**IMPLEMENTATION OF INTERNATIONAL CONVENTIONS IN EFFORTS TO OVERCOME CYBER CRIME IN INDONESIA**

PENERAPAN KONVENSI INTERNASIONAL DALAM UPAYA PENANGGULANGAN KEJAHATAN SIBER DI INDONESIA

NAMA : Maulana Mubaraqal Haj

NPM : 1827350303

Universitas : Sekolah Tinggi Ilmu Hukum Iblam

Alamat : Jl. Kramat Raya No. 25 Senen Jakarta Pusat

|  |
| --- |
| ***Abstract*** |

*Massive technology development brings various problems in society. One of the impacts is the invention of a new interactive media called cyberspace. In cyberspace people are free to do anything anonymously because no one knows your actual profile and citizenship. This is used by a certain people to commit such crime called cybercrime. There are many attempts to regulate rules in cyberspace, whether from international law or national law. One of the attempts was created by the Council of Europe who produced the Convention on Cybercrime with jurisdiction as one special aspect that is important because none of the countries in the world like their jurisdiction violated by other countries, including Indonesia. In Indonesia cybercrime regulation is enacted in Law number 19 Year 2016 about the change Law number 11 Year 2008 regarding Information and Electronic Transaction. The ITE Law has followed the provisions of the Convention on cybercrime, but in practice Indonesia still has difficulty dealing with cybercrime if it is committed from outside Indonesia, unless Indonesia also ratifies the cybercrime Convention which can facilitate cooperation with participants, especially if the perpetrator commits cybercrime outside Indonesia.*

***Keywords:*** *International Law, Jurisdiction, Cybercrime, Council of Europe*

|  |
| --- |
| **Abstrak** |

Perkembangan teknologi yang begitu pesat memunculkan berbagai permasalahan di masyarakat. Salah satu akibatnya tersebut adalah terciptanya sebuah media baru untuk berinteraksi yang disebut *cyberspace*. Di *cyberspace* orang bebas melakukan apapun tanpa diketahui oleh orang lain karena tidak diketahui asal-usul maupun kewarganegaraan asli seseorang. Hal ini dimanfaatkan oleh sebagian orang untuk melakukan suatu kejahatan yang disebut *cybercrime*. Telah banyak usaha untuk melakukan pengaturan di *cyberspace* untuk mencegah terjadinya *cybercrime* baik oleh hukum internasional maupun hukum nasional. Salah satunya adalah dengan lahirnya *Convention on Cybercrime* yang dibuat oleh Dewan Eropa (*European Council*), aspek yang menjadi perhatian khusus dalam konvensi ini adalah masalah yurisdiksi sebuah negara dalam menangani kasus *cybercrime* karena semua negara tidak senang yurisdiksi negaranya dilampaui oleh negara lain, termasuk Indonesia. Di Indonesia sendiri pengaturan mengenai *cybercrime* diatur dalam Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang ITE telah mengikuti ketentuan dalam Konvensi tentang *cybercrime* namundalam prakteknya Indonesia masih kesulitan menangani kejahatan siber jika dilakukan dari luar Indonesia, kecuali Indonesia ikut meratifikasi Konvensi *cybercrime* yang dapat mempermudah kerjasama dengan peserta terutama jika pelaku melakukan kejahatan siber di luar Indonesia.

**Kata Kunci :** Hukum Internasional Yurisdiksi, Cybercrime, Dewan Eropa

1. **PENDAHULUAN**

Dengan kemajuan teknologi yang cepat, kita kini menjadi sangat bergantung pada sebuah alat elektronik bernama komputer. Kata "komputer" berasal dari kata Latin "computare", yang artinya "untuk menghitung". Sementara "internet" merupakan jaringan komputer global yang saling terkait. Hal ini memberikan dampak pada setiap sisi kehidupan kita.

Perkembangan komputer saat ini sungguh luar biasa pesat, seperti yang ditunjukkan oleh riset terbaru dari Josephson Junction. Dalam studi tersebut, Josephson berupaya mengganti komponen dasar prosesor dengan helium cair yang telah didinginkan hingga mendekati nol absolut (sekitar minus 200 derajat Celcius). Metode ini berpotensi meningkatkan kapasitas pemrosesan prosesor hingga tingkat yang sangat tinggi. Josephson terinspirasi dari novel fiksi "2001: Space Odyssey" karya Arthur C. Clarke. Dalam novel tersebut, terdapat sebuah komputer bernama "HAL 9000" yang mewujudkan visi komputer generasi kelima. Komputer ini, yang dilengkapi dengan kecerdasan buatan, mampu berkomunikasi dengan manusia, memproses informasi visual, dan belajar dari pengalamannya sendiri.

Perangkat lunak dan jaringan yang mendukung fungsi komputer telah berkembang pesat sejalan dengan evolusi komputer. Salah satunya adalah kemunculan internet, teknologi yang saat ini banyak dimanfaatkan oleh sebagian besar orang. Kata "internet" bisa memiliki dua pengertian:

a) "internet" (dengan huruf awal kecil) merujuk pada sebuah sistem komunikasi di mana berbagai komputer dapat saling berhubungan dan berkomunikasi, meskipun menggunakan perangkat keras dan lunak yang beragam (disebut juga sebagai "mekanisme internet").

b) "Internet" (dengan huruf awal besar) mengacu pada kumpulan dari berbagai jaringan, yang dikenal pula sebagai jaringan dari jaringan, melibatkan jutaan komputer yang saling berkomunikasi.

Namun, *The Federal Networking Council* (FNC) memberikan definisi terkait internet pada resolusinya yang dikeluarkan pada 24 Oktober 1995. Definisi tersebut adalah:

*The Internet is a global information system that:*

1. *Is logically connected through a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions;*
2. *Is capable of supporting communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its extensions, as well as other IP-compatible protocols; and*
3. *Provides, utilizes, or facilitates access, whether public or private, to high-level services built upon the communications and related infrastructure described herein.*

Sejarah internet bermula ketika Uni Soviet meluncurkan satelit buatan pertamanya, Sputnik, selama era perang dingin pada tahun 1957. Sebagai respons terhadap langkah Uni Soviet, Amerika Serikat mendirikan *Agency for Advance Research* (ARPA) pada tahun 1958 di bawah *Department of Defense* (DoD). ARPA dibentuk dengan misi untuk melindungi data dan informasi penting. J.C.R. Licklider, seorang pakar komputer dari *Massachusetts Institute of Technology* (MIT), diangkat untuk memimpin program komputer di *Defense Advanced Research Project Agency* (DARPA), sub-bagian dari ARPA yang menangani riset pertahanan dan keamanan. Salah satu misi awal dari ARPA adalah menciptakan sebuah jaringan yang bisa melindungi informasi dan data penting tersebut, yang kemudian menghasilkan ARPANET.

Pertama kali ARPANET dikomersilkan oleh kontraktornya, *Bolt, Beranek & Newman* (BBN), dengan meluncurkan layanan paket data pertama untuk publik bernama telnet. Istilah 'internet' mulai dikenal luas pada tahun 1982, saat ARPANET bukan lagi menjadi host utama yang mengkoneksikan semua komputer dunia. Sebagai alternatif, *Transmission Control Protocol/Internet Protocol* (TCP/IP) diterapkan sebagai protokol universal yang memungkinkan pengguna komputer untuk terkoneksi ke host tertentu tanpa harus mengetahui jalur spesifik menuju host tersebut.

Setelah adopsi TCP/IP, antara tahun 1980-1990, Tim Berners-Lee, yang bekerja sebagai kontraktor di *European Organization for Nuclear Research* (CERN) di Swiss, menciptakan ENQUIRE, sebuah basis data untuk staf CERN. Dia menerapkan ide *hypertext* yang diperkenalkan oleh Ted Nelson pada 1965. Hypertext memungkinkan halaman untuk terhubung langsung melalui tautan tanpa perlu memasukkan alamat halaman yang dituju secara manual. Kemudian, Berners-Lee bekerja sama dengan Robert Cailliau untuk mengintegrasikan *hypertext* dengan internet. Hasil dari kolaborasi mereka adalah lahirnya halaman web pertama di dunia pada tahun 1990, yang dikenal sebagai *World Wide Web* (WWW). Pada periode 1994-1996, WWW mulai dikomersilkan. Ide yang diperkenalkan oleh Berners-Lee dan Cailliau diadopsi oleh DARPA, yang kemudian mendirikan *World Wide Web Consortium* (W3C). Saat ini, internet telah berkembang menjadi era yang dikenal sebagai web 2.0, dengan tampilan dan bahasa pemrograman yang lebih canggih dan kompleks.

Kemajuan internet yang begitu cepat telah menginspirasi berbagai konsep baru dalam teknologi informasi, salah satunya adalah gagasan *cyberspace* sebagai "dunia atau tempat tinggal yang baru". Istilah *cyberspace* pertama kali dikenalkan ke publik oleh William Gibson melalui novel fiksi ilmiahnya, Neuromancer. Dalam esensi, cyberspace bisa diartikan sebagai ruang tak berbatas di mana data tersusun dan diintegrasikan melintasi berbagai media. Definisi lainnya menyebutkan bahwa cyberspace adalah manifestasi dari dunia digital yang kini menjadi bagian dari hampir semua aspek kehidupan manusia.

Meskipun internet menjadi sarana penyampaian informasi yang efisien, ia juga memiliki sisi negatif, khususnya dari aspek keamanan. Walaupun saat ini banyak tersedia program-program yang dirancang untuk melindungi data penting di internet, seperti firewall, tetap saja ada individu yang memanfaatkannya untuk tujuan kriminal. Beberapa orang awalnya hanya tertarik menembus keamanan jaringan sebagai sebuah tantangan atau hobi, dan mereka sering disebut sebagai cracker. Namun, ada juga kelompok yang tidak hanya berfokus pada penetrasi keamanan, tetapi juga menyalahgunakan serta memodifikasi informasi untuk aktivitas ilegal seperti penipuan, pencurian, atau pencemaran nama baik. Kelompok ini lebih dikenal dengan nama hacker, dan mereka dapat mengakses jaringan rahasia dari berbagai tempat di dunia.

Untuk melawan tindakan cracker dan hacker, diperlukan regulasi hukum yang ketat bagi setiap individu yang mengakses internet. Namun, tantangan besar yang muncul adalah terkait yurisdiksi antarnegara: apakah suatu negara memiliki kewenangan untuk mengadili pelaku cybercrime yang berasal dari negara lain? Sebagai upaya menangani isu ini, berbagai negara telah berupaya membahas masalah cybercrime secara intensif. Dewan Eropa, misalnya, telah aktif mendiskusikan dan mengkaji isu ini. Hasil dari diskusi tersebut adalah terciptanya suatu konvensi internasional mengenai cybercrime yang dikenal sebagai The Council of Europe Convention on Cybercrime atau lebih dikenal dengan Convention on Cybercrime. Konvensi ini ditandatangani di Budapest, Hungaria pada 23 November 2001. Dalam konvensi ini, berbagai isu termasuk yurisdiksi menjadi salah satu fokus utama pembahasan. Sampai dengan 15 Juli 2020, sebanyak 65 negara telah meratifikasi konvensi ini.

Pada 2009, isu cybercrime mendapatkan perhatian internasional ketika dugaan mata-matai digital oleh China menjadi sorotan. Awal mula kasus ini terungkap ketika aktivis pro-Tibet menduga bahwa informasi penting tentang Dalai Lama dan pejabat pemerintahan pengasingan Tibet telah disusupi dan diambil secara ilegal oleh pihak yang tidak dikenal. Dengan bantuan ahli IT dari Jerman dan Kanada, mereka mengusut jejak digital dari serangan ini. Hasil investigasi menunjukkan bahwa sekitar 1300 komputer dari pemerintah di 103 negara telah dipantau, diduga kuat oleh pemerintah China, termasuk komputer di Indonesia.

Indonesia mulai berupaya mengatur aspek hukum terkait cybercrime sejak tahun 1998-1999 dengan diterbitkannya Undang-Undang No. 36 Tahun 1999 mengenai telekomunikasi. Meski undang-undang tersebut tidak secara eksplisit membahas cybercrime, namun telah mencakup aspek-aspek awal dari cybercrime, seperti akses ilegal. Kemudian, dalam perkembangannya, Indonesia menerbitkan Undang-Undang No. 19 Tahun 2016, yang merupakan revisi dari Undang-Undang No. 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (ITE). Saat pertama kali diterapkan, regulasi ini memicu perdebatan di masyarakat. Meskipun demikian, seiring waktu, keberadaan undang-undang ini menegaskan komitmen Indonesia untuk menjawab tantangan kejahatan di era digital.

Dari konteks yang telah dijelaskan sebelumnya, penulis mengidentifikasi beberapa isu yang akan diteliti, yaitu:

1. Bagaimana regulasi Hukum Internasional terkait yurisdiksi atas kejahatan cyber?

2. Bagaimana Indonesia menerapkan konvensi internasional dalam mengatasi kejahatan siber?

Dalam pembuatan karya tulis ilmiah ini, penulis memilih metode penelitian hukum normatif. Melalui studi literatur, penulis berupaya mengumpulkan data yang relevan dan mendukung topik yang sedang dibahas. Sumber-sumber yang digunakan meliputi:

1. Sumber Hukum Primer: Ini mencakup sumber hukum dengan otoritas hukum yang mengikat dan relevan dengan penelitian, seperti The Council of Europe Convention on Cybercrime, Undang-Undang Telekomunikasi, Undang-Undang Penyiaran, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dan Undang-Undang Keterbukaan Informasi Publik.

2. Sumber Hukum Sekunder: Ini mencakup buku teks, riset online, artikel ilmiah, jurnal, majalah, koran, makalah, dan skripsi.

3. Sumber Hukum Tersier: Sumber ini memberikan petunjuk atau klarifikasi mengenai sumber hukum primer dan sekunder, contohnya adalah kamus.

Studi ini merupakan penelitian deskriptif yang memberikan deskripsi mendalam mengenai kejahatan siber dalam konteks hukum internasional, berbagai teori dan prinsip dasar yang terkait, serta regulasi nasional di Indonesia. Tujuannya adalah untuk melakukan analisis hukum normatif, di mana pembentukan hipotesa tidak menjadi prioritas utama.

1. **PEMBAHASAN**
2. ***Cyberspace* sebagai Medan Baru bagi Kejahatan Siber**

Era digital yang muncul seiring dengan kemunculan internet telah memperkenalkan terminologi baru, salah satunya adalah "cyberspace" atau sering disebut dengan dunia maya. Istilah ini pertama kali dikenalkan oleh William Gibson dalam novel karyanya, Neuromancer, yang terbit di dekade 1980-an. Gibson menggambarkan cyberspace sebagai suatu wilayah tanpa batasan di mana informasi-informasi tersusun rapi lintas platform.

Cyberspace dan kejahatan siber saling berkaitan, mirip dengan interaksi antara manusia dan lingkungannya, yang menunjukkan keterkaitan antara aktivitas dengan medinya. Namun, analogi ini kurang tepat jika kita bicara tentang territorial atau batas wilayah. Di dunia nyata, kita bisa dengan mudah menentukan area di mana suatu aktivitas berlangsung. Namun, dalam cyberspace, aktivitas yang terjadi tidak terikat oleh batasan geografis. Isu teritorial ini sangat krusial dalam menentukan hukum mana yang berlaku untuk suatu insiden.

Cyberspace menawarkan sejumlah karakteristik khas yang berpengaruh terhadap aspek hukum, antara lain:

a. Tanpa Batas Geografis (Tanpa Pembatasan Wilayah)

Salah satu sifat paling mencolok dari cyberspace adalah ketiadaan pembatasan geografis. Ini karena semua yang berlangsung di cyberspace adalah interaksi digital yang bisa menyeberangi batasan negara dengan mudah. Sebagai ilustrasi, komunikasi lewat chat dapat berlangsung antara individu dari negara yang berbeda tanpa adanya aturan yang membatasi. Dalam jurnal David G.Post dengan judul “Anarchy, State and The Internet: An Essay on Law Making in Cyberspace”, ada pandangan yang menyatakan bahwa cyberspace bukanlah tentang banyak yurisdiksi, tapi justru tentang ketiadaan yurisdiksi. Ini mengimplikasikan bahwa cyberspace cenderung menjadi area yang bebas dari aturan hukum (sebuah surga tanpa hukum).

b. Kemampuan Menyembunyikan Identitas (Anonimitas)

Di cyberspace, individu bisa masuk dan berinteraksi sambil menyembunyikan identitas aslinya, seringkali dengan menggunakan nama samaran. Informasi pribadi lainnya pun bisa disamarkan atau bahkan dimodifikasi oleh pengguna. Karakteristik ini menimbulkan tantangan bagi penegak hukum, karena individu yang melanggar aturan atau melakukan tindak kejahatan bisa dengan mudah mengelabui sistem dengan identitas palsu, membuatnya sulit dilacak.

c. Kemudahan Bergerak (Mobilitas)

Cyberspace memungkinkan pengguna untuk beraktivitas tanpa terikat oleh lokasi fisik tertentu. Ini artinya, seseorang dapat mengakses dan berpartisipasi dalam dunia digital dari mana saja. Hal ini sejalan dengan konsep online yang menekankan bahwa interaksi di cyberspace tidak harus terikat pada lokasi tertentu.Dampaknya dalam hukum dengan sifat fleksibilitas tersebut, pelaku kejahatan di *cyberspace* dapat dengan mudah lolos dengan berpindah-pindahnya lokasi tempat aktifitas *cybercrime* yang berlangsung dari satu yurisdiksi ke yurisdiksi lainnya yang dengan mudah memilih negara yang kondisi penegakkan hukumnya lemah, sehingga semaikin membuka peluang untuk lolos dari jeratan hukum.

1. **Distingsi antara Kejahatan yang berkaitan dengan Siber dengan *Cybercrime***

Kemajuan dalam ilmu dan teknologi telah menciptakan infrastruktur berupa teknologi informasi, yang sering dikenal sebagai teknologi telekomunikasi, yang memfasilitasi aktivitas manusia. Kemunculan komputer dan internet telah mengubah cara komunikasi sehingga tidak lagi dibatasi oleh batasan geografis suatu negara.

Peningkatan penggunaan teknologi, khususnya internet, telah memberikan banyak manfaat bagi kemajuan masyarakat, terlihat dari munculnya layanan online seperti e-commerce, e-banking, e-pemerintahan, dan e-pendidikan. Namun, setiap kemajuan selalu disertai dengan tantangan, dalam hal ini kejahatan siber. Beberapa pelaku memanfaatkan internet untuk melakukan kejahatan yang melibatkan komputer, seperti penipuan melalui kartu kredit dan pasar modal, eksploitasi anak dalam bentuk pornografi, dan aksi terorisme. Selain itu, ada juga yang menjadikan komputer sebagai sasarannya, misalnya dengan melakukan perubahan tampilan situs web (defacing), peretasan (cracking), atau manipulasi sinyal telepon (phreaking).

1. Kejahatan Terkait Komputer (Cyber-related Crime)

Banyak pakar yang telah berusaha memberikan definisi terhadap konsep kejahatan terkait komputer, baik dari perspektif literatur (dalam konteks kriminologi) atau dari kerangka hukum (dalam konteks yuridis). Akibatnya, banyak definisi yang muncul sesuai dengan tujuan dan perspektif berbeda dari masing-masing sumber. Sebagai contoh, salah satu definisi kejahatan terkait komputer disajikan oleh IBM. Inc. Jepang, sebuah perusahaan yang spesialis di bidang komputer.

*a. Crimes that utilize computers as tools for theft, fraud, embezzlement, and the like.*

*b. Offenses committed through computer systems, such as tampering with, stealing, and deleting data and programs.*

Berdasarkan definisi di atas, kita dapat menyimpulkan bahwa kejahatan komputer dapat didefinisikan sebagai tindakan ilegal yang melibatkan penggunaan komputer baik sebagai alat maupun sebagai sasaran, dengan atau tanpa tujuan mendapatkan keuntungan, yang merugikan pihak lain. Secara lebih spesifik, kejahatan komputer juga dapat diartikan sebagai tindakan yang melanggar hukum dengan memanfaatkan teknologi komputer yang mutakhir.

Berikut adalah beberapa pendapat mengenai kategorisasi kejahatan komputer:

Menurut Jongerius, kejahatan komputer dapat dikategorikan menjadi:

1. Intervensi komputer;

2. Pengintaian digital;

3. Gangguan sistem komputer melalui perusakan atau penghancuran perangkat dan/atau jaringannya;

4. Penggunaan komputer tanpa otorisasi;

5. Akses ilegal ke sistem komputer.

Sebuah studi dari Kongres Amerika Serikat mengidentifikasi empat jenis kejahatan komputer, yaitu:

1. Memasukkan data palsu ke dalam komputer;

2. Menggunakan fasilitas yang terkait dengan komputer;

3. Modifikasi atau kerusakan informasi atau file;

4. Pencurian, baik secara digital atau metode lain, dari uang, fasilitas, dan data berharga.

Sementara itu, klasifikasi lain menempatkan kejahatan komputer ke dalam empat kategori besar:

1. Sabotase dan vandalisme terhadap sistem komputer;

2. Penggunaan fasilitas komputer tanpa izin sebagai bentuk pencurian;

3. Kejahatan terkait barang melalui penggunaan komputer;

4. Kejahatan terhadap informasi atau pencurian data.

Dari berbagai klasifikasi atau kategorisasi di atas, jelas bahwa banyak kejahatan komputer pada dasarnya adalah bentuk kejahatan konvensional yang melibatkan komputer, baik sebagai alat pelaku maupun sebagai target. Hanya beberapa jenis kejahatan yang benar-benar spesifik terkait dengan komputer, seperti aktivitas hacking.

1. **Definisi *Cybercrime***

Convention on Cybercrime memang tidak memberikan definisi langsung untuk istilah "cybercrime". Namun, konvensi tersebut menyajikan definisi dari empat istilah lain: "computer system", "computer data", "service provider", dan "traffic data".

Kata cybercrime merupakan gabungan dari dua kata: cyber dan crime. Kata "cyber" berasal dari istilah cybernetics. Menurut Encyclopedia of Knowledge, yang dikutip oleh Edmon Makarim, dikatakan:   
"...the term was formerly used to describe an interdisciplinary approach to studying control and communication among animals, humans, machines, and organizations. The word itself..."

Sedangkan "crime" mengacu pada perbuatan yang salah. Dalam pengertian sederhananya, kejahatan dapat dijelaskan sebagai tindakan yang anti sosial.

1. Jenis-jenis Cybercrime Berdasarkan Convention on Cybercrime, tindakan yang dapat dikategorikan sebagai cybercrime diatur dalam pasal 2-5, dan jenis-jenis dari tindakan tersebut meliputi:
2. *Illegal Access*

*Illegal access* mencakup pelanggaran terhadap dasar-dasar ancaman yang berpotensi merusak terhadap integritas data dan sistem komputer. Perlindungan dari Illigal Acces ini mencerminkan kepentingan berbagai organisasi atau kelompok serta individu yang menginginkan sistem mereka beroperasi tanpa gangguan atau halangan.

1. *Illegal Interception*
2. Definisi *Interception* menurut Laporan Penjelasan Terhadap Convention on Cybercrime adalah, "Interception using technical means involves listening to, monitoring, or surveilling the content of communications, obtaining data content either directly through access and use of a computer system, or indirectly through the use of electronic eavesdropping or recording devices. Interception can also entail recording.". Tujuan dari pasal tersebut adalah untuk melindungi hak kebebasan komunikasi data. Pelanggaran ini khususnya ditargetkan pada pemindahan data komputer yang bersifat pribadi.
3. *Data Interception*

Ketentuan mengenai perusakan data diatur sebagai tindak pidana dengan maksud untuk memberi perlindungan yang setara pada data komputer dan program komputer seperti halnya benda fisik. Misalnya, menyisipkan kode berbahaya (*malicious codes*), *Viruses*, dan *Trojan Horse* ke dalam sistem komputer dianggap melanggar berdasarkan Pasal 4 ayat 1 dan dianggap sebagai tindak pidana jika dilakukan secara sengaja untuk merusak, menghapus, memburukkan, mengubah, atau memodifikasi data komputer tanpa izin.

1. *System Interference*

Dalam Pasal 5 konvensi tersebut, gangguan sistem diatur sebagai tindak pidana apabila dilakukan dengan sengaja, yang serius menghambat fungsi dari sistem komputer tanpa hak. Hal ini harus dilakukan dengan cara memasukkan, menyebarkan, merusak, menghapus, atau menyembunyikan data komputer. Tujuan dari pengaturan ini adalah untuk mencegah gangguan serius terhadap fungsi sistem komputer tanpa otorisasi.

1. **Yurisdiksi Berdasarkan Konvensi *Cybercrime***

Masalah yurisdiksi menurut Konvensi Cybercrime yang disusun oleh Dewan Eropa ditempatkan secara khusus pada suatu pasal, yaitu pasal 22. Pasal ini memiliki lima ayat yang menjelaskan mengenai:

1. *Each Party shall adopt such legislative and other measures as  maybe necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:*
2. *in its territory; or*
3. *on board a ship flying the flag of that Party; or*
4. *on board an aircraft registered under the laws of that Party; or*
5. *by one of its nationals, if the offence is punishable under criminal law  
   where it was committed or if the offence is committed outside the territorial jurisdiction of any State.*
6. *Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.*
7. *Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.*
8. *This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.*
9. *When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.*

Pasal 22 ini memuat sejumlah kritreria yang mewajibkan setiap pihak dalam konvensi ini untuk menerapkan yurisdiksinya terhadap kejahatan-kejahatan yang disebutkan mulai dari pasal 2 hingga pasal 11 dalam konvensi ini. Kejahatan-kejahatan tersebut antara lain :

1) Penyadapan secara tidak sah (illegal interception),

2) Memasuki suatu sistem komputer secara tidak sah (illegal access),

3) Intervensi terhadap data (data intervention),

4) Intervensi terhadap sistem (system interference),

5) Penyalahgunaan alat (misuse of device),

6) Pemalsuan melalui komputer (computer related forgery),

7) Penipuan melalui komputer (computer realted fraud),

8) Kejahatan pornografi anak (offences related to child pornography),

9) Pelanggaran hak cipta dan hak-hak lainnya yang terkait (offences related  
to infringements of copyright and related rights),

10) Segala bentuk percobaan, pembantuan, dan persekongkolan yang berkaitan dengan kejahatan-kejahatan tersebut diatas.

Ayat pertama dalam pasal ini menganut prinsip teritorial, artinya setiap negara yang menjadi pihak dalam konvensi ini berhak mengadili terhadap kejahatan-kejahatan yang tercantum dalam konvensi ini yang dilakukan di wilayahnya.

1. **Regulasi Cyber Crime di Indonesia**

Dalam konteks regulasi yang berkaitan dengan cybercrime di Indonesia, kita masih berada di tahap awal. Saat ini, hanya ada satu regulasi yang secara eksplisit mengatur isu cybercrime, yakni Undang-Undang No 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (dikenal juga sebagai UU ITE). Sebelumnya, Indonesia hanya memiliki regulasi yang berkaitan dengan telekomunikasi, yaitu Undang-Undang No 3 tahun 1989 yang selanjutnya diperbarui melalui Undang-Undang No 36 Tahun 1999 tentang materi yang sama. Dalam proses pengesahannya, undang-undang ini menjadi subjek perdebatan karena dinilai berpotensi menghambat kebebasan berekspresi di dunia maya. Namun, dalam UU ini, detil mengenai tindakan-tindakan yang termasuk dalam kategori cybercrime diuraikan dengan jelas, yang tercantum dalam Pasal 27 hingga Pasal 37.

1. **PENUTUP**
   1. **KESIMPULAN**

Dalam hukum internasional yang berkaitan dengan cybercrime, yurisdiksi diatur dalam Convention on Cybercrime. Masalah yurisdiksi yang ditekankan dalam Convention on Cybercrime, yang disusun oleh Council of Europe, khususnya dijelaskan dalam satu pasal, yaitu pasal 22. Pasal tersebut, yang terbagi dalam lima ayat, dinyatakan sebagai berikut:

Dari penjelasan tentang Pasal 22 di atas, terlihat bahwa Convention on Cybercrime yang dirancang oleh Council of Europe masih mengadopsi konsep yurisdiksi yang telah dikenal dan digunakan di tingkat internasional. Selain itu, meskipun konvensi ini tidak secara eksplisit mendukung konsep analogi, tampaknya konvensi cenderung 'membebaskan' diri dari konsep pemisahan. Hal ini dapat dipahami, mengingat urgensi untuk menciptakan regulasi khusus bagi cyberspace saat ini masih dalam tahap diskusi yang berkelanjutan dan belum ada konsep pasti yang diterima luas. Sementara itu, frekuensi kejahatan siber, sebagai dampak negatif dari kemajuan teknologi, terus meningkat. Kondisi tersebut bisa berujung pada ketidakstabilan di cyberspace jika tidak ada regulasi yang jelas. Selain itu, dengan keberadaan ketentuan yurisdiksi dalam Pasal 22, negara anggota konvensi memiliki dasar hukum yang jelas untuk menerapkan yurisdiksi mereka terhadap kejahatan siber, sehingga potensi konflik akibat tumpang tindih yurisdiksi bisa diminimalisir.

Setelah penerapan Undang-Undang No 11 tahun 2008 mengenai Informasi dan Transaksi Elektronik, yurisdiksi didefinisikan secara khusus dalam pasal 2. Berdasarkan penjelasan Pasal 2, dapat diinterpretasikan bahwa regulasi ini mengikuti prinsip objective territoriality (teritorial objektif) dimana yang menjadi fokus utama adalah dampak dari tindakan yang diuraikan dalam pasal-pasal tersebut. Kesimpulannya, tidak ada pergeseran pandangan terkait yurisdiksi antara UU Telekomunikasi dan UU ITE. Kedua regulasi ini berpegang pada prinsip objective territoriality (teritorial objektif), yang menekankan lebih pada hasil dari tindakan ketimbang lokasi di mana tindakan tersebut dilakukan.

* 1. **SARAN**

1. Pemerintah perlu meresmikan Convention on Cybercrime untuk memfasilitasi kolaborasi dengan negara-negara peserta saat menghadapi kasus cybercrime yang merugikan Indonesia, sekaligus memperkuat kerjasama dalam sektor teknologi informasi, memastikan Indonesia tetap up-to-date dalam menanggulangi kasus cybercrime.
2. Undang-Undang Informasi dan Transaksi Elektronik perlu direvisi untuk menyesuaikannya dengan Convention on Cybercrime, baik dari aspek substantif maupun prosedur. Selain itu, Undang-Undang Keterbukaan Informasi Publik harus diperkaya dengan ketentuan mengenai yurisdiksi, sehingga apabila terdapat penyalahgunaan informasi publik melalui dunia maya, hukum Indonesia dapat diterapkan.
3. Untuk menjaga data penting dan rahasia negara dari akses yang tidak sah (seperti peretasan atau penyadapan), Kementerian Komunikasi dan Informasi seharusnya mulai mengembangkan sebuah sistem atau jaringan komputer dengan keamanan yang ketat. Langkah ini dapat dilakukan dengan memasang firewall berlapis-lapis dan memastikan penggunaan kata sandi yang kompleks dan sulit ditembus.
4. **DAFTAR PUSTAKA**

Arief Mansur, Dikdik M. dan Elisatris Gultom. Cyber Law-Aspek Hukum

Teknologi Informasi, Cet.1. Bandung. PT Refika Aditama, 2005.

Barry, Colin. the Future of Cyberterrorism, Crime and Justice International, March 1997.

Burk, Dan L. Jurisdiction in a World Without Border.www.cyberjurisdiction.net

diakses tanggal 5 Mei 2009.

Connoly, Chris. An Introduction to Internet Content Regulation in Asia and the

Pacific. Galexia intelligence reports, articles, papers, conferences and

seminars. [www.galexia.com](http://www.galexia.com) , diakses pada tanggal 25 Juni 2009.

Dressler, Joshua. ed. The Encyclopedia of Crime and Justice, edition 2. New

York. Macmillian Reference, 2001.

Granville, Johanna. The Transnational Dimension of Cybercrime and Terrorism.

British Journal of Criminology volume .43, 2003.

Graycar, Adam. Cybercrime: Old Wine in New Bottles?. Makalah disampaikan

dalam seminar dengan tema Cybercrime di Centre for Crimnology, The

University of Hongkong, tanggal 24 Februari 2000.

Gregory Lastwoka, F and Dan Hutter. Virtual Crime.

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=564801> , pada tanggal 5

Maret 2009.

Goodman, Mark D. and Susan W. Brenner. The Emerging Consensus On Criminal

Conduct in Cyberspace. http://www.lawtechjournal.com/articles/2002/

03\_020625\_goodmanberner.php . Diakses pada tanggal 1 April 2009.

Hariyanti Chandra, Francisca. Internet:Information Superhighway, Makalah pada

Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan

Presentasi Melalui Media Komputer bagi Dosen PTS Kopertis Wilayah V1 di Semarang, 4-8 September 1995.

Hamano, Masaki. Comparative Study I The Approach to Jurisdiction in

Cyberspace.[www.cyberjurisdiction.net](http://www.cyberjurisdiction.net) , diakses tanggal 13 Mei 2009.

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

1990.

Istijar, Muhammad. Korupsi Kejahatan Luar Biasa.<www.hokionline>, diakses

pada 30 Juni 2009.

Johnson, David R. and David G. Post. And How Should The Internet Be

Governed?.[www.itworld.com](http://www.itworld.com) , diakses tanggal 13 Mei 2009.

Keyser, Mike. The Council of Europe Convention on Cybercrime. Journal of

Transnational Law and Policy, volume 12, 2003.

Kanter, E.Y dan S.R Sianturi. Asas-asas Hukum Pidana Di Indonesia Dan

Penerapannya, Cet.2. Jakarta. Storia Grafika, 2002.

Karnasudirja. Eddy Djunaidi. Yurisprudensi Kejahatan Komputer. Jakarta. CV.

Tanjung Agung, 1993.

Lloyd, Ian J. Information and Technology Law. third edition. London.

Butterworths. 2000.

Makarim, Edmon. Kompilasi Hukum Telematika, cet kedua. Jakarta.

Rajagrafindo, 2003.

Menthe, Darrel. Jurisdiction in Cyberspace : A Theory of International Spaces.

[www.mttlr.org/volfour/menthe\_art.html](http://www.mttlr.org/volfour/menthe_art.html) , diakses pada tanggal 20 April

2009.

Murphy, John F. Civil Liability for the Commision of International Crimes as an

Alternative to Criminal Prosecution. Harvard Human Rights Journal 9 th

edition 2007.

Nawawi Arief, Barda. Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tidak

Pidana Maya Antara. Makalah pada seminar nasional dalam rangka

penyusunan RUU teknologi informasi.

Oberding, Juliet M. and Treje Norderhaug. A Separate Jurisdiction for

Cyberspace.[www.cyberjurisdiction.net](http://www.cyberjurisdiction.net) , diakses pada 16 Mei 2009.

Pattiradjawane. Rene L. Cyberlaw: Apakah bisa Melindungi Pribadi Pengguna

Internet?. <www.kompas.com>, diakses tanggal 23 Mei 2009.

Post, David G. Anarchy, State and The Internet: An Essay on Law Making in

Cyberspace. Journal of Online Law, 1995.

Purbo, Onno W. Sejarah Internet, <www.ilmukomputer.com> , diakses pada

tanggal 15 Maret 2009.

Rasch, Mark D. Criminal Law and The Internet. <www.cybercrime.net>, diakses

tanggal 20 April.

Rahardjo, Agus. Cybercrime :Pemahaman dan Upaya Pencegahan Kejahatan

Berteknologi. Bandung. Citra Aditya, 2002.

Ramli, Ahmad M. Cyberlaw dan HaKI Dalam Sistem Hukum Indonesia, cet-1.

Bandung. PT Refika Aditama, 2004.

Reinhard Golose, Peter. Perkembangan Cybercrime dan Penanganannya di

Indonesia oleh POLRI. Makalah disampaikan pada seminar nasional

mengenai “Penanganan Cybercrime di Indonesia ke Arah Pengembangan

Kebijakan Menyeluruh dan Terpadu”, tanggal 10 Agustus 2006.

Roden, Adrian. Computer Crime and The Law. Criminal Law Journal, 1991.

Sanford, Kadish and May T Morrison. ed.Encyclopedia of Crime and

Justice”,Law University of California, Berkeley, Volume I.

Sarwoko, Djoko. Computer Crime sebagai Dimensi Baru Tindak Pidana Ekonomi.

Varia Peradilan Nomor 21 Tahun II, Juni 1987.

Starke, J.G. Introduction to International Law. 9th ed. London. Butterworths, 2000

Sudirman, Ivan dan Romi Satria. Sejarah Komputer. Makalah disampaikan pada

Training Ilmu Komputer,bahan didownload dari <www.ilmukomputer.com>

Sood, Vivek. Cyber Law Simplified. New Delhi. Tata McGraw-Hill Publishing

Co.Ltd, 2001.

Sutadi, Heru. “Cybercrime, apa yang bisa diperbuat?”,

<http://www.sinarharapanbaru.co.id/berita/0304/05/op01.html> , diakses

tanggal 15 April 2009.

UNESCO. The International Demension of Cyberspace Law. England. Ashgate

Publishing Ltd., 2000.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang

Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Wilske, Stephen and Teresa Schiller. International Jurisdiction in Cyberspace:

Which States May Regulate The Internet. [www.cyberjurisdiction.net](http://www.cyberjurisdiction.net) ,

diakses tanggal 23 Mei 2009.

Wisnubroto, A.L. Kebijakan Hukum Pidana dalam Penanggulangan

Penyalahgunaan Komputer. Yogjakarta. Penerbitan Universitas Atmajaya,

2001.

Yuridiksi berdasarkan..., Afitrahim M.R, FHUI, 2009

Weber, A. M. (2003). The Council of Europe’s Convention on Cybercrime. *Berkeley Technology Law Journal*, *18*(1), 425–446. http://www.jstor.org/stable/24120528