Citra Mahendra, " Strategi Penanganan Keamanan Siber (Cyber Security) di Indonesia, vol. 6, No. 2, 2023, hlm. 1946-1947.

5.0

Era Society 5.0 menghadirkan berbagai tantangan, terutama dari perspektif pemerintah. Salah satunya adalah keterbatasan sumber daya manusia yang memiliki keahlian di bidang teknologi dan keamanan, serta kemampuan untuk merancang dan mengimplementasikan sistem keamanan siber di Indonesia. Dengan pesatnya perkembangan teknologi, pembaruan teknologi keamanan siber juga perlu dilakukan secara berkala. Jika para ahli di bidang keamanan tidak mengikuti perkembangan teknologi, maka sistem keamanan siber yang ada saat ini akan kesulitan menghadapi ancaman-ancaman baru yang terus berkembang.[13]

Menurut Hasyim Gautama, dikutip dari Ardiyanti (2014) adabeberapa obstacle atau tantanganyang akan dihadapi terhadapperkembangan cyber security dalam skala nasional, diantaranya:

1) Penyelenggara negara masih memiliki pemahaman yanglemah tentang masalah cyber security.
2) Beberapa layanan internet masih menggunakan server di luar negeri.
3) Kurangnya sistem yang aman.
4) Sering terjadinya kejahatan dunia maya yang membuatnya sulit untuk ditangani.
5) Masalah dengan tata kelola lembaga keamanansiber nasional.
6) Lemahnya kesadaran akan ancaman serangan dunia maya.
7) Kurangnya industri yang mengembangkan perangkat keras untuk memperkuat keamanan dunia maya.

Implikasi Hukum terhadap Cyber

Implikasi hukum terhadap kejahatan siber (cybercrime) di Indonesia sangat penting untuk menghadapi ancaman yang muncul seiring dengan pesatnya perkembangan teknologi digital. Kejahatan siber, seperti penipuan online, pencurian identitas, dan peretasan data, dapat merugikan individu, perusahaan, dan pemerintah, sehingga

[13] M. Fahli Saputra, "Peran dan Tantangan Cyber Security di Era Socienty 5.0", Vol. 2, (7), 2022, hlm. 353.

hukum berperan memberikan perlindungan bagi korban melalui Undang-Undang ITE (Informasi dan Transaksi Elektronik) yang mengatur berbagai tindakan ilegal di ruang siber. Tindakan pidana siber, seperti penyebaran informasi ilegal atau pemalsuan elektronik, diatur dengan sanksi pidana, baik penjara maupun denda, sesuai tingkat keparahan kejahatannya. Namun, tantangan utama dalam penegakan hukum adalah sifat kejahatan siber yang lintas batas, yang sering kali melibatkan pelaku di luar negeri, memerlukan kerjasama internasional dalam penanganannya. Selain itu, ketersediaan infrastruktur hukum dan sumber daya manusia yang terlatih masih terbatas, yang mempersulit penegakan hukum, terutama dengan adanya teknologi yang digunakan pelaku untuk menyembunyikan identitas mereka. Oleh karena itu, diperlukan peningkatan kapasitas penegak hukum, kerjasama antar lembaga, dan upaya preventif melalui edukasi dan kesadaran masyarakat tentang pentingnya keamanan siber untuk menciptakan ekosistem digital yang aman dan mencegah kejahatan siber lebih lanjut.

Implikasi Hukum terhadap Penegakan HAM di Era Digital

Hukum sangat diperlukan untuk menjaga tatanan masyarakat yang aman dan damai, di mana setiap individu memiliki batasan yang harus dihormati dalam menggunakan smartphone di era digital ini. Bahkan ketika seseorang ingin menyampaikan pendapat, memberikan penilaian, atau berargumen, hal tersebut tetap memiliki batasan yang tidak boleh melukai atau merugikan orang lain, baik secara fisik maupun non-fisik.

Etika dalam penggunaan media sosial sangat penting untuk menjaga batasan diri agar dapat hidup harmonis dalam masyarakat. Etika membantu kita untuk lebih selektif dalam menyaring informasi yang diterima dan tidak mudah terpengaruh oleh informasi yang tidak jelas sumbernya, atau yang biasa disebut sebagai hoaks. Sebagai pengguna media sosial yang baik, kita juga seharusnya menghindari memberikan komentar sembarangan dan menyebarkan informasi yang dapat menimbulkan dampak negatif, seperti perundungan, ujaran kebencian, atau konten sensitif yang bisa merugikan orang lain. Oleh karena itu, hukum diperlukan untuk memberikan batasan yang jelas bagi pengguna media sosial.

Sebagai negara hukum, Indonesia memiliki kewajiban untuk menegakkan dan melindungi hak asasi manusia, termasuk memberikan kebebasan berekspresi dengan menetapkan batasan yang jelas dalam penggunaan media sosial. Hal ini sesuai dengan Pasal 28I ayat (4) UUD 1945 yang menyatakan: "Perlindungan, pemajuan, penegakan, dan pemenuhan hak asasi manusia adalah tanggung jawab negara, terutama pemerintah." Dengan demikian, peran hukum sangat penting untuk mengatur pendapat, penilaian, dan sanggahan agar pengguna digital dapat menggunakan teknologi dengan bijak di era yang terus berkembang. (MKRI, 2023).[14]

Hukum sebagai Pencegahan Cyber Bullying, Berita Hoaks, Disinformasi, Misinformasidan Pencemaran Nama Baik

Selain berfungsi sebagai batasan bagi individu dalam menilai, menyanggah, dan berpendapat, hukum juga berperan penting sebagai pelindung untuk mencegah terjadinya cyberbullying, penyebaran hoaks, disinformasi, misinformasi, serta pencemaran nama baik. Undang-Undang ITE (Informasi dan Transaksi Elektronik) adalah regulasi yang mengatur penggunaan teknologi informasi dan elektronik. Undang-undang ini bertujuan untuk memastikan agar pengguna teknologi informasi dan elektronik dapat menggunakannya dengan lebih aman dan efektif.[15]

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga mencakup sejumlah pasal yang mengatur berbagai aspek terkait penggunaan teknologi informasi dan transaksi elektronik, seperti hak dan kewajiban pengguna internet, perlindungan data pribadi, tindakan pidana yang berkaitan dengan penyalahgunaan teknologi informasi, serta prosedur penyelesaian sengketa elektronik. Berikut ini adalah beberapa pasal penting yang terdapat dalam Undang-Undang ITE:

1) Pasal 27 Ayat (3): Penyebaran Informasi dan/atau Dokumen Elektronik yang melanggar kesusilaan.

[14] Siti Nur Bayinah, "Implikasi Hukum Tergadap Penegakan Ham di Era Digital", Vol. 3, No 6, 2023, hlm.

[15] Siti Nur Bayinah, "Implikasi Hukum Tergadap Penegakan Ham di Era Digital", Vol. 3, No 6, 2023, hlm. 6.

2) Pasal 27 Ayat 4: Penghinaan dan/atau pencemaran nama baik melalui media elektronik.
3) Pasal 28: Penghinaan dan/atau pencemaran nama baik.
4) Pasal 45 Ayat 1: Pelanggaran terhadap hak cipta dan/atau hak terkait.
5) Pasal 51 Ayat 2: Tindak pidana penyebaran konten yang melanggar norma agama dan/atau norma kesusilaan. Dan,6.Pasal 54: Penyimpanan data elektronik.[16]

Cyberbullying, atau perundungan dunia maya, merujuk pada perilaku bullying yang dilakukan dengan memanfaatkan teknologi digital. Bentuk perundungan ini dapat terjadi di media sosial, platform obrolan, platform game, maupun melalui ponsel. Menurut Think Before Text, cyberbullying adalah tindakan agresif yang dilakukan dengan tujuan tertentu oleh individu atau kelompok, menggunakan media elektronik, secara berulang-ulang terhadap seseorang yang dianggap tidak mampu melawan tindakan tersebut. Dalam hal ini, terdapat ketidakseimbangan kekuatan antara pelaku dan korban, yang mengacu pada perbedaan dalam kapasitas fisik dan mental. Dalam hukum Indonesia, cyberbullying diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 45 ayat (5) UU ITE secara jelas menyatakan bahwa "Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan." Artinya, pelaku cyberbullying dapat dijatuhi pidana berdasarkan pengaduan yang diajukan oleh korban itu sendiri.[17] Berikut adalah beberapa jenis-jenis cyberbullying:

1) Outing and Trickery: Outing adalah tindakan membocorkan rahasia atau foto pribadi seseorang yang dapat menyebabkan rasa malu atau depresi. Sedangkan trickery adalah penipuan untuk membujuk korban agar memberikan rahasia atau foto pribadi mereka.

2) Flaming: Flaming merujuk pada upaya untuk memprovokasi, mengejek, atau menghina korban dengan tujuan menyinggung

[16] Siti Nur Bayinah, "Implikasi Hukum Tergadap Penegakan Ham di Era Digital", Vol. 3, No 6, 2023, hlm. 7.

[17] Fergie Brillian Arthaleza, "Perspektif Hukum Telematika Terhadap Kasus Cyber Crime di Indonesia", hlm. 7.

perasaan mereka. Biasanya dilakukan dengan mengirim pesan yang mengandung kata-kata marah dan emosional.

3) Impersonation: Impersonation adalah tindakan menyamar atau berpura-pura menjadi orang lain untuk mengirim pesan atau status yang merugikan korban. Hal ini sering dilakukan melalui akun palsu di media sosial seperti Twitter dan Instagram.

4) Harassment: Harassment adalah tindakan mengirimkan komentar atau pesan secara berulang dengan tujuan menyebabkan kegelisahan pada korban. Biasanya, pesan tersebut berisi hasutan agar orang lain mengikuti perilaku yang sama.

5) Cyberstalking: Cyberstalking adalah tindakan mengintai, mengganggu, dan merusak reputasi seseorang secara intens, yang membuat korban merasa terancam dan sering kali mengalami depresi.

6) Denigration: Denigration adalah tindakan sengaja untuk merusak reputasi seseorang dengan menyebarkan keburukan mereka melalui internet, yang bertujuan untuk merusak nama baik dan kredibilitas orang tersebut.

Kebocoran data merujuk pada pengunggahan data pribadi yang sensitif ke internet secara tidak hati-hati atau berlebihan, tanpa mempertimbangkan dampak yang mungkin timbul. Istilah lain untuk kebocoran data adalah data leakage, yang sering menjadi ancaman bagi perusahaan yang menyimpan data penting atau rahasia. Ancaman ini muncul karena adanya kemungkinan orang-orang yang tidak bertanggung jawab dapat mengakses dan memanipulasi data tersebut. Ada enam penyebab utama kebocoran data, yaitu kesalahan dalam konfigurasi perangkat lunak, penipuan yang dilakukan melalui rekayasa sosial, penggunaan kata sandi yang sama berulang kali, pencurian perangkat yang mengandung data sensitif, kerentanannya perangkat lunak, serta penggunaan kata sandi bawaan atau default password.[18]

[18] Fergie Brillian Arthaleza, "Perspektif Hukum Telematika Terhadap Kasus Cyber Crime di Indonesia", hlm. 8.

Kebocoran data ini termasuk dalam tindak pidana penyalahgunaan data pribadi, yang diatur dalam UU No 11 Tahun 2008 tentang ITE, khususnya Pasal 26 Ayat 1 yang menyatakan, "Setiap penggunaan informasi melalui media elektronik yang melibatkan data pribadi seseorang harus dilakukan dengan persetujuan dari orang tersebut." Ketentuan ini kemudian dijabarkan lebih lanjut dalam PP No 82/2012 dan PP No 71/2019.

Kebijakan Hukum Pidana dalam Penanggulangan Cyber Crime

Kebijakan pencegahan kejahatan dunia maya dengan menggunakan hukum pidana mencakup kebijakan penal yang merupakan bagian dari kebijakan kriminal. Dari perspektif kebijakan pidana, upaya untuk mencegah kejahatan (termasuk cybercrime) tidak dapat dilakukan secara terpisah hanya dengan hukum pidana, melainkan harus melalui pendekatan yang lebih sistematis.[19]

Pada dasarnya, politik atau kebijakan hukum pidana bertujuan untuk merumuskan hukum pidana secara tepat, memberikan pedoman bagi pembentuk undang-undang, dan memastikan pelaksanaannya. Kebijakan legislatif sangat berperan dalam tahap-tahap selanjutnya, karena saat peraturan perundang-undangan pidana dibuat, tujuan yang ingin dicapai sudah ditentukan. Dalam hal ini, Pasal 26 ayat (2) UU ITE tidak memberikan sanksi pidana kepada pelaku, sehingga korban hanya dapat mengajukan gugatan perdata. Selain itu, Pasal 26 UU ITE hanya mencakup perlindungan dasar. Pakar teknologi informasi menilai bahwa Pasal 26 UU ITE memiliki kelemahan, terutama karena tidak memberikan perlindungan bagi pengguna yang data pribadinya dimanfaatkan untuk memperoleh keuntungan oleh perusahaan. Keamanan data bertujuan untuk 1) Melindungi data agar tidak dapat diakses oleh pihak yang tidak berkepentingan, dan 2) Mencegah pihak yang tidak berkepentingan untuk memasukkan atau menghapus data.

- Kebijakan kriminalisasi atau rumusan hukum pidana di Indonesia terkait permasalahan cybercrime selamaini dapat

[19] James Popham, Mary McCluskey and Michael Ouellet, Exploring Police-Reported Cybercrime In Canada Variation AndCorrelates, Policing: An International Journal, Vol. 43, No. 1, 2020, hlm. 35.

diidentifikasi sebagai berikut:

1) Dalam KUHP

Rumusan tindak pidana dalam Kitab Undang-Undang Hukum Pidana (KUHP) sebagian besar masih bersifat konvensional dan belum secara langsung mengakomodasi perkembangan cybercrime. Selain itu, terdapat berbagai kelemahan dan keterbatasan dalam menghadapi kemajuan teknologi serta kejahatan yang terkait dengan teknologi tinggi yang sangat beragam. Sebagai contoh, KUHP mengalami kesulitan dalam menangani kasus pemalsuan kartu kredit dan transfer dana elektronik karena tidak ada aturan khusus yang mengatur hal tersebut. Ketentuan yang ada hanya mencakup: a) sumpah atau pernyataan palsu (Pasal 242); b) penghindaran mata uang dan uang kertas (Pasal 244-252); c) pemalsuan stempel dan tanda (Pasal 253-262); dan d) pemalsuan surat (Pasal 263-276) (Nurianto Rachmad Soepadmo, Impact Analysis of Information and Electronic Transactions Law).[20]

2) Undang-undang di luar KUHP

a) Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi menetapkan ancaman pidana terhadap: a) Manipulasi akses ke jaringan telekomunikasi (Pasal 50 jo. Pasal 22); b) Gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi (Pasal 55 jo. Pasal 38); c) Penyadapan informasi melalui jaringan telekomunikasi (Pasal 56 jo. Pasal 40).

b) Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan atas UU No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi; Pasal 38 UU No. 15 Tahun 2002 tentang Tindak Pidana

[20] Law No. 19 Year 2016) onthe Level of Cyber-Crime in Social Media, International Journal of Innovation, Creativity and Change, Vol. 12, No. 8, 2020, hlm. 490.

Pencucian Uang; dan Pasal 44 ayat (2) UU No. 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi, mengakui rekaman elektronik sebagai alat bukti yang sah.

3) Undang-Undang No. 32 Tahun 2002 tentang Penyiaran mengatur tindak pidana, antara lain: 1) Pasal 57 jo. Pasal 36 ayat (5) mengancam pidana terhadap siaran yang: a) mengandung fitnah, hasutan, penyesatan, atau kebohongan; b) menonjolkan unsur kekerasan, cabul, perjudian, atau penyalahgunaan narkotika dan obat terlarang; atau c) memicu pertentangan antara suku, agama, ras, dan antar golongan; 2) Pasal 57 jo. Pasal 36 ayat (6) mengancam pidana terhadap siaran yang merendahkan, melecehkan, atau mengabaikan nilai agama, martabat manusia, atau merusak hubungan internasional; 3) Pasal 58 jo. Pasal 46 ayat (3) mengancam pidana terhadap siaran iklan niaga yang memuat: a) promosi yang berkaitan dengan ajaran agama, ideologi, individu, atau kelompok yang dapat menyinggung perasaan atau merendahkan martabat orang lain; b) promosi minuman keras, zat adiktif, atau rokok yang menampilkan wujud rokok; c) hal-hal yang bertentangan dengan kesusilaan dan nilai-nilai agama; atau d) eksploitasi anak di bawah umur.[21]

4) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mencantumkan ketentuan pidana bagi siapa saja yang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, atau membuat informasi elektronik atau dokumen elektronik yang mengandung muatan:[22] 1) Pelanggaran kesusilaan, perjudian, penghinaan, pencemaran nama baik, pemerasan,

[21] Muhammad Isnaeni Puspito Adhi and Eko Soponyono, Crime Combating Policy of Carding in Indonesia in the PoliticalPerspective of Criminal Law, Law Reform, Vol. 17, No. 2, 2021, hlm. 140.

[22] Sri Hartati, Hadi Karyono, and Hudi Karno Sabowo, Implementation of The Law on Information and Electronic Transactionsand Pancasila Law Enforcement Related to Cybercrimes in Indonesia, International Journal of Educational Research & Social Sciences,Vol. 3, No. 1, 2022, hlm. 430.

atau pengancaman (Pasal 27); 2) Penyebaran berita bohong yang merugikan konsumen dalam transaksi elektronik atau yang dapat menimbulkan kebencian atau permusuhan berdasarkan SARA (Pasal 28); 3) Pengiriman informasi yang berisi ancaman kekerasan (Pasal 29); 4) Akses ilegal ke komputer atau sistem elektronik milik orang lain (Pasal 30); 5) Intersepsi atau penyadapan informasi elektronik yang tidak bersifat publik (Pasal 31-33); 6) Penyalahgunaan perangkat keras atau perangkat lunak untuk melakukan perbuatan dalam Pasal 27-33 (Pasal 34); 7) Manipulasi data elektronik agar tampak otentik (Pasal 35); 8) Tindakan yang menyebabkan kerugian bagi orang lain (Pasal 36); 9) Perbuatan yang dilarang di luar wilayah Indonesia terhadap sistem elektronik di Indonesia (Pasal 37); 10) Perbuatan yang dilarang di dalam wilayah Indonesia terhadap sistem elektronik di Indonesia (Pasal 38).

Kesimpulan

Keamanan siber telah menjadi isu yang sangat penting di era digital, terutama dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi dalam berbagai sektor kehidupan. Perkembangan teknologi ini, meskipun memberikan banyak manfaat, juga memunculkan risiko besar berupa kejahatan siber (cybercrime). Di Indonesia, kejahatan siber mencakup berbagai bentuk, seperti pencurian data pribadi, peretasan, penyebaran virus komputer, penipuan daring, dan pencemaran nama baik. Ancaman-ancaman ini tidak hanya berdampak pada individu dan perusahaan tetapi juga berpotensi mengancam keamanan nasional. Pemerintah Indonesia telah mengeluarkan sejumlah regulasi, termasuk UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan revisinya pada 2016, untuk menangani tantangan ini. UU ITE menjadi dasar hukum utama dalam menangani isu-isu siber, termasuk transaksi elektronik, perlindungan data pribadi, dan penanganan konten ilegal. Meskipun demikian, terdapat beberapa kelemahan dalam implementasi hukum ini, seperti cakupan yang terbatas dalam menangani kejahatan yang berkembang pesat dan belum adanya regulasi khusus yang lebih terperinci untuk ancaman modern.

Tantangan tersebut meliputi kurangnya infrastruktur hukum yang memadai, kapasitas penegakan hukum yang masih terbatas, rendahnya kesadaran masyarakat akan keamanan digital, serta sifat kejahatan siber yang lintas batas negara. Selain itu, dengan semakin luasnya adopsi teknologi di Indonesia, ancaman terhadap infrastruktur vital seperti data pemerintah dan informasi sensitif menjadi semakin mengkhawatirkan. Hal ini menunjukkan perlunya langkah hukum yang lebih komprehensif, pengembangan teknologi keamanan yang lebih mutakhir, dan kolaborasi internasional untuk melindungi kedaulatan digital negara.Upaya ke depan perlu difokuskan pada penguatan kerangka hukum nasional yang responsif terhadap perkembangan teknologi, peningkatan sumber daya manusia di bidang keamanan siber, penyusunan kebijakan keamanan yang lebih terintegrasi, serta edukasi publik tentang pentingnya keamanan siber untuk mengurangi dampak kejahatan di dunia maya.

Referensi

Ardiyanti, Handrini. "Cyber-security dan tantangan pengembangannya di indonesia." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 5.1 (2016).

Ersya, Muhammad Prima. "Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia." *Journal of Moral and Civic Education* 1.1 (2017): 50-62.

Ketaren, Eliasta. "Cybercrime, cyber space, dan cyber law." *Jurnal Times* 5.2 (2016): 35-42. Nugraha, Riko. "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di

Indonesia." Jurnal Ilmiah Hukum Dirgantara 11.2 (2021).

Ramadhan, Iqbal. "Strategi Keamanan Cyber Security di Kawasan Asia Tenggara." *Jurnal Asia Pacific Studies* 3.2 (2019): 181-192.

Najwa, Fadhila Rahman. "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia." *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dah Hukum* 2.1 (2024): 8-16.

Mahendra, Yustika Citra, and Ni Komang Desy Setiawati Arya Pinatih. "Strategi Penanganan Keamanan Siber (Cyber Security) Di

Indonesia." *Jurnal Review Pendidikan Dan Pengajaran (JRPP)* 6.4 (2023): 1941-1949.

Ajamalus, H., and Agung Cucu Purnawirawan. "Perkembangan Hukum Cyber di Indonesia: Tantangan dan Peluang." Bulletin of Community Engagement 4.3 (2024): 109-116.

Saputra, Muhammad Fahli, and Aji Wibawa. "Peran dan Tantangan Cyber Security di Era Society 5.0." *Jurnal Inovasi Teknologi dan Edukasi Teknik* 2.7 (2022): 349-354.

Muchtar, Panca, et al. "MENJELAJAHI DUNIA CYBER TANTANGAN, PELUANG, DAN

ETIKA DI ERA DIGITAL." *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora* 2.1 (2024): 293-300.

Bayinah, Siti Nur, and Sefi Anggraini Nur Vitasari. "Implikasi hukum terhadap penegakan HAM di era digital." *Innovative: Journal Of Social Science Research* 3.6 (2023): 10498-10508.

Ramayanti, Herni, and Arief Fahmi Lubis. "Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional." *Jurnal Hukum dan HAM Wara Sains* 2.09 (2023): 904-912.

Arthaleza, Fergie Brillian, et al. "PERSPEKTIF HUKUM TELEMATIKA TERHADAP KASUS CYBER CRIME DI INDONESIA."

Kasim, Zainuddin. "Kebijakan Hukum Pidana Untuk Penanggulangan Cyber Crime Di Indonesia." *Indragiri Law Review* 2.1 (2024): 18-24.