MAQASIDI
Vol. 4, No. 1 (2024), p 40-55
DOI: 10.47498/maqasidi.v4i1.2966
ISSN: p-2798-981X, e-2798-9801

# Tinjaun Yuridis Penegakkan Hukum Kejahatan *Cyber Crime* Studi Implementasi Undang-Undang Nomor 11 Tahun 2008

**Budi Handoyo[1], Husamuddin MZ[2], Ida Rahmah[3], Asy'ari[4]**
[1,2,3,4]STAIN Teungku Dirundeng Meulaboh, Indonesia
E-mail korespondens: budihandoyo@staindirundeng.ac.id

**Abstrak**

Penegakan hukum terhadap kejahatan *cyber crime* merupakan tantangan yang kompleks dalam konteks perkembangan teknologi informasi dan transaksi elektronik. Studi ini bertujuan untuk memberikan tinjauan yuridis serta menganalisis implementasi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam penegakan hukum terhadap kejahatan *cyber crime*. Metode penelitian yang digunakan adalah analisis dokumen dan studi pustaka untuk mengumpulkan data tentang peraturan hukum yang berkaitan dengan kejahatan *cyber crime* serta studi implementasi Undang-Undang Nomor 11 Tahun 2008. Hasil analisis menunjukkan bahwa kejahatan *cyber crime*, termasuk tindak pidana yang kompleks, memunculkan berbagai tantangan dalam penegakan hukum. Meskipun demikian, Undang-Undang Nomor 11 Tahun 2008 memberikan landasan hukum yang penting untuk menangani kejahatan tersebut. Penegakan hukum *cyber crime* juga memerlukan kerjasama erat antara pihak kepolisian dan penyedia layanan internet (ISP) serta kesadaran hukum masyarakat. Kesimpulannya, penegakan hukum terhadap kejahatan *cyber crime* memerlukan pendekatan yang holistik dan terpadu, dengan penguatan peraturan hukum yang relevan dan upaya preventif yang efektif. Implementasi Undang-Undang Nomor 11 Tahun 2008 menjadi landasan yang penting dalam membangun kerangka kerja untuk penegakan hukum yang lebih efektif terhadap kejahatan *cyber crime*.

**Kata kunci:** Hukum, Kejahatan, Cyber crime, Undang-Undang

## Pendahuluan

Hukum dan perkembangan teknologi informasi merupakan dua hal yang tak terpisahkan. Kemajuan dalam peradaban, ilmu pengetahuan, dan teknologi memengaruhi berbagai aspek kehidupan manusia (Hamdi et al., 2013). Begitu juga, hukum perlu bisa mengikuti perkembangan zaman. Kemunculan dunia digital adalah salah satu aspek dari kemajuan ilmu pengetahuan dan teknologi.

Indonesia saat ini secara aktif terlibat dalam penggunaan dan pemanfaatan teknologi informasi, yang dibuktikan dengan tingginya adopsi internet (Rizki, 2022). Penggunaan siber ini terutama populer dalam gaya hidup dan hiburan, seperti mengakses media sosial, mengunduh musik, menonton film, mencari informasi tentang hobi atau hiburan, membaca cerita, serta mengakses berita olahraga. Selain itu, bermain game pada berbagai perangkat elektronik juga merupakan bagian dari pemanfaatan siber.

Pemanfaatan siber juga melibatkan penggunaan sebagai mesin pencari, jejaring sosial, konektivitas smartphone dan internet mobile, serta mengikuti perkembangan industri komputasi awan sebagai media penyimpanan data (Aksenta et al., 2023). Pertumbuhan teknologi informasi dan komunikasi yang cepat telah mengubah cara masyarakat berperilaku secara global, serta menghasilkan perubahan sosial yang mencolok dengan kecepatan yang tinggi (Saputra, 2016). Meskipun pemanfaatan teknologi ini memiliki banyak manfaat positif, perlu diperhatikan juga dampak negatif yang mungkin timbul.

Penggunaan teknologi tanpa pengawasan yang memadai dapat dimanfaatkan untuk kegiatan merugikan pihak lain. Munculnya hukum siber atau hukum telematika mencerminkan respons terhadap perkembangan ini (Sugeng, 2024). Hukum siber mencakup semua aspek hukum yang berkaitan dengan penggunaan teknologi informasi dan komunikasi, sementara hukum telematika muncul dari perpaduan hukum telekomunikasi, hukum media, dan hukum informatika.

Isu-isu hukum yang kerap timbul terkait dengan pengiriman informasi, komunikasi, dan/atau transaksi elektronik. Penggunaan komputer telah menjadi umum dalam berbagai aktivitas manusia, namun perlu diwaspadai kemungkinan dampak negatifnya akibat kelalaian, ketidakmampuan, atau niat jahat. Perkembangan teknologi informasi memerlukan penyesuaian hukum lebih lanjut untuk memastikan penggunaan teknologi dalam batas hukum.

Munculnya berbagai tindak pidana baru, termasuk *Cyber crime*, merupakan tantangan bagi hukum dalam menghadapi perubahan sosial (Efendi & Hadana, 2022). Penggunaan teknologi sebagai sarana komunikasi global menawarkan peluang positif bagi kemajuan ilmu pengetahuan, namun juga menimbulkan tantangan ketika tidak diimbangi dengan kemampuan mengoperasikan teknologi dan pengaturan hukum yang memadai.

**Metode Penelitian**

Metode penelitian kepustakaan dalam tinjauan yuridis terhadap penegakan hukum kejahatan *cyber crime* dengan studi implementasi Undang-Undang Nomor 11 Tahun 2008 melibatkan analisis literatur dan dokumen yang relevan dengan topik tersebut. Pertama, peneliti akan mengumpulkan berbagai sumber referensi, seperti buku, jurnal ilmiah, laporan riset, dan dokumen hukum terkait Undang-Undang ITE serta kasus-kasus *cyber crime* yang telah diputuskan oleh pengadilan.

Kedua, peneliti akan melakukan evaluasi mendalam terhadap literatur yang telah dikumpulkan untuk memahami konsep-konsep hukum yang mendasari penegakan hukum terhadap kejahatan *cyber crime*. Ini meliputi analisis terhadap ketentuan-ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 serta interpretasi dan aplikasinya dalam kasus-kasus nyata.

Langkah selanjutnya adalah melakukan sintesis dan interpretasi terhadap temuan-temuan dari literatur yang telah dievaluasi. Peneliti akan menyusun dan

menganalisis argumen-argumen yang disajikan dalam literatur tersebut, serta mencari pola atau tren dalam implementasi Undang-Undang ITE dalam penegakan hukum terhadap kejahatan *cyber crime*.

Dengan menggunakan metode penelitian kepustakaan ini, diharapkan peneliti dapat memberikan pemahaman yang lebih mendalam mengenai efektivitas Undang-Undang Nomor 11 Tahun 2008 dalam penegakan hukum terhadap kejahatan *cyber crime*, serta menyajikan pemikiran-pemikiran baru atau rekomendasi untuk meningkatkan penegakan hukum di bidang tersebut berdasarkan tinjauan yuridis yang komprehensif.

**Pembahasan/hasil**

**A. Tindak Pidana Elektronik (*Cyber crime*)**

Adami Ghazawi menjelaskan bahwa dalam perundang-undangan pidana Indonesia, istilah "tindak pidana" secara umum digunakan. Moeljatno juga menganggap istilah "tindak pidana" dapat sinonim dengan "perbuatan pidana" (Chazawi, 2002). Menurut Moeljatno, tindak pidana adalah suatu tindakan yang dilarang oleh hukum dan diancam dengan hukuman, yang melibatkan larangan yang ditujukan kepada pelakunya, dan terdapat hubungan yang erat antara larangan tersebut dan ancaman hukuman (Moeljatno, 1983).

Asal-usul istilah "cyber" dapat ditelusuri kembali ke "cybernetics", sebuah disiplin yang menggabungkan robotika, matematika, teknik listrik, dan psikologi, yang dikembangkan pada tahun 1948 oleh Nobert Wiener (Prabowo et al., 2023). Dalam konteks perkembangan teknologi informasi, telekomunikasi, dan multimedia, istilah "cyber crime" mengacu pada kejahatan yang terjadi di ruang maya (cyber space). Cyber space dianggap sebagai lingkungan komunikasi yang berasal dari komputer, yang kita kenal sebagai internet dalam kehidupan sehari-hari. (Habibi & Liviani, 2020).

Kemajuan teknologi komputer dan internet membawa manfaat besar dalam berbagai sektor kehidupan manusia, termasuk dalam keperluan rumah tangga. Meskipun membuka cakrawala baru dalam komunikasi dan pertukaran informasi, kemajuan ini juga membawa konsekuensi negatif, di antaranya adalah peningkatan kejahatan *cyber crime* (Ma'nunah, 2018).

Internet, yang juga dikenal sebagai cyber space, telah mengubah konsepsi tentang batasan jarak dan waktu dalam cara kerjanya. Namun, kemudahan yang ditawarkan oleh teknologi informasi ini juga memungkinkan para penjahat untuk melakukan kejahatan dengan lebih mudah (Maskun, 2022). *Cyber crime* atau kejahatan komputer menjadi fenomena yang berkembang dengan adanya teknologi ini. Kejahatan *cyber crime* merupakan bentuk kejahatan yang tidak terbatas oleh batasan wilayah atau waktu. Menurut Abdul Manan, kejahatan ini dapat dilakukan dengan menggunakan komputer atau internet, tanpa harus melakukan penetrasi terhadap

sistem (Manan, 2013). Maskun menjelaskan bahwa kejahatan *cyber crime* tidak hanya melibatkan teknologi komputer, tetapi juga teknologi telekomunikasi dalam pelaksanaannya (Maskun, 2022).

Kejahatan *cyber crime* dianggap sebagai kejahatan luar biasa yang serius dan dapat mengancam kehidupan masyarakat, bangsa, dan negara. Dengan perkembangan teknologi informasi yang tanpa batas, kejahatan ini telah menimbulkan dampak buruk yang dapat merugikan individu, lembaga, dan negara lainnya. Diperlukan kerja sama internasional, baik dalam bentuk perjanjian bantuan timbal balik maupun perjanjian ekstradisi, untuk mengatasi masalah kejahatan *cyber crime* ini, sesuai dengan konvensi Palermo dan deklarasi ASEAN (Bahri, 2020).

## B. Bentuk Kejahatan yang ditimbulkan dari Perkembangan Informasi dan Teknologi Elektronik

Menurut Pasal 1 ayat (1) dari Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Informasi Elektronik dijelaskan sebagai data elektronik tunggal atau kelompok, yang mencakup namun tidak terbatas pada teks, suara, gambar, peta, desain, foto, Electronic Data Interchange (EDI), surel (email), telegram, teks telepon, faksimili, atau format sejenis lainnya, serta karakter, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diproses agar dapat dipahami oleh individu yang memiliki kemampuan untuk memahaminya. Di sisi lain, Pasal 1 ayat (3) dari undang-undang yang sama menjelaskan Teknologi Informasi sebagai metode yang digunakan untuk mengumpulkan, mengatur, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

Manusia menggunakan media komputer dan internet sebagai alat atau sarana untuk memanfaatkan Informasi Elektronik dan Teknologi Informasi. Menurut Maskun, internet adalah suatu jaringan yang menghubungkan komputer-komputer satu sama lain melalui serangkaian perangkat atau komputer yang dikenal sebagai router, yang mengintegrasikan berbagai jaringan menjadi satu entitas besar. Bagian-bagian dari internet ini dapat mencakup berbagai jenis jaringan lokal (LAN), komputer mini, mainframe, superkomputer, bahkan hanya sebuah komputer personal (PC). Pada masa kini, beragam aplikasi dapat dijalankan melalui internet, seperti Telnet atau Remote Login, FTP (File Transfer Protocol), email, berita, Gopher, Wais, dan juga WWW (World Wide Web) (Maskun, 2022).

Walaupun kemajuan Teknologi Informasi dan Elektronik melalui internet memberikan dampak yang menguntungkan bagi kesejahteraan manusia, namun juga menimbulkan konsekuensi negatif yang signifikan dengan munculnya berbagai jenis kejahatan yang memanfaatkan teknologi canggih (Rivai et al., 2022). Selanjutnya, kejahatan yang terkait dengan penggunaan teknologi berbasis komputer dan jaringan telekomunikasi dapat diklasifikasikan ke dalam berbagai bentuk sesuai dengan cara operasinya (Saragih & Azis, 2020).

1. *Unauthorized Access to Computer System and Service*

   Kejahatan yang terjadi melalui penetrasi atau masuk secara tidak sah ke dalam suatu jaringan komputer tanpa izin atau pengetahuan dari pemiliknya merupakan peristiwa yang umum terjadi. Umumnya dilakukan oleh pelaku yang dikenal sebagai hacker, yang melakukan tindakan tersebut dengan maksud untuk sabotase atau mencuri informasi penting dan rahasia. Namun, ada juga yang melakukannya semata-mata untuk menguji kemampuan mereka dalam menembus sistem yang memiliki tingkat proteksi tinggi. Fenomena semacam ini semakin sering terjadi seiring dengan perkembangan teknologi Internet dan intranet.
2. *Illegal Contens*

   Kejahatan yang terlibat dalam menyebarkan informasi yang tidak benar, tidak etis, dan memiliki potensi untuk melanggar hukum atau mengganggu ketertiban umum, merupakan praktik yang umum terjadi di dunia maya. Contoh dari kejahatan semacam ini termasuk penyebaran berita palsu atau fitnah yang bertujuan merusak reputasi atau harga diri seseorang, materi yang terkait dengan pornografi, atau pengungkapan informasi rahasia negara. Selain itu, kejahatan ini juga mencakup agitasi dan propaganda yang bertujuan untuk menggulingkan pemerintahan yang sah dan tindakan serupa.
3. *Data Forgery*

   Manipulasi data pada dokumen-dokumen penting yang disimpan secara digital melalui Internet merupakan tindakan kriminal yang dikenal sebagai *Data Forgery*. Biasanya, kejahatan ini terjadi pada dokumen-dokumen e-commerce dengan menciptakan kesan "kesalahan pengetikan" yang pada akhirnya menguntungkan pelaku. Hal ini karena korban mungkin akan diminta memasukkan data pribadi dan nomor kartu kredit yang dapat disalahgunakan.
4. *Cyber Espionage*

   Cyber Espionage adalah tindakan kriminal yang memanfaatkan Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan cara meretas atau memasuki sistem jaringan komputer target. Kejahatan ini sering kali ditujukan kepada pesaing bisnis yang menyimpan dokumen atau data penting, seperti basis data, dalam sistem yang terhubung dalam jaringan komputer.
5. *Cyber Sabotage and Extortion*

   Cyber Sabotage and Extortion merujuk pada tindakan yang melibatkan gangguan, kerusakan, atau penghancuran terhadap data, program komputer, atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya, kejahatan ini dilakukan dengan menyisipkan logic bomb, virus komputer, atau program khusus lainnya untuk menyebabkan data, program komputer, atau sistem jaringan komputer menjadi tidak dapat digunakan, tidak beroperasi dengan benar, atau beroperasi sesuai keinginan pelaku.

6. *Infringements of Privacy*

   Pelanggaran Privasi adalah kejahatan yang sering kali bertujuan untuk mendapatkan informasi pribadi seseorang yang tersimpan dalam formulir data pribadi yang diolah secara komputer. Jika informasi tersebut diketahui oleh pihak lain, dapat menyebabkan kerugian bagi korban baik secara materiil maupun imateriil. Contoh informasi tersebut meliputi nomor kartu kredit, nomor PIN ATM, kondisi cacat atau penyakit yang dirahasiakan, dan lain sebagainya.

Teguh Sulistia, mengemukakan bentuk-bentuk kejahatan *cyber crime*, yang dikutip dari *Network Computer Information Services* (NCIS) diantaranya meliputi (Sulistia & Zurnetti , 2012):

1. *Recreational Hackers,*

   Recreational Hackers, atau sering disebut sebagai hacker rekreasi, adalah mereka yang melakukan kegiatan iseng-iseng di internet, khususnya oleh pengguna yang masih pemula, dengan maksud untuk menguji kelemahan sistem keamanan atau data dari sebuah perusahaan. Meskipun kegiatan iseng-iseng ini bertujuan hanya untuk hiburan semata, namun bisa berdampak pada kejahatan cyber yang merugikan orang lain secara langsung atau tidak langsung.
2. *Crackers atau Minded Hackers*

   *Crackers* atau *Minded Hackers* adalah mereka yang biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, melakukan sabotase, atau menghancurkan data dari pihak korban.
3. *Political Hackers*

   Political Hackers, atau biasa disebut sebagai aktivis atau *hactivist* politik, terlibat dalam kegiatan politis di mana mereka merusak ratusan situs web untuk memajukan agenda politik tertentu. Mereka menggunakan internet sebagai alat untuk menyebarkan pesan yang mencemarkan nama baik lawan politik mereka.
4. *Denial of Service Attack*

   Serangan Denial of Service (DoS), bertujuan untuk mengganggu sistem dengan menghalangi akses pengguna internet yang sah. Taktik yang digunakan adalah dengan mengirim atau membanjiri situs web dengan "data sampah" yang tidak bermanfaat bagi pengguna yang dituju. Dampaknya adalah pemilik situs web mengalami kerugian, karena memulihkan dan mengendalikan kembali situs web tersebut memerlukan waktu dan upaya yang besar.
5. *insiders (intertenal) Hackers*

   Insiders (internal) Hackers, merupakan tindakan yang dilakukan oleh individu yang bekerja di dalam perusahaan. Biasanya, hal ini dilakukan oleh karyawan yang merasa tidak puas atau memiliki konflik dengan pimpinan perusahaan, yang kemudian merusak data atau menghalangi akses data dalam proses bisnis perusahaan.

6. *Viruses*

   Virus adalah program perangkat lunak berbahaya yang menyebar dengan cara menyematkan dirinya dalam aplikasi internet, dan dapat menular ketika diakses oleh pengguna. Sebelum ditemukannya internet, penyebaran virus oleh peretas hanya bisa dilakukan melalui floppy disk. Namun, dengan kemajuan internet saat ini, virus dapat disembunyikan dalam file atau diunduh oleh pengguna, bahkan dapat menyebar melalui email.

7. *Piracy*

   Pembajakan perangkat lunak atau software komputer merupakan tren yang sedang terjadi saat ini, karena dianggap lebih mudah dan menguntungkan bagi para pembajak. Produsen perangkat lunak yang membuat produk asli seperti permainan, film, dan lagu dapat mengalami kerugian besar karena karya mereka dibajak melalui unduhan dari internet dan disalin dalam bentuk CD-ROM tanpa izin.

8. *Cyber Porngraphy atau Paedophilia*

   Kejahatan dalam bentuk pornografi yang muncul akibat perkembangan dunia maya memiliki dampak negatif yang serius, karena dapat melanggar nilai-nilai etika, moral, dan estetika. Dengan memanfaatkan pembukaan news group, ruang obrolan (chat rooms), dan WWW, penyebaran pornografi dapat membahayakan serta merusak moral, pikiran, dan kesehatan mental individu, terutama anak-anak di bawah umur.

9. *Cyber Stalking*

   Ini adalah jenis pesan email yang tidak diinginkan oleh pengguna dan sering kali masuk ke folder sampah, bahkan terkadang dengan cara yang memaksa. Meskipun email sampah ini tidak diinginkan oleh pengguna dan sering kali berisi surat kaleng yang dikirim secara paksa dengan menggunakan detail pribadi dari korban, namun pesan-pesan spam ini sangat mengganggu dan membuang-buang waktu pengguna untuk membersihkan kotak masuk komputer dari pesan-pesan tidak diundang ini.

10. *Hate Sites*

    Hate Sites, atau situs-situs kebencian, seringkali menjadi target dari serangan sensor dan menjadi platform untuk menyampaikan komentar-komentar yang kasar dan vulgar. Situs-situs ini dikelola oleh kelompok-kelompok ekstremis yang menggunakan mereka untuk menyerang pihak-pihak yang tidak disukai mereka.

11. *Carding*

    Ini adalah tindak kejahatan yang dilakukan dengan menggunakan kartu kredit ATM secara ilegal (Mardani, 2009).

Berdasarkan jenis-jenis kejahatan *cyber crime* di atas dan cara operasinya. Hacking adalah induk dari bentuk kejahatan ini yang dapat menghasilkan berbagai bentuk kejahatan siber lainnya. Dalam konteks ini, Maskun menjelaskan bahwa

Hacking, yang dilakukan oleh seorang hacker, adalah suatu keterampilan dalam meretas sistem komputer untuk memahami bagaimana sistem tersebut bekerja. Hacking dianggap ilegal karena melibatkan akses dan pembacaan data seseorang tanpa izin secara diam-diam, yang sama halnya dengan menyinggung perasaan orang atau menipu, karena itu para hacker/phreaker selalu berusaha untuk menyamarkan atau menyembunyikan identitas mereka (Maskun, 2013).

Kejahatan-kejahatan tersebut mewakili aspek negatif dari kemajuan teknologi informasi yang memanfaatkan kecanggihan internet dan dapat merugikan kepentingan negara-negara berdaulat.

**C. Peranan Hukum Pidana dalam Penanggulangan Cyber-Crime**

Hukum memiliki tujuan untuk mengakomodasi berbagai aktivitas masyarakat yang terus berubah sesuai dengan perkembangan zaman (Ali & Haryani, 2012). Menurut Sudarto, tujuan hukum secara umum adalah mencapai kesejahteraan masyarakat baik secara materiil maupun spiritual, sehingga perbuatan yang merugikan masyarakat tidak diinginkan (Sudarto, 2007). Kejahatan *cyber crime* termasuk kejahatan yang dapat menimbulkan kerugian bagi masyarakat, baik secara materiil maupun spiritual.

Para pelaku kejahatan cyber crime seringkali sulit ditangkap karena batasan yurisdiksi hukum dan pengadilan di Indonesia. Hal ini dikarenakan kejahatan tersebut sering melibatkan pelaku dari negara-negara lain, namun memiliki dampak hukum di Indonesia. Dalam konteks hukum internasional, ada tiga jenis yurisdiksi yang penting: yurisdiksi untuk membuat undang-undang, menegakkan hukum, dan memberikan putusan (Maskun et al., 2020).

Beberapa negara di Asia sudah lebih maju daripada Indonesia dalam membentuk undang-undang terkait teknologi informasi, seperti The Computer Crime Act of 1997 (Malaysia), The Computer Misuse Act of 1998 (Singapura), dan The Information Technology Act of 1999 (India). Negara-negara tersebut memiliki kebijakan pidana yang jelas dan tegas dalam menangani kejahatan *cyber crime* sebagai bagian dari politik kriminal (Sulistia & Zurnetti, 2012).

Barda Nawawi Arief mengemukakan bahwa politik kriminal merupakan upaya untuk membentuk peraturan yang sesuai dengan kondisi dan situasi terkini, serta kebijakan negara dalam menetapkan regulasi yang mencerminkan nilai-nilai masyarakat dan mencapai tujuan yang diinginkan. Di sisi lain, politik hukum pidana bertujuan untuk merancang undang-undang pidana yang sesuai dengan kondisi pada masa tertentu dan untuk kepentingan masa depan (Arief, 2011). Petrus Reinhard Golose menyampaikan bahwa undang-undang yang diinginkan seharusnya mampu menyesuaikan diri dengan kemajuan teknologi dan mampu mengantisipasi masalah yang timbul, termasuk dampak negatif dari

penyalahgunaan Internet yang berpotensi merugikan korban baik secara materiil maupun non-materiil (Maulana, 2023).

Peraturan hukum Indonesia telah mengatur beberapa ketentuan tentang tindak pidana yang terkait dengan kejahatan *cyber crime* dalam berbagai pasal perundang-undangan yang terpisah (Ali & Haryani, 2014).

1. Kitab Undang Undang Hukum Pidana

   Kitab Undang-Undang Hukum Pidana (KUHP) pada dasarnya belum sepenuhnya efektif dalam menangani pelaku kejahatan *cyber crime*, karena unsur-unsur materiil kejahatan dunia maya belum secara menyeluruh tercakup dalam KUHP. Dalam konteks pembuktian, KUHP mengikuti asas legalitas, seperti yang dijelaskan dalam Pasal 1 ayat (1) KUHP, yang menyatakan bahwa suatu perbuatan tidak dapat dianggap pidana jika tidak diatur dalam undang-undang. Hal ini berarti bahwa pelaku kejahatan *cyber crime* tidak selalu dapat dihukum secara pidana. Namun, Pasal 10 angka (1) Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman menegaskan bahwa pengadilan tidak boleh menolak untuk memeriksa atau mengadili suatu perkara dengan alasan ketidakjelasan hukum, melainkan wajib untuk melakukan pemeriksaan dan pengadilan. Oleh karena itu, tugas hakim adalah untuk berijtihad, yaitu menemukan hukum yang relevan dalam menangani kasus tersebut.

   Dalam konteks ini, dunia hukum telah mengadopsi praktik memperluas penafsiran asas dan norma hukum ketika menghadapi kejahatan yang tidak berwujud, seperti kasus pencurian listrik sebagai contoh kejahatan benda. Kejahatan *cyber crime* pada dasarnya dapat dijerat berdasarkan KUHP karena pada dasarnya kejahatan *cyber crime* sama dengan kejahatan dunia nyata. Penyidik dan hakim dalam menangani kasus-kasus ini sering menggunakan analogi atau perumpamaan terhadap pasal-pasal yang ada dalam KUHP. Biasanya, beberapa pasal dalam KUHP digunakan secara bersamaan karena melibatkan beberapa tindakan, seperti yang dapat diterapkan dalam kasus *cyber crime*, antara lain:

   1) Pasal 362 KUHP yang digunakan dalam kasus carding mengacu pada tindakan di mana pelaku mencuri nomor kartu kredit orang lain, meskipun tidak secara fisik, hanya dengan mengambil nomor kartu menggunakan perangkat lunak pembuat kartu (card generator) yang tersedia di internet untuk melakukan transaksi di platform e-commerce. Setelah transaksi berhasil dilakukan dan barang dikirim, penjual yang hendak menarik uangnya di bank menemui penolakan karena pemilik kartu sebenarnya bukanlah pelaku transaksi tersebut.
   2) Pasal 378 KUHP bisa dipakai dalam kasus penipuan di mana seseorang menawarkan dan menjual produk atau barang dengan menempatkan iklan di salah satu situs web, menarik minat orang untuk membelinya, dan menerima pembayaran. Namun, pada kenyataannya, barang yang dijanjikan tidak ada.

Kebenaran ini terungkap setelah pembeli mengirimkan uang dan barang yang dipesan tidak pernah sampai, sehingga pembeli menjadi korban penipuan.

3) Pasal 311 KUHP bisa dijadikan dasar dalam kasus pencemaran nama baik yang melibatkan penggunaan media Internet. Cara kerjanya adalah pelaku menyebar email kepada kontak korban dengan cerita palsu atau mengirimkan email ke daftar email tertentu sehingga banyak orang menjadi tahu tentang cerita tersebut.
4) Pasal 303 KUHP dapat digunakan untuk menindak perjudian daring yang dijalankan melalui internet dengan penyelenggara yang beroperasi dari wilayah Indonesia.
5) Pasal 282 KUHP dapat digunakan untuk menangani penyebaran pornografi atau situs web porno yang tersebar luas dan mudah diakses melalui internet. Meskipun kontennya berbahasa Indonesia, menindak pelakunya menjadi sulit karena mereka mendaftarkan domain di luar negeri, di mana pornografi yang melibatkan orang dewasa bukanlah kegiatan yang melanggar hukum.
6) Kasus penyebaran foto atau film pribadi seseorang yang bersifat vulgar di internet bisa ditangani dengan Pasal 282 dan 311 KUHP.
7) Pasal 406 KUHP bisa digunakan dalam kasus deface atau hacking yang mengakibatkan sistem milik orang lain, seperti situs web atau program, menjadi tidak berfungsi atau tidak dapat digunakan sebagaimana semestinya.

Dengan demikian, Pasal-Pasal dalam KUHP masih dapat digunakan tanpa perlu adanya regulasi baru untuk menangani kejahatan melalui internet (*cyber crime*), sehingga tidak terjadi kekosongan hukum. Dalam hal ini, hakim seharusnya menggunakan interpretasi yang luas dari pasal-pasal KUHP yang relevan dengan kejahatan *cyber crime* tanpa menyebutkan secara spesifik. Mereka hanya menerapkan aturan hukum yang ada dengan interpretasi yang sesuai. Selain itu, penting bagi hakim untuk memperhatikan Pasal 5 angka (1) Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman. Pasal tersebut menegaskan bahwa hakim memiliki kewajiban untuk memahami nilai-nilai hukum dan rasa keadilan yang berlaku dalam masyarakat.

2. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Aturan yang terdapat dalam KUHP tidak selalu mencukupi untuk menindak tindak pidana cyber crime karena unsur-unsur kejahatan di dunia maya seringkali tidak terpenuhi dalam KUHP. Dalam proses pembuktian, KUHP menganut prinsip legalitas yang menegaskan bahwa tidak ada tindak pidana tanpa penegasan undang-undang sebelumnya. Hal ini menyiratkan bahwa pelaku kejahatan cyber crime mungkin tidak selalu terkena sanksi pidana. Namun, Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman menegaskan bahwa pengadilan memiliki kewajiban untuk memeriksa dan

mengadili setiap perkara yang diajukan, meskipun terdapat argumen bahwa hukumnya tidak jelas. Oleh karena itu, hakim perlu menggunakan penafsiran yang luas terhadap pasal-pasal KUHP yang terkait dengan kejahatan cyber crime tanpa harus menyebutkannya secara eksplisit.

Selain itu, beberapa undang-undang di luar KUHP juga mengatur tentang kejahatan pembajakan komputer, penyalahgunaan komunikasi, dan perlindungan dokumen. Namun, regulasi di luar KUHP ini belum memberikan jaminan kepastian hukum yang memadai dalam menangani tindak pidana *cyber crime*.

Fenomena siber telah menjadi semakin kompleks karena tidak lagi terikat pada batas-batas negara dan dapat diakses dengan mudah dari mana saja. Kerugian dapat timbul baik bagi pelaku transaksi maupun pihak lain yang tidak terlibat dalam transaksi, seperti dalam kasus pencurian dana kartu kredit melalui pembelian online. Karena itu, penting untuk memperhatikan aspek keamanan dan kepastian hukum dalam penggunaan teknologi informasi, media, dan komunikasi agar dapat mengalami perkembangan yang optimal.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dimaksudkan untuk memastikan pengakuan dan penghormatan terhadap hak dan kebebasan individu, serta untuk memastikan keadilan sesuai dengan pertimbangan keamanan dan ketertiban umum dalam masyarakat yang demokratis. Meskipun Undang-Undang Nomor 11 Tahun 2008 merupakan langkah pertama dalam pengaturan teknologi informasi dan transaksi elektronik, implementasinya menghadapi beberapa hambatan.

Pertama, Undang-Undang ini telah beberapa kali mengalami pengujian materi di Mahkamah Konstitusi yang menghasilkan beberapa putusan yang mengubah interpretasi hukum terkait dengan kejahatan siber. Kedua, pasal-pasal mengenai penyidikan kejahatan teknologi informasi dan transaksi elektronik menimbulkan tantangan karena pelaku dapat dengan mudah menghapus bukti kejahatan. Ketiga, sifat virtual dari ruang siber memungkinkan konten ilegal, seperti pencemaran nama baik atau penyebaran kebencian, untuk tersebar dengan mudah. Oleh karena itu, diperlukan tindakan untuk mencegah penyebaran konten ilegal dan memberikan wewenang kepada penyidik untuk meminta informasi dari penyelenggara sistem elektronik.

Undang-Undang ITE memberlakukan yurisdiksi yang luas untuk tindakan hukum yang dilakukan di luar wilayah Indonesia, mengingat teknologi informasi dapat digunakan lintas batas. Harapannya, undang-undang ini dapat memberikan efek jera bagi para pelaku kejahatan cyber crime dan memiliki ketentuan yang lebih rinci mengenai berbagai jenis kejahatan siber.

Pasal 27

*(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.*
*(2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.*
*(3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.*
*(4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.*

Pasal 28 UU ITE mengantur tentang perlindungan konsumen dan aspek sara.

Pasal 28

(*1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.*
*(2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).*

Pasal 29 dalam Undang-Undang ITE mengatur mengenai hukum terkait dengan ancaman yang seringkali dilontarkan atau ditujukan kepada individu yang menggunakan media informasi atau dokumen elektronik.

Pasal 29

*Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.*

Pasal 30

*(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.*
*(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.*
*(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.*

Pasal 31 dalam Undang-Undang ITE menyiratkan legitimasi hukum terkait dengan tindakan penyadapan, terutama mengingat meningkatnya kasus penyadapan yang dilakukan oleh lembaga penegak hukum, seperti Komisi

Pemberantasan Korupsi (KPK), dalam upaya memberantas korupsi. Untuk pemahaman lebih lanjut, rujuklah pada pasal tersebut.

Pasal 31

*(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.*

*(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/ atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.*

*(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.*

Pasal 32 dan 33 dalam Undang-Undang ITE mengatur perlindungan terhadap informasi atau dokumen elektronik, baik yang dimiliki oleh individu lain maupun oleh publik, yang bersifat rahasia (confidential). Seperti yang telah dijelaskan.

Pasal 32

*(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.*

*(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.*

*(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.*

Pasal 33

*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.*

Pasal 34 hingga Pasal 37 menyoroti kategori tindakan yang dilarang, yang sejalan dengan prinsip yang terdapat dalam Pasal 27 hingga Pasal 33. Selain mengadopsi pendekatan punitif dalam kerangka peraturan hukum, pendekatan budaya digunakan untuk meningkatkan kesadaran masyarakat dan aparat penegak hukum terhadap kasus cyber crime sebagai isu pidana. Ini dilakukan dengan

menyebarkan dan mengajarkan etika penggunaan komputer yang baik melalui lembaga pendidikan. Pendekatan ini menjadi penting dalam mengembangkan kode etik dan perilaku yang berkaitan dengan penggunaan teknologi internet yang canggih di tengah masyarakat yang beragam. Pendekatan nonpenal diharapkan dapat mengurangi pelanggaran hukum yang melibatkan teknologi sebagai langkah pencegahan kejahatan. Upaya pencegahan dianggap lebih efektif daripada intervensi setelah terjadinya tindak kejahatan (Hatta et al., 2018).

Selain itu, kerja sama erat antara kepolisian dengan Internet Service Providers (ISP) perlu dilakukan sebagai upaya pencegahan kejahatan *cyber crime* secara prematif dan preventif. Meskipun tugas pokok ISP terkait dengan layanan internet, mereka memiliki catatan lengkap tentang aktivitas pengguna internet. Hal ini karena ISP dapat mengidentifikasi pelaku tindak pidana *cyber crime* melalui log file yang mereka miliki, yang dapat digunakan sebagai bukti oleh penyidik kepolisian. Kerja sama penuh dari ISP akan mempermudah penyidikan kejahatan *cyber crime* yang sering terjadi di Indonesia.

Penegakan hukum terhadap kejahatan *cyber crime* membutuhkan keterampilan teknis di bidang teknologi informasi, bukan hanya senjata konvensional. Oleh karena itu, penegakan hukum memerlukan aturan hukum yang jelas, lembaga yang menjalankan aturan tersebut, dan kesadaran hukum dari masyarakat (Efendi & Hendra, 2022). Semua ini akan menentukan keberhasilan penegakan hukum terhadap kejahatan *cyber crime* di Indonesia, baik saat ini maupun di masa depan (Nawawi et al., 2023).

**Kesimpulan**

Dalam kajian ini, telah terungkap bahwa penegakan hukum terhadap kejahatan *cyber crime* di Indonesia masih menghadapi sejumlah tantangan. Meskipun Undang-Undang Nomor 11 Tahun 2008 telah memberikan landasan hukum yang jelas, implementasinya seringkali terkendala oleh kurangnya pemahaman dan keterampilan teknis di kalangan penegak hukum. Selain itu, perubahan teknologi yang cepat juga menuntut adanya adaptasi dan pembaruan konstan dalam pendekatan penegakan hukum terhadap kejahatan cyber. Oleh karena itu, perlu langkah-langkah konkret untuk meningkatkan kapasitas dan keterampilan penegak hukum, serta kerjasama lintas sektoral antara pemerintah, lembaga swasta, dan masyarakat sipil guna mengatasi tantangan ini secara efektif.

Di samping itu, penting untuk diakui bahwa kejahatan *cyber crime* tidak mengenal batas-batas geografis dan memerlukan pendekatan yang lintas negara. Oleh karena itu, kerja sama internasional dalam pertukaran informasi dan pengembangan strategi bersama juga merupakan hal yang sangat penting. Dengan memperkuat kerangka kerja kerja sama regional dan global dalam penegakan hukum *cyber crime*, kita dapat meningkatkan efektivitas dalam menanggulangi ancaman kejahatan cyber dan melindungi masyarakat serta infrastruktur digital dari

serangan yang merugikan. Dalam hal ini, upaya diplomasi hukum menjadi kunci dalam membangun kerjasama yang kokoh dan berkelanjutan di tingkat internasional untuk menangani tantangan kejahatan cyber secara holistik dan efisien.

**Daftar Pustaka**

Aksenta, A., Irmawati, Ridwan, A., Hayati, N., Sepriano, Herlinah, Silalah, A. T., Pipin, S. J., Abdurrohim, I., Boari, Y., Mardiana, S., Sutoyo, Muh. N., Sumardi, Gani, I. P., & Ginting, T. W. (2023). *Literasi Digital: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 dan Sociaty 5.0.* PT. Sonpedia Publishing Indonesia.

Ali, A., & Haryani, W. (2014). *Sosiologi Hukum: Kajian Empiris Terhadap Pengadilan*. Kencana.

Arief, B. N. (2011). *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*. Citra Aditya Bakti.

Bahri, I. S. (2020). *Cyber Crime Dalam Sorotan Hukum Pidana*. Bahasa Rakyat.

Chazawi, A. (2002). *Kejahatan Terhadap Keamanan dan Keselamatan Negara*. PT. Raja Grafindo Persada.

Efendi, S., & Hadana, E. S. (2022). Criminal Law and Social Development in Aceh. *PROCEEDINGS: Dirundeng International Conference on Islamic Studies*, 185–196. https://doi.org/10.47498/dicis.v1i1.1034

Efendi, S., & Hendra. (2022). STAIN TDM Students' Legal Awareness Level of Aceh Jinayah Qanun. *PROCEEDINGS: Dirundeng International Conference on Islamic Studies*, 1–21. https://doi.org/https://doi.org/10.47498/dicis.v2i1.1347

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Hamdi, S., Suhaimi, & Mujibussalim. (2013). Bukti Elektronik Dalam Sistem Pembuktian Pidana. *Jurnal Ilmu Hukum*, *1*(4), 25–31.

Hatta, M., Rajamanickam, R., Abdullah, D., Hartono, H., Bunga, M., Adji, H. S., Amiruddin, Djanggih, H., Hipan, N., Salle, S., Salmawati, S., Azis, A., Wahab, M., Karinda, K., Saleh, A. A., Sudarsana, I. K., Purnomo, A., Anam, F., & Rianita, D. (2018). Efforts to Overcome Cyber Crime Actions in Indonesia. *Journal of*

*Physics: Conference Series*, *1114*, 012081. https://doi.org/10.1088/1742-6596/1114/1/012081

Manan, A. (2013). *Aspek-Aspek Pengubah Hukum*. Kencana.

Ma'nunah, N. S. (2018). Pencemaran Nama Baik melalui Media Sosial perspektif Hukum Islam. *Al-Jinayah: Jurnal Hukum Pidana Islam*, *3*(2), 403–425. https://doi.org/10.15642/aj.2017.3.2.403-425

Maskun. (2022). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media.

Maskun, M., Achmad, A., Naswar, N., Assidiq, H., Syafira, A., Napang, M., & Hendrapati, M. (2020). Qualifying Cyber Crime as a Crime of Aggression in International Law. *Journal of East Asia and International Law*, *13*(2), 397–418. https://doi.org/10.14330/jeail.2020.13.2.08

Maulana, W. (2023). *Peranan Kepolisian Dalam Kontra Cyber Terorism*. Universitas Islam Sultan Agung Semarang.

Moeljatno. (1983). *Perbuatan Pidana dan Pertanggungjawaban Dalam Hukum Pidana*. Bina Aksara.

Nawawi, J., Darmawati, D., Tajuddin, M. A., & Nutakor, B. S. M. (2023). The Law Enforcement Related to Cyber Crime by Involving the Role of the Cyber Patrol Society in Achieving Justice. *Jurnal IUS Kajian Hukum Dan Keadilan*, *11*(3), 437–447. https://doi.org/10.29303/ius.v11i3.1289

Prabowo, I. A., Pomalingo, S., Istiono, W., Muhariya, A., Irmawati, Sugianto, C. A., Khairunnisa, Pratiwi, M., Ernawati, T., Setiadi, T., Permana, A. A., & Ekawati, N. (2023). *Sistem Komputer dan Informasi*. CV. Gita Lentera.

Rivai, V., Veithzal, A. P., & Fawzi, M. G. H. (2022). *Islamic Transaction Law In Business*. Bumi Aksara.

Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Saputra, R. W. (2016). A survey of cyber crime in Indonesia. *2016 International Conference on ICT For Smart Society (ICISS)*, 1–5. https://doi.org/10.1109/ICTSS.2016.7792846

Saragih, Y. M., & Azis, D. A. (2020). Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal di Era Globalisasi. *Soumatera Law Review*, *3*(2), 265–279. https://doi.org/http://doi.org/10.22216/soumlaw.v3i2.4125

Sugeng. (2024). *Hukum Telematika Indonesia: Edisi Revisi*. Kencana.