JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 2 No: 5, Oktober – November 2025
E-ISSN : 3046-4560

PENERAPAN HUKUM ACARA PIDANA TERHADAP KEJAHATAN SIBER (CYBERCRIME)

APPLICATION OF CRIMINAL PROCEDURE LAW TOWARDS CYBERCRIME

Frank Bradley Refra
Fakultas Hukum, Universitas Bung Karno
Email: frankrefra01@gmail.com

Article Info

Article history :
Received : 04-11-2025
Revised : 05-11-2025
Accepted : 07-11-2025
Pulished : 09-11-2025

Abstract

The development of information technology has brought significant changes in various aspects of human life, including in the field of criminal law. One of the negative impacts of technological advancement is the emergence of cybercrime, which refers to criminal acts committed through computer networks or the internet as the main medium. Cybercrime presents new challenges for Indonesia's criminal justice system due to its distinct characteristics compared to conventional crimes. Although the Indonesian Criminal Procedure Code (KUHAP) remains the primary foundation for investigation, prosecution, and trial procedures, the application of criminal procedural law to cybercrime still faces various obstacles, particularly in terms of evidence, jurisdiction, and offender identification. This study aims to analyze how criminal procedural law is applied in handling cybercrime cases in Indonesia and to assess its effectiveness in ensuring legal certainty and protecting human rights. The research method used is normative juridical, employing statutory, conceptual, and comparative approaches. The data are obtained from legislation, legal literature, and relevant court decisions concerning cybercrime cases. The results show that the application of KUHAP to cybercrime cases remains limited, as it does not explicitly regulate digital evidence or forensic procedures. Although Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and Supreme Court Regulation No. 4 of 2020 provide additional legal bases for electronic evidence and digital trials, several obstacles persist, including the limited technical capacity of law enforcement officials, inconsistent standards of proof, and inadequate international cooperation in addressing transnational cybercrime. Therefore, it is necessary to reform the criminal procedural system to make it more adaptive to technological advancements, by formally recognizing digital evidence, strengthening law enforcement capacity, and establishing cross-border cooperation mechanisms for effective cyber law enforcement.This research is expected to contribute to the development of Indonesia's criminal procedural law so that it can effectively respond to the challenges of the digital era while upholding the principles of justice, legal certainty, and human rights protection in criminal proceedings.

Keywords: Criminal Procedure Law, Cybercrime, ITE Law

Abstrak

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam bidang hukum pidana. Salah satu dampak negatif dari kemajuan teknologi adalah munculnya kejahatan siber (cybercrime), yaitu tindak pidana yang dilakukan dengan menggunakan jaringan komputer atau internet sebagai sarana utama. Kejahatan siber menimbulkan tantangan baru bagi sistem peradilan pidana Indonesia karena karakteristiknya yang berbeda dengan tindak pidana konvensional.

JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 2 No: 5, Oktober – November 2025
E-ISSN : 3046-4560

Meskipun Kitab Undang-Undang Hukum Acara Pidana (KUHAP) masih menjadi dasar utama dalam proses penyidikan, penuntutan, dan pemeriksaan perkara pidana, namun dalam praktiknya penerapan hukum acara pidana terhadap cybercrime sering menghadapi kendala, terutama dalam hal pembuktian, yurisdiksi, dan identifikasi pelaku. Penelitian ini bertujuan untuk menganalisis bagaimana hukum acara pidana diterapkan dalam penanganan kejahatan siber di Indonesia serta menilai efektivitasnya dalam memberikan kepastian hukum dan perlindungan terhadap hak asasi manusia. Metode penelitian yang digunakan adalah yuridis normatif, dengan pendekatan perundang-undangan, konseptual, dan komparatif. Data diperoleh dari peraturan perundang-undangan, literatur hukum, serta berbagai putusan pengadilan yang relevan dengan kasus kejahatan siber. Hasil penelitian menunjukkan bahwa penerapan KUHAP terhadap tindak pidana siber masih terbatas karena belum secara eksplisit mengatur mengenai alat bukti elektronik dan prosedur digital forensik. Meskipun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Mahkamah Agung Nomor 4 Tahun 2020 telah memberikan dasar hukum tambahan untuk pembuktian dan persidangan elektronik, masih terdapat kendala berupa kurangnya kemampuan teknis aparat penegak hukum, perbedaan standar pembuktian, serta keterbatasan kerja sama internasional dalam menangani pelaku lintas negara. Oleh karena itu, diperlukan reformasi hukum acara pidana yang lebih adaptif terhadap perkembangan teknologi, termasuk pengakuan formal terhadap bukti digital, penguatan kapasitas sumber daya manusia penegak hukum, dan pembentukan mekanisme kerja sama lintas negara dalam penegakan hukum siber. Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan hukum acara pidana di Indonesia agar mampu menjawab tantangan era digital, dengan tetap menjunjung tinggi asas keadilan, kepastian hukum, dan perlindungan hak asasi manusia dalam proses peradilan pidana.

Kata Kunci: Hukum Acara Pidana, Cybercrime, UU ITE

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era globalisasi telah membawa dampak yang sangat signifikan terhadap berbagai aspek kehidupan manusia. Perubahan yang terjadi tidak hanya dalam bidang sosial, ekonomi, dan budaya, tetapi juga dalam bidang hukum, khususnya hukum pidana. Internet dan teknologi digital telah menciptakan dunia baru tanpa batas geografis, di mana interaksi manusia dapat berlangsung secara cepat dan lintas negara. Namun, kemajuan teknologi ini juga menimbulkan tantangan baru berupa munculnya berbagai bentuk kejahatan yang dilakukan melalui jaringan komputer atau sistem elektronik, yang dikenal sebagai kejahatan siber (cybercrime).

Fenomena ini menjadi perhatian serius karena dapat merugikan individu, korporasi, bahkan negara, baik secara ekonomi maupun sosial.Kejahatan siber memiliki karakteristik yang berbeda dari kejahatan konvensional. Jika kejahatan konvensional biasanya terjadi di dunia fisik, maka cybercrime berlangsung di dunia maya (cyberspace) yang bersifat virtual dan tidak mengenal batas yurisdiksi. Bentuk kejahatan ini sangat beragam, mulai dari peretasan (hacking), pencurian data pribadi, penyebaran malware, penipuan daring (online fraud), pornografi anak, penyebaran hoaks, hingga kejahatan siber yang bersifat politik seperti cyber terrorism. Kompleksitas dan sifat lintas batas dari kejahatan siber menyebabkan proses penegakan hukumnya menjadi jauh lebih sulit dibandingkan dengan tindak pidana biasa. Aparat penegak hukum sering kali menghadapi kendala dalam mengidentifikasi pelaku, mengumpulkan alat bukti digital, serta menentukan yurisdiksi yang berwenang untuk memproses perkara tersebut.

Rumusan Masalah

1. Konsep Tindak Pidana Siber (Cyber)
2. Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di

Indonesia.

Tujuan

Penulisan ini bertujuan untuk memberikan pemahaman yang komprehensif mengenai konsep tindak pidana siber (cybercrime) dalam sistem hukum di Indonesia, serta menelaah berbagai aspek hukum, sosial, dan teknologi yang terkait dengan kejahatan di dunia maya. Secara khusus, tujuan penelitian ini adalah sebagai berikut:

1. Menjelaskan secara mendalam konsep dan karakteristik tindak pidana siber, termasuk perbedaan mendasar antara kejahatan siber dan tindak pidana konvensional, baik dari sisi pelaku, modus operandi, alat yang digunakan, maupun ruang lingkup hukumnya. Penjelasan ini diharapkan dapat memperluas wawasan akademik tentang bentuk-bentuk kejahatan baru yang lahir akibat perkembangan teknologi informasi.
2. Menganalisis dasar hukum dan regulasi yang mengatur tindak pidana siber di Indonesia, dengan meninjau Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta kaitannya dengan hukum pidana umum dalam KUHP dan hukum internasional seperti Budapest Convention on Cybercrime tahun 2001.
3. Mengidentifikasi bentuk-bentuk kejahatan siber yang berkembang di era digital, seperti peretasan (hacking), penyebaran malware, pencurian data pribadi, penipuan daring (online fraud), cyber terrorism, dan cyber espionage. Setiap bentuk kejahatan tersebut dianalisis dari aspek hukum dan dampaknya terhadap keamanan nasional maupun kehidupan sosial masyarakat.
4. Mengkaji efektivitas penegakan hukum terhadap pelaku tindak pidana siber di Indonesia, termasuk kendala yang dihadapi aparat penegak hukum dalam proses penyelidikan, pembuktian alat bukti elektronik, hingga proses penuntutan di pengadilan. Kajian ini mencakup pula penerapan prinsip due process of law dalam konteks hukum digital.
5. Menelusuri peran dan tanggung jawab lembaga-lembaga negara dalam penanggulangan kejahatan siber, seperti Kepolisian Negara Republik Indonesia (Polri), Kejaksaan, Kementerian Komunikasi dan Informatika (Kominfo), serta Badan Siber dan Sandi Negara (BSSN), dalam membangun sistem keamanan siber nasional yang kuat dan berkelanjutan.
6. Menilai pentingnya kerja sama internasional dan regional dalam memberantas kejahatan siber lintas negara (transnational cybercrime), mengingat kejahatan di dunia maya tidak mengenal batas yurisdiksi. Hal ini mencakup kerja sama dengan organisasi internasional, pertukaran informasi intelijen digital, serta mekanisme ekstradisi pelaku lintas negara.
7. Memberikan rekomendasi strategis terhadap kebijakan dan regulasi hukum nasional agar mampu menjawab tantangan era digital, termasuk penguatan literasi digital masyarakat, peningkatan kapasitas sumber daya manusia di bidang hukum dan teknologi, serta perlindungan hukum bagi korban kejahatan siber.
8. Menegaskan pentingnya perlindungan hak asasi manusia dan privasi individu di ruang digital, agar upaya penegakan hukum terhadap tindak pidana siber tidak bertentangan dengan prinsip-prinsip keadilan, kebebasan berekspresi, dan hak atas perlindungan data pribadi sebagaimana

diatur dalam konstitusi serta peraturan perundang- undangan yang berlaku.

Secara keseluruhan, penelitian ini diharapkan dapat menjadi kontribusi ilmiah bagi pengembangan ilmu hukum pidana di Indonesia, khususnya dalam menghadapi tantangan baru yang muncul akibat pesatnya kemajuan teknologi informasi. Dengan memahami konsep dan tujuan penanganan tindak pidana siber, diharapkan terbentuk sistem hukum yang adaptif, adil, dan mampu memberikan perlindungan hukum yang efektif bagi seluruh masyarakat di era digital.

HASIL DAN PEMBAHASAN

Konsep Tindak Pidana Cyber

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam tatanan kehidupan manusia modern. Aktivitas sosial, ekonomi, hingga politik kini banyak dilakukan melalui media digital. Namun, kemajuan ini tidak hanya membawa manfaat, melainkan juga menimbulkan bentuk kejahatan baru yang dikenal dengan istilah tindak pidana cyber atau cybercrime. Kejahatan ini tidak lagi terbatas pada ruang dan waktu sebagaimana tindak pidana konvensional, melainkan terjadi di dunia maya (cyberspace) yang bersifat tanpa batas (borderless).

Indonesia sebagai salah satu negara dengan tingkat penggunaan internet yang tinggi juga menghadapi tantangan serius dalam menangani tindak pidana siber. Kejahatan siber tidak hanya berdampak pada individu, tetapi juga dapat mengancam stabilitas ekonomi, keamanan nasional, serta kepercayaan publik terhadap sistem digital. Oleh karena itu, memahami konsep dasar tindak pidana cyber menjadi penting dalam rangka membangun sistem hukum yang adaptif terhadap kemajuan teknologi.

Pengertian Tindak Pidana Cyber

Tindak pidana cyber (cybercrime) merupakan bentuk kejahatan yang dilakukan dengan menggunakan teknologi komputer, jaringan internet, atau perangkat digital lainnya sebagai alat, sasaran, maupun lokasi terjadinya tindak pidana. Menurut Barda Nawawi Arief (2006), cybercrime merupakan salah satu bentuk negatif dari perkembangan teknologi yang berdampak luas terhadap berbagai aspek kehidupan manusia modern.

Sementara itu, Girasa (2002) menyebutkan bahwa cybercrime mencakup berbagai tindak pidana yang ditemukan dalam hukum pidana, namun pelaksanaannya dilakukan dengan bantuan teknologi komputer sebagai perangkat utama. Dengan kata lain, komputer dapat berfungsi sebagai objek, alat, maupun sarana dari tindak pidana tersebut.

Cybercrime dapat dibedakan menjadi dua pengertian, yaitu:

1. Cybercrime dalam arti sempit, yaitu tindak pidana yang dilakukan terhadap sistem komputer atau jaringan komputer, misalnya peretasan (hacking), penyadapan, atau pengrusakan sistem.
2. Cybercrime dalam arti luas, yaitu semua tindak pidana yang dilakukan dengan menggunakan sarana komputer atau teknologi informasi, termasuk penipuan daring, pencucian uang digital, penyebaran hoaks, dan sebagainya (Aldriano & Priyambodo, 2022).

Perbedaan ini penting untuk memahami ruang lingkup tindak pidana cyber, karena tidak semua kejahatan yang melibatkan komputer dapat dikategorikan sama beratnya. Dalam beberapa kasus, cybercrime dapat berakibat lebih kompleks dibanding tindak pidana konvensional karena

sifatnya yang borderless, sulit dilacak, dan melibatkan pelaku lintas negara.

Latar Belakang Munculnya Cybercrime

Kemunculan cybercrime tidak terlepas dari revolusi digital dan meningkatnya ketergantungan manusia terhadap teknologi informasi. Menurunnya interaksi sosial secara fisik dan meningkatnya aktivitas daring telah menciptakan ruang baru bagi pelaku kejahatan. Dunia maya menjadi tempat yang memungkinkan pelaku untuk bertindak tanpa harus hadir secara fisik di lokasi kejadian.

Indonesia pertama kali merasakan dampak nyata dari cybercrime pada tahun 1997, ketika terjadi serangan cracking terhadap beberapa situs pemerintah. Serangan tersebut menjadi peringatan bahwa negara ini belum siap menghadapi ancaman kejahatan digital. Setelah melalui perdebatan panjang, pemerintah akhirnya mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang menjadi dasar hukum utama dalam menangani kejahatan siber di Indonesia.

UU ITE kemudian mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016, yang memperkuat beberapa aspek hukum pidana siber, terutama dalam hal pembuktian elektronik dan perlindungan data pribadi. Dengan adanya regulasi ini, Indonesia resmi mengakui kejahatan siber sebagai bentuk tindak pidana yang dapat dikenai sanksi hukum sebagaimana kejahatan konvensional lainnya.

Jenis-Jenis Tindak Pidana Cyber

Secara umum, cybercrime dapat diklasifikasikan ke dalam beberapa kategori berdasarkan objek dan motif kejahatannya. Berdasarkan Konvensi Kejahatan Siber Budapest tahun 2001, terdapat empat kategori utama, yaitu:

Tindak Pidana terhadap Kerahasiaan, Integritas, dan Ketersediaan Data serta Sistem Komputer

Kategori ini mencakup perbuatan seperti:

1. Akses ilegal (Unauthorized Access): perbuatan memasuki sistem komputer tanpa izin, yang termasuk di dalamnya hacking dan cracking.
2. Intersepsi ilegal (Illegal Interception): penyadapan atau pengambilan data dari jaringan komunikasi tanpa otorisasi.
3. Interferensi data (Data Interference): pengubahan, penghapusan, atau perusakan data elektronik secara tidak sah.
4. Interferensi sistem (System Interference): tindakan yang mengganggu atau merusak fungsi sistem komputer.
5. Penyalahgunaan perangkat (Misuse of Devices): pembuatan atau distribusi perangkat lunak berbahaya seperti virus, malware, atau trojan.

Tindak pidana dalam kategori ini sering kali ditujukan untuk merusak sistem, mencuri data, atau mengganggu aktivitas pihak lain, baik individu maupun institusi.

Tindak Pidana Terkait Komputer

Jenis ini meliputi tindakan kriminal yang menggunakan komputer sebagai sarana utama untuk melakukan kejahatan, seperti:

1. Pemalsuan menggunakan komputer (Computer-related Forgery), yaitu membuat data atau dokumen palsu dalam bentuk digital untuk tujuan menipu pihak lain.
2. Penipuan menggunakan komputer (Computer-related Fraud), yaitu menggunakan sistem elektronik untuk memperoleh keuntungan secara tidak sah, seperti kasus phishing, scam, atau online fraud.

Kedua tindak pidana ini banyak ditemukan dalam transaksi e-commerce, perbankan digital, dan platform media sosial.

Tindak Pidana yang Berkaitan dengan Konten

Kejahatan siber juga dapat terjadi dalam bentuk penyebaran konten terlarang atau merugikan pihak lain. Contohnya meliputi:

1. Penyebaran pornografi atau kekerasan melalui media digital.
2. Penyebaran ujaran kebencian (hate speech), fitnah, dan hoaks.
3. Konten yang mengandung pelanggaran hak cipta atau pencemaran nama baik.

Dalam konteks hukum Indonesia, banyak kasus pelanggaran konten digital ditangani dengan pasal 27 dan 28 UU ITE, yang mengatur tentang kesusilaan, pencemaran nama baik, serta penyebaran informasi yang menimbulkan kebencian berdasarkan SARA.

Tindak Pidana yang Berkaitan dengan Hak Kekayaan Intelektual dan Ekonomi Digital Jenis kejahatan ini meliputi pembajakan perangkat lunak, pencurian data pribadi, dan pelanggaran hak cipta digital. Selain itu, muncul pula bentuk kejahatan ekonomi siber seperti:

1. Carding, yaitu pencurian data kartu kredit untuk transaksi ilegal.
2. Spamming, yaitu pengiriman pesan berulang yang merugikan penerima.
3. Phishing, yaitu usaha mencuri informasi pribadi melalui situs atau email palsu.

Tindak pidana dalam kategori ini seringkali berdampak ekonomi besar karena dapat menimbulkan kerugian finansial baik bagi individu maupun perusahaan.

Bentuk Khusus Cybercrime

Selain kategori umum, terdapat pula bentuk- bentuk khusus dari kejahatan siber yang memiliki karakteristik dan dampak lebih serius, antara lain:

Cyber Terrorism

Cyber terrorism adalah penggunaan teknologi informasi untuk menimbulkan ketakutan, kerusakan, atau ancaman terhadap keamanan publik dan negara. Bentuknya bisa berupa serangan terhadap infrastruktur penting seperti sistem energi, transportasi, atau jaringan pemerintahan.

Menurut Lewis (2002), tujuan utama cyber terrorism adalah merusak stabilitas nasional dan menekan pemerintah atau masyarakat sipil. Jenis tindakannya mencakup hacking, cyber sabotage,

extortion, serta media hijacking. Dalam konteks global, serangan terhadap sistem pemerintahan Amerika Serikat atau jaringan energi di Eropa menjadi contoh nyata bahaya cyber terrorism.

Cyber EspionageCyber espionage atau spionase siber merupakan tindakan memata- matai dengan menggunakan jaringan internet untuk mencuri informasi penting atau rahasia dari pihak lain. Aktivitas ini dapat menyasar data militer, ekonomi, atau politik, dan sering kali melibatkan negara sebagai pelaku.

Menurut Susila & Salim (2024), spionase siber merupakan bentuk modern dari spionase tradisional yang bertujuan mengumpulkan data sensitif dari negara atau organisasi pesaing. Bentuk kejahatan ini menjadi ancaman serius terhadap kedaulatan dan keamanan nasional karena dapat mengungkap rahasia strategis suatu negara.

Penegakan Hukum terhadap Tindak Pidana Cyber di Indonesia

Penegakan hukum terhadap kejahatan siber di Indonesia diatur dalam UU ITE, KUHP, serta beberapa peraturan pelaksana lainnya seperti PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Namun, dalam praktiknya, masih terdapat beberapa kendala, di antaranya:

1. Kendala teknis, karena keterbatasan kemampuan aparat dalam melacak jejak digital pelaku yang menggunakan teknologi tinggi.
2. Kendala yurisdiksi, karena kejahatan siber sering melibatkan pelaku lintas negara.
3. Kendala pembuktian, karena alat bukti elektronik harus melalui proses verifikasi ilmiah agar dapat diterima di pengadilan.

Oleh sebab itu, prinsip due process of law harus diterapkan secara ketat dalam setiap proses penyidikan dan penuntutan perkara siber. Alat bukti elektronik harus diverifikasi keasliannya melalui proses forensik digital agar tidak terjadi manipulasi data atau pelanggaran hak privasi.

Upaya Pencegahan dan Kerja Sama Internasional

Dalam menghadapi kejahatan siber, pencegahan menjadi langkah utama selain penindakan. Upaya ini mencakup:

1. Peningkatan literasi digital masyarakat, agar pengguna internet memahami keamanan data pribadi.
2. Kerja sama lintas negara, melalui organisasi seperti Interpol Cybercrime Directorate dan Budapest Convention.
3. Penguatan lembaga siber nasional, seperti Badan Siber dan Sandi Negara (BSSN) di Indonesia, yang berperan menjaga keamanan siber nasional.
4. Pengembangan regulasi perlindungan data pribadi, sebagaimana diatur dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP).

Kerja sama internasional sangat penting karena kejahatan siber bersifat lintas batas. Melalui perjanjian dan koordinasi antarnegara, pelaku kejahatan yang berada di luar yurisdiksi nasional dapat lebih mudah dilacak dan ditindak. Tindak pidana cyber merupakan fenomena kejahatan modern yang muncul akibat perkembangan pesat teknologi informasi.Berbeda dengan kejahatan

konvensional, cybercrime memiliki karakteristik khusus seperti ruang lingkup global, modus yang canggih, serta kesulitan pembuktian. Oleh karena itu, sistem hukum nasional perlu terus menyesuaikan diri dengan perkembangan teknologi.

Indonesia telah memiliki dasar hukum melalui UU ITE dan berbagai regulasi turunannya. Namun, tantangan terbesar masih terletak pada penegakan hukum yang efektif, kemampuan teknis aparat, serta kesadaran masyarakat terhadap keamanan digital. Dengan sinergi antara regulasi, penegakan hukum, dan literasi digital, diharapkan Indonesia dapat menghadapi tantangan kejahatan siber secara komprehensif dan menjaga kedaulatan hukum di ruang digital.

Perlindungan Huku da Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia

Cybercrime dalam Konteks Hukum Positif di Indonesia. Kejahatan siber merupakan bentuk kejahatan modern yang berkembang seiring pesatnya kemajuan teknologi informasi dan komunikasi. Kejahatan ini memiliki keterkaitan erat dengan penggunaan komputer dan jaringan internet dalam pelaksanaannya. Tindak pidana siber dapat mengancam privasi, integritas, serta eksistensi data milik masyarakat maupun negara. Mengingat karakteristiknya yang berbeda dengan kejahatan konvensional, kejahatan siber menuntut perhatian khusus dari pemerintah dalam upaya pencegahan dan penanggulangannya.

Banyak kasus kejahatan siber terjadi dan menimbulkan kerugian besar bagi masyarakat. Salah satu penyebab utama adalah dinamika sosial yang belum diimbangi dengan pemahaman teknologi secara menyeluruh, serta tingginya ketergantungan masyarakat terhadap kemajuan teknologi digital. Dalam konteks hukum nasional, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)—yang terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024—menjadi dasar hukum utama yang mengatur berbagai aspek keamanan siber di Indonesia.

Ruang lingkup UU ITE mencakup keamanan informasi, perlindungan data pribadi, transaksi elektronik, serta pencegahan tindak pidana siber. Undang- undang ini juga mengatur penyebaran informasi yang dapat merugikan, menipu, atau melanggar norma kesusilaan. Melalui ketentuan tersebut, hukum memberikan batasan yang jelas mengenai tindakan- tindakan yang dapat dikategorikan sebagai tindak pidana dalam dunia maya, seperti penipuan daring (online fraud), pencurian identitas (identity theft), dan penyebaran konten ilegal.

UU ITE berfungsi sebagai pilar utama dalam membangun kerangka hukum keamanan siber nasional. Undang-undang ini berperan penting dalam mengatur transaksi elektronik, distribusi informasi digital, serta mekanisme perlindungan terhadap penyalahgunaan teknologi. UU ITE tidak hanya menitikberatkan pada aspek legalitas transaksi elektronik, tetapi juga mengatur tata cara penyebaran informasi di internet, perlindungan data pribadi warga negara, dan penetapan standar penanganan kejahatan siber yang semakin kompleks.

Secara garis besar, landasan hukum dalam menangani kejahatan siber di Indonesia berfokus pada UU ITE. Regulasi ini mengatur berbagai bentuk kegiatan dan transaksi elektronik, termasuk penyebaran konten ilegal, penipuan daring, pencurian data pribadi, serta tindakan peretasan (hacking). Dengan demikian, UU ITE menjadi instrumen hukum yang menargetkan seluruh jenis pelanggaran siber, mulai dari pelanggaran ringan hingga kejahatan berat yang mengancam

keamanan nasional.

Selain itu, hadir pula Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai respons terhadap meningkatnya kasus penyalahgunaan data pribadi dalam dunia digital. Undang-undang ini menegaskan bahwa perlindungan data pribadi merupakan bagian dari hak konstitusional warga negara yang wajib dijaga oleh negara. UU PDP memberikan dasar hukum yang kuat melalui pembentukan Lembaga Perlindungan Data Pribadi, pengaturan mekanisme pengawasan administratif, serta penerapan sanksi pidana yang tegas terhadap pelanggaran data.

Pelanggaran yang mencakup pengambilan, penyebaran, atau pemalsuan data pribadi tanpa izin diancam dengan hukuman pidana penjara dan/atau denda bernilai miliaran rupiah. Selain itu, pelaku juga dapat dijatuhi pidana tambahan berupa kewajiban ganti rugi kepada korban. UU PDP turut menegaskan tanggung jawab korporasi dalam menjaga keamanan data pribadi pengguna. Korporasi yang lalai dapat dikenai sanksi administratif berat seperti denda tinggi, pembekuan izin, bahkan pembubaran badan usaha.

UU PDP memiliki hubungan yang sinergis dengan UU ITE. Keduanya saling melengkapi dalam mengatur ranah hukum digital. Jika UU ITE berfokus pada aspek kriminalitas siber dan akses ilegal terhadap sistem elektronik, maka UU PDP memberikan perlindungan terhadap hak-hak subjek data dan mekanisme pengelolaannya, baik dalam bentuk elektronik maupun non- elektronik. Sinergi antara kedua undang- undang ini memperkuat sistem hukum pidana siber di Indonesia, khususnya dalam melindungi privasi individu, meningkatkan akuntabilitas penyelenggara sistem elektronik, serta memberikan kepastian hukum bagi masyarakat sebagai pengguna layanan digital.

Perkembangan teknologi informasi telah membawa perubahan besar dalam seluruh aspek kehidupan manusia. Di satu sisi, kemajuan teknologi memberikan berbagai manfaat, seperti kemudahan memperoleh informasi, peningkatan peluang kerja, partisipasi dalam kehidupan politik dan demokrasi, serta kemajuan ekonomi. Namun di sisi lain, kemajuan tersebut juga menghadirkan ancaman baru berupa kejahatan siber yang berdampak luas terhadap individu, lembaga, bahkan negara.

Kejahatan siber menjadi tantangan serius bagi pemerintah dan aparat penegak hukum karena memerlukan kemampuan teknis serta pemahaman hukum yang mendalam. Dampak negatif dari kejahatan ini tidak hanya dirasakan secara ekonomi, tetapi juga dapat mengganggu stabilitas sosial dan keamanan nasional. Salah satu penyebabnya adalah rendahnya tingkat literasi digital masyarakat serta lemahnya perlindungan dan sistem keamanan data pribadi yang belum sepenuhnya efektif.

Secara umum, kejahatan siber memiliki beberapa karakteristik yang membedakannya dari tindak pidana konvensional. Di antaranya adalah sifatnya yang tanpa batas wilayah (borderless), menggunakan teknologi canggih, sulit dilacak, serta dapat dilakukan secara anonim. Kejahatan ini sering melibatkan pelaku lintas negara dan menuntut kerja sama internasional dalam penegakan hukumnya. Oleh karena itu, penguatan sistem hukum nasional melalui UU ITE dan UU PDP merupakan langkah penting untuk memastikan bahwa Indonesia memiliki perlindungan hukum yang memadai dalam menghadapi era digital yang semakin kompleks.

Karakteristik Kejahatan Cyber

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.
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
5. (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi).
6. Pelaku adalah individu yang menguasai penggunaan internet dan
7. aplikasinya.
8. Kejahatan seringkali dilakukan secara transnasional atau melintasi batas negara.

Dalam konteks hukum positif Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya pada tahun 2016 menempati posisi yang sangat strategis dalam membangun sistem hukum nasional di era digital. Lahirnya UU ini merupakan respons atas perkembangan teknologi informasi dan komunikasi yang begitu pesat serta kebutuhan akan perlindungan hukum yang jelas di ruang siber. Dunia digital, yang kini menjadi bagian tak terpisahkan dari kehidupan manusia modern, menimbulkan berbagai potensi manfaat sekaligus risiko yang signifikan, terutama dalam aspek keamanan data, privasi individu, dan kejahatan berbasis teknologi.

Ruang lingkup UU ITE sangat luas karena tidak hanya mengatur tentang transaksi elektronik, tetapi juga mengenai keamanan informasi, perlindungan data pribadi, pencegahan kejahatan siber, serta larangan terhadap penyebaran konten yang bersifat merugikan, menipu, atau melanggar kesusilaan. Dengan kata lain, UU ITE menjadi dasar hukum utama bagi negara dalam menata kehidupan masyarakat di dunia maya agar selaras dengan prinsip hukum dan norma sosial yang berlaku. Undang-undang ini juga menunjukkan bahwa pemerintah Indonesia berupaya menyeimbangkan kemajuan teknologi dengan kepastian hukum dan perlindungan terhadap hak-hak masyarakat digital.

Seiring meningkatnya kasus cybercrime di Indonesia, pemerintah semakin menyadari urgensi pengaturan hukum yang tegas untuk menghadapi pelaku kejahatan di dunia maya. Cybercrime memiliki karakteristik unik karena dapat dilakukan kapan saja, di mana saja, dan bahkan lintas batas negara tanpa mengenal ruang dan waktu. Oleh sebab itu, UU ITE hadir untuk memberikan dasar hukum dalam menindak pelaku kejahatan digital dengan sanksi pidana yang tegas. Pemerintah berharap melalui pengaturan ini, tindak kejahatan di dunia siber dapat diminimalisasi, dikendalikan, bahkan dicegah sedini mungkin.

Lebih lanjut, ketentuan-ketentuan yang mengatur tentang kejahatan siber dalam UU ITE dapat ditemukan dalam sejumlah pasal penting.

1. Pasal 29 UU ITE mengatur mengenai ancaman kekerasan atau tindakan menakut-nakuti yang dilakukan melalui media elektronik. Misalnya, seseorang yang mengirimkan pesan berisi

ancaman kekerasan secara daring dapat dijerat dengan ketentuan ini.

2. Pasal 34 UU ITE berfokus pada tindakan kriminal berupa memproduksi, menjual, mendistribusikan, mengimpor, atau memiliki perangkat lunak maupun perangkat keras yang digunakan untuk melakukan kejahatan siber.
3. Pasal 30 juncto Pasal 46 UU ITE mengatur tentang akses ilegal dan pencurian data, termasuk praktik carding, yakni pencurian data kartu kredit milik orang lain untuk transaksi online.
4. Pasal 34 ayat (1) juncto Pasal 50 menjelaskan keterlibatan pihak lain atau kerja sama dalam melakukan carding.
5. Pasal 35 juncto Pasal 51 ayat (1) dan Pasal 32 juncto Pasal 48 menegaskan tentang penipuan digital dan penggunaan data pribadi tanpa hak.

Selain itu, ketentuan dalam KUHP Pasal 362, 363, dan 378 mengenai pencurian dan penipuan juga dapat diterapkan pada kasus kejahatan siber karena memiliki unsur delik yang serupa.

Kejahatan siber menuntut penanganan yang lebih komprehensif dan lintas sektoral, sebab pelaku dapat beroperasi dari wilayah atau bahkan negara lain. Hal ini menjadi tantangan besar bagi aparat penegak hukum karena memerlukan kemampuan teknis, kerja sama internasional, serta sistem digital yang kuat untuk melacak dan menindak pelaku. Sayangnya, masih banyak masyarakat Indonesia yang memiliki ketergantungan tinggi terhadap teknologi tanpa diimbangi dengan pemahaman mendalam mengenai keamanan digital. Kurangnya kesadaran tersebut membuat masyarakat mudah menjadi korban—mulai dari penipuan online, pencurian data pribadi, hingga penyalahgunaan informasi untuk tujuan kriminal.

Kondisi ini memperlihatkan bahwa tantangan terbesar dalam menghadapi cybercrime tidak hanya terletak pada aspek penegakan hukum, tetapi juga pada pembentukan kesadaran digital masyarakat. Literasi digital yang rendah menjadikan pengguna internet di Indonesia sering kali abai terhadap pentingnya keamanan siber, seperti penggunaan kata sandi yang lemah, membagikan informasi pribadi sembarangan, atau mengklik tautan berbahaya. Akibatnya, kejahatan siber semakin mudah terjadi dan menimbulkan kerugian yang luas, baik secara ekonomi maupun psikologis.

Berdasarkan analisis terhadap berbagai regulasi tersebut, dapat disimpulkan bahwa perlindungan hukum di dunia digital Indonesia masih bersifat parsial dan belum terintegrasi secara maksimal. Artinya, meskipun sudah terdapat berbagai undang- undang seperti UU ITE dan Undang-Undang Perlindungan Data Pribadi (UU PDP), koordinasi antarinstansi dan penerapan hukumnya masih belum optimal. Kondisi ini menuntut pembenahan dari segi kebijakan, sumber daya manusia, dan infrastruktur teknologi. Pemerintah perlu memperkuat lembaga-lembaga yang berwenang menangani keamanan siber serta membangun kerja sama dengan pihak swasta dan komunitas digital untuk meningkatkan efektivitas perlindungan.

Selain itu, Indonesia juga perlu memiliki fasilitas dan sistem pengamanan siber nasional yang lebih kuat dan modern. Pembangunan infrastruktur keamanan digital seperti pusat data nasional, sistem deteksi dini serangan siber, serta mekanisme penanggulangan darurat menjadi hal yang mendesak. Investasi negara dalam pengembangan teknologi keamanan siber, riset, serta pelatihan tenaga ahli di bidang digital sangat diperlukan untuk menghadapi ancaman kejahatan siber

yang semakin canggih dan kompleks.

Dengan demikian, penegakan hukum terhadap cybercrime tidak hanya bergantung pada regulasi semata, tetapi juga pada sinergi antara kebijakan pemerintah, kesadaran masyarakat, dan kesiapan teknologi nasional. Jika seluruh unsur tersebut dapat berjalan selaras, Indonesia akan mampu membangun ruang siber yang aman, beretika, dan berkeadilan, sekaligus memperkuat kedaulatan digital di tengah arus globalisasi teknologi.

KESIMPULAN

Kejahatan siber merupakan tantangan besar di era digital yang menuntut perhatian serius dari pemerintah, masyarakat, dan aparat penegak hukum. Melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Indonesia telah memiliki dasar hukum untuk menanggulangi tindak pidana siber. Namun, penerapan kedua regulasi tersebut masih menghadapi kendala dalam penegakan, pemahaman masyarakat, serta kesiapan infrastruktur teknologi. Oleh karena itu, diperlukan sinergi dan pembaruan sistem hukum yang lebih adaptif terhadap perkembangan teknologi agar perlindungan hukum di dunia digital dapat berjalan secara efektif dan berkeadilan.

Saran

1. Pemerintah perlu memperkuat koordinasi antar lembaga dalam penegakan hukum siber serta meningkatkan kapasitas aparat melalui pelatihan di bidang teknologi informasi.
2. Masyarakat perlu meningkatkan literasi digital agar lebih waspada terhadap ancaman kejahatan siber dan menjaga keamanan data pribadi.
3. Diperlukan pembaruan regulasi dan infrastruktur keamanan siber nasional yang lebih modern dan responsif terhadap bentuk-bentuk kejahatan baru di ruang digital.

DAFTAR PUSTAKA

(Times New Roman 12, Reguler, spasi 1, spacing before 6 pt, after 6 pt).

Aldriano, & Priyambodo, P. (2022). *Kejahatan Siber dan Tantangan Penegakan Hukumnya di Indonesia.* Jakarta: Mitra Wacana Media.

Arief, B. N. (2006). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan.* Jakarta: Kencana Prenada Media Group

Kitab Undang-Undang Hukum Pidana (KUHP).

Konvensi Kejahatan Siber (Budapest Convention on Cybercrime). (2001). Council of Europe, Budapest..

Mansur, D., & Gultom, E. (2005). Cyber Law: *Aspek Hukum Teknologi Informasi.* Bandung: Refika Aditama.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 2).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 190).