# Implementasi Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Di Bidang Komputer

**Abdul Rauf, Hardi**
Jurusan Sistem Informasi STMIK Dipanegara Makassar
Alamat : Jl. Perintis Kemerdekaan Km.9 Makassar Telp. (0411) 587194
a_rauf2002@yahoo.com, hardi@dipayahoo.com

**ABSTRAK**

Permasalahan yang dibahas dalam penelitian ini adalah bagaimanakah bentuk upaya penanggulangan *cybercrime* dengan menggunakan sarana penal serta mekanisme pertanggungjawaban pidananya. Metode penelitian yang digunakan adalah *statuta approach, conseptual approach,* dan *comparative approach*. Tipe penelitiannya adalah *Normative Legal Research*. Hasil penelitian menunjukkan bahwa upaya penanggulangan *cybercrime* dengan menggunakan kebijakan hukum pidana (*penal policy*) harus mengikuti perkembangan jaman. Oleh karena itu dibentuklah undang-undang informasi dan transaksi elektronik sebagai upaya untuk mengatasi masalah sebelumnya terkait dengan pengaturan tentang penanggulangan *cybercrime* yang masih tersebar dalam berbagai bentuk peraturan. Pertanggungjawaban pidana dalam undang-undang informasi dan transaksi elektronik dapat dikenakan kepada *individu* maupun *korporasi.* Namun demikian sistem pertanggungjawaban korporasi belum cukup jelas dan terperinci, khususnya berkaitan dengan kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggungjawab dan sanksi pidana yang dapat dijatuhkan.

Kata Kunci : Cybercrime, Pidana, Kebijakan Penal, ITE.

***ABSTRACT***

*The problems addressed in this study is how to shape the response to cybercrime by means of penal and criminal accountability mechanisms. The method used is the statutory approach, conceptual approach, and comparative approach. Type of research is Normative Legal Research. The results showed that the response to cybercrime by using the policy of criminal law (penal policy) should keep abreast of the times. Therefore the established laws of information and electronic transactions in an attempt to overcome the problems previously associated with regulations on prevention of cybercrime are still scattered in various forms of regulation. Criminal liability under the laws of information and electronic transactions can be imposed on individuals and corporations. However, corporate accountability system is not sufficiently clear and detailed, particularly with regard to the corporation when it is said to be committing a crime, who is responsible and criminal sanctions which can be imposed.*

*Key word : Cybercrime, Criminal, Penal Policy, ITE.*

## 1. Pendahuluan

Kejahatan dunia maya atau dikenal juga dengan istilah *cyber crime* adalah suatu istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer, baik sebagai alat, sasaran atau tempat terjadinya kejahatan. Walaupun kejahatan dunia maya atau *cyber crime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, namun istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana peralatan computer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi [1]. Kejahatan ini dapat dilakukan oleh seseorang dari suatu tempat yang sangat pribadi misalnya di kamar tidur, tapi

menimbulkan kerugian pada seseorang, atau institusi di tempat lain, yang mungkin terpisahkan oleh jarak ribuan kilometer, bahkan seringkali bersifat lintas batas territorial. Dengan demikian kejahatan ini kemudian membawa sifat *transnational crimes,* yaitu kejahatan yang bersifat lintas batas teritorial (*transnational boundaries*).

*Hacking* adalah bentuk pertama dalam kejahatan ini (*first crime*) sebagaimana ditetapkan oleh kongres PBB ke-X di Wina tahun 2000. Hal ini disebabkan bentuk perbuatan ini merupakan sesuatu yang istimewa, karena mempunyai kelebihan dari bentuk *cyber crime* lainnya. Diantaranya adalah bahwa pelaku kejahatan ini sudah barang tentu dapat melakukan *cyber crime* lainnya. Secara teknis imbas dari aktivitas *hacking* menghasilkan kualitas akibat yang lebih serius dibandingkan dengan bentuk *cyber crime* lainnya. Untuk menyebarkan gambar porno atau *cyber pornography,* orang tidak perlu kemampuan *hacking,* namun cukup dengan kemampuan minimal di bidang internet[2].

Berdasarkan pada berbagai unsur perbuatan yang terdapat dalam Pasal 167 ayat (1) dan (2) KUHP, maka akan timbul pertanyaan jika dikaitkan dengan perbuatan *hacking.* Pertanyaan tersebut adalah; apakah sistem komputer seseorang atau sebuah organisasi, atau *website* dalam jaringan komputer (internet) dapat dikategorikan sebagai objek yang diatur dalam Pasal 167 KUHP. Dengan kata lain, apakah dapat disamakan memasuki sistem komputer orang lain dengan memasuki pekarangan atau rumah orang lain?. Apakah menyadap *password* dapat disamakan dengan menggunakan kunci palsu sebagaimana diatur dalam pasal tersebut?. Untuk menjawab pertanyaan tersebut maka hakim harus melakukan penafsiran yang mendalam, yang penggunaanya dalam hukum pidana masih menimbulkan perdebatan.

Model penegakan hukum, yang membutuhkan penafsiran meluas seperti diatas menimbulkan ketidakpuasan dibanyak kalangan. Ketidakpuasan tersebut karena perbedaan persepsi di antara penegak hukum yang menimbulkan diskriminasi dalam penegakan hukum, sampai kepada ancaman pidana dalam pasal-pasal KUHP yang tidak sebanding dengan tingkat kerugian yang ditimbulkan oleh *cyber crime.* Desakan kepada pemerintah untuk segera meregulasi bentuk kejahatan ini akhirnya terjawab ketika pemerintah bersama Dewan Perwakilan Rakyat (DPR) menyetujui untuk memberlakukan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Meski tidak secara khusus merupakan undang-undang tentang *cybercrime,* beberapa pasal dalam undang-undang tersebut mengatur tentang *cybercrime.*

Berdasarkan uraian tersebut di atas, maka permasalahan yang hendak dikaji dalam karya tulis ini adalah bagaimanakah bentuk upaya penanggulangan cybercrime atau kejahatan di bidang computer dengan menggunakan sarana penal serta mekanisme pertanggungjawaban pidananya sebagaimana yang diatur dalam undang-undang informasi dan transaksi elektronik.

## 2. Landasan Teori

Kejahatan dalam bidang teknologi informasi secara umum dapat dikategorikan menjadi dua kelompok. Pertama, kejahatan biasa yang menggunakan teknologi informasi sebagai alat bantunya. Dalam kejahatan ini terjadi peningkatan modus operandi dari semula menggunakan peralatan biasa, sekarang telah memanfaatkan teknologi informasi. Dampak dari kejahatan biasa yang telah menggunakan teknologi informasi ternyata cukup serius, terutama jika dilihat dari segi jangkauan dan nilai kerugian yang ditimbulkan oleh kejahatan tersebut. Pencurian uang dengan pembobolan bank atau pembelian barang menggunakan kartu kredit curian melalui media internet dapat menelan korban di wilayah hukum negara lain, suatu hal yang jarang terjadi dalam kejahatan konvensional. Kedua, kejahatan yang muncul setelah adanya internet, dimana sistem komputer sebagai korbannya. Kejahatan yang menggunakan aplikasi internet adalah salah satu perkembangan dari kejahatan teknologi informasi. Jenis kejahatan dalam kelompok ini makin bertambah seiring dengan kemajuan teknologi informasi. Contoh dari kejahatan kelompok ini adalah perusakan situs internet, pengiriman virus atau program-program komputer yang tujuannya merusak sistem kerja komputer.

Internet (*interconnected Network*) adalah konvergensi telematika yang merupakan perpaduan antara teknologi komputer, media dan teknologi informasi. Internet merupakan jaringan komputer yang terdiri dari ribuan bahkan jutaan jaringan komputer independent yang dihubungkan satu dengan yang lainnya. Jaringan ini dapat dimanfaatkan untuk kepentingan sosial, ekonomi, politik, militer bahkan untuk propaganda maupun terorisme.

Belum ada definisi yang seragam mengenai istilah *cybercrime,* istilah ini banyak banyak dipakai terhadap suatu bentuk kejahatan yang berkaitan dengan dunia virtual dan tindakan kejahatan yang menggunakan sarana komputer. Jenis aktivitas kejahatan yang berkaitan dengan komputer sangat

beragam, sehingga banyak muncul istilah-istilah baru di antaranya: *hacking, cracking, viruses, booting, troyan horse, spamming* dan sebagainya.

### 2.1 Pengaturan tentang *Cybercrime* secara Internasional

Teknologi mutakhir terus diciptakan untuk dapat membantu segala aktivitas manusia agar lebih mudah, cepat, efektif dan efisien dalam melakukan segala aktifitasnya. Teknologi sebagai karya cipta manusia memiliki sisi positif dan sisi negatif. Namun pada dasarnya, teknologi bersifat netral, artinya dampak positif atau negatif itu muncul tergantung tujuan penggunaannya. Internet merupakan produk teknologi abad ini yang sedang berkembang di dunia, termasuk di Indonesia.

Perangkat hukum internasional sudah dibentuk dengan adanya beberarapa kongres-kongres PBB, dan hal tersebut wajib untuk diratifikasi oleh Negara anggota. Langkah yang ditempuh adalah memasukkan *cybercrime* dalam sistem hukumnya masing-masing. Dalam rangka menanggulangi cybercrime, Resolusi Kongres PBB VIII/1990 mengenai *Computer Related Crimes* dan *International Industry Congres (IIIC)* 2000 *Millenium Congres* di *Quebec* pada tanggal 19 September 2000 dan Kongres PBB mengenai *The Prevention of Crime and The Treatment of Offenders*, mengajukan beberapa kebijakan antara lain:

1) Menghimbau Negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan computer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
   a) Melakukan modernisasi hukum pidana meteriil dan hukum acara pidana;
   b) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
   c) Melakukan langkah-langkah untuk membuat warga masyarakat, aparat pengadilan dan penegak hukum sensitive terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer (*cybercrime*);
   d) Memperluas rules of ethics dalam penggunaan computer dan mengajarkannya dalam kurikulum informatika;
   e) Mengadopsi kebijakan perlindungan korban cybercrime sesuai dengan deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya cybercrime.
2) Menghimbau negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan cybercrime.
3) Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*committee on Crime Preventon And Control*) PBB untuk :
   a) Menyebarluaskan pedoman dan standar untuk membantu Negara anggota menghadapi cybercrime di tingkat nasional, regional dan internasional;
   b) Mengembangkan penelitian dan analisa lebih lanjut guna menemukan cara-cara baru menghadapi problem cybercrime di masa depan;
   c) Mempertimbangkan cybercrime sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerjasama di bidang penanggulangan kejahatan.

Berdasarkan definisi yang dikemukakan oleh *The US Supreme Court* bahwa internet disebut sebagai *international Network of interconnected computers, yang* artinya jaringan internasional dari komputer-komputer yang saling berhubungan, sehingga melewati batas-batas territorial suatu Negara [3]. Melalui internet seseorang dapat melakukan beberapa aktivitas secara bersamaan tanpa harus keluar rumah, misalnya berdiskusi, belanja, transfer uang, kuliah dan lain-lain. Hal ini merupakan sisi positif dari internet, namun internet tidak lepas dari sisi negatif berupa pemanfaatannya sebagai media untuk melakukan kejahatan yang dikenal dengan istilah *cyber crime*. Volodymyr Golubev menyebutnya sebagai *"the new form of anti-social behavior"*[4]. Ada beberapa jenis kejahatan ini, misalnya *economic cyber crime, cyber terrorism, cyber stalking, cyber sex* dan *cyberporn.* Hal ini menunjukkan bahwa segala bentuk kejahatan di dunia nyata telah terjadi pula di dunia maya.

Dalam *background paper* lokakarya Kongres PBB X pada tahun 2000 juga memberikan definisi *cybercrime*, akan tetapi membagi definisi tersebut dalam *narrow sense* (*arti sempit*) dan *broader sense* (*arti Luas*), yang menyatakan bahwa:

> *"Cybercrime in narrow sense is Any illegal behavior directed by means of elctronic operations that targets the security of computer systems and the data processed by them". "Cybercrime as a*

*broader sense* adalah *Any illegal behavior commited by means of, or in relation to, a computer system or network, including such crimes is illegal possession, offering or distributing information by means of a computer system or network"*[5].

Istilah "*cybercrime*", "*computer crime*", dan "*high-tech-crime*" seringkali digunakan secara bergantian untuk merujuk kepada dua kategori, dimana suatu perbuatan telah dianggap melawan hukum. Dua kategori itu adalah, pertama, komputer merupakan target bagi perbuatan pelaku. Dalam hal ini pelaku dapat melakukan akses secara illegal, penyerangan kepada jaringan (pembobolan) dan lain lain yang terkait dengan sistem pengamanan jaringan (*networking*). Kategori kedua adalah bahwa perbuatan tersebut mengandung maksud dan tujuan seperti layaknya kejahatan konvensional, misalnya pencurian atau pemalsuan.

Sesuai sifat global internet, ruang lingkup kejahatan ini juga bersifat global. *Cybercrime* seringkali dilakukan secara transnasional, melintasi batas negara sehingga sulit dipastikan yuridikasi hukum negara yang berlaku terhadap pelaku. Karakteristik internet di mana orang dapat berlalu-lalang tanpa identitas *(anonymous)* memungkinkan terjadinya berbagai aktivitas jahat yang tak tersentuh hukum. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain:

1) *Unauthorized Access to Computer System and Service*
2) *Illegal Contents*
3) Data *Forgery*
4) *Cyber Espionage*
5) *Cyber Sabotage and Extortion*
6) *Offense against Intellectual Property*
7) *Infringements of Privacy*

Menurut *Convention on Cybercrime*, tindak pidana yang dapat digolongkan sebagai *cybercrime* diatur dalam Pasal 2-5, adapun jenis tindak pidana tersebut adalah :

1) *Illegal Access*

*Illegal access* melingkupi pelanggaran dasar dari ancaman-ancaman yang berbahaya dari serangan terhadap keamanan data dan sistem computer [6]. Perlindungan terhadap pelanggaran *illegal access* ini merupakan gambaran dari kepentingan organisasi atau kelompok dan orang-orang yang ingin mengatur, menjalankan dan mengendalikan sistem mereka berjalan tanpa ada ganguan dan hambatan.

2) *Illegal Interception*

*Illegal Interception* adalah tindakan tidak sah berupa pencegatan atau menahan tanpa hak bentuk pemindahan data komputer yang dilakukan secara pribadi yang dilakukan melalui faximile, *email*, atau pemindahan *file*. Tujuan dari pasal ini adalah perlindungan atas hak atas kebebasan dalam komunikasi data. Pelanggaran ini hanya ditujukan terhadap pemindahan pribadi dari data komputer.

3) *Data Interception*

*Data Interception* diatur dalam Pasal 4 *Cybercrime Convention*, yang pada dasarnya berkaitan dengan ketentuan pengrusakan data sehingga menjadi tindak pidana. Ketentuan ini bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program komputer sebagaimana dengan benda-benda berwujud. Sebagai contoh adalah memasukan kode-kode jahat (*malicous codes*), *Viruses*, dan *Trojan Horse* ke suatu sistem computer. Hal ini merupakan pelangagaran menurut ketentuan dalam pasal ini.

4) *System Interference*

*System Interference* diatur dalam Pasal 5 *Cybercrime Convention.* Dalam Pasal 5 konvensi ini disebutkan bahwa *system interference* ditetapkan sebagai pelanggaran pidana apabila *"... when committed intentionally, the serious hindering without right of the functioning of a computer system…"*, yang dilakukan dengan memasukkan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer. Gangguan terhadap sistem dijadikan sebagai tindak pidana dengan bertujuan untuk mencegah *"…the serious hindering without right of the functioning of a computer system.."*.

5) *Misuse of Device*

*Misuse of Device* diatur dalam Pasal 6 konvensi ini adapun yang termasuk jenis kejahatan ini adalah pencurian ,penyediaan, penjualan dan distribusi dari data komputer yang diperoleh dari sebuah alat. Sedangkan yang dimaksud sebagai alat adalah *hardware* maupun *software* yang telah di modifikasi untuk mendapatkan akses dari sebuah komputer atau jaringan komputer. Contohnya apabila ada sesorang yang memasukkan *keylogger* dalam jaringan bank untuk mendapatkan data-data nasabah mulai dari alamat sampai ke *password* ATM dan data-data tersebut dijual, digunakan atau didistribusikan untuk kejahatan lain.

### 2.2 Harmonisasi Konvensi Cybercrime Dalam Hukum Nasional

Indonesia sebagai bagian dari negara bangsa di dunia, termasuk sebagai salah satu negara yang cukup banyak memiliki penyalahgunaan dalam pemanfaatan jaringan internet, khususnya dalam hal pemesanan barang-barang atau perdagangan dengan menggunakan media internet [7]. Kondisi ini dapat merugikan pihak Indonesia, khususnya dalam dunia perdangangan melalui internet, karena transaksi internet dengan menggunakan kartu yang dikeluarkan oleh pihak perbankan Indonesia berpotensi untuk ditolak oleh pihak luar negeri.

*European Convention on Cyber Crime* merupakan konvensi tentang *cyber crime* yang disepakati oleh Negara-negara anggota Uni Eropa, namun konvensi ini terbuka bagi Negara lain di luar Uni Eropa untuk mengikutinya. Oleh karena banyak Negara yang mengikuti konvensi tersebut, maka isi perjanjian ini menjadi model bagi banyak pengaturan cyber crime di berbagai negara. Oleh karenanya menjadi penting bagi Indonesia untuk merujuk konvensi ini sebagai salah satu pembanding dalam pengaturan *cyber crime,* terlebih lagi J.E Sahetapy pernah mengemukakan bahwa hukum pidana di Indonesia, belum siap menghadapi kejatahan komputer, karena tidak segampang itu menganggap kejahatan komputer berupa pencurian data sebagai pencurian. Kalau dikatakan pencurian, tentu harus ada barang yang hilang. Padahal dalam kejahatan komputer, data si pemilik masih ada kendati sudah dicuri orang lain [8]. Bagaimana dengan *cybercrime*, tentu tantangan yang dihadapi menjadi lebih berat. Barda Nawawi Arief menyatakan bahwa *cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Ada beberapa faktor yang mempengaruhi terjadinya *cybercrime*, yaitu faktor politik, faktor ekonomi dan faktor sosial budaya [9].

Berbagai bentuk perbuatan *cyber crime* dalam *European Convention on Cyber Crime* yang dapat menjadi rujukan oleh pihak Indonesia dalam pengaturan tentang *Cyber Crime* adalah :

1) Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan system computer, yaitu:
   a) Mengakses system computer tanpa hak (*illegal acces*);
   b) Tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*);
   c) Tanpa hak merusak data (*data interference*);
   d) Tanpa hak mengganggu system (*system interference*);
   e) Menyalahgunakan perlengkapan (*misuse of device*).
2) Delik-delik yang berhubungan dengan computer, pemalsuan, dan penipuan (*computer related pffences; forgery and fraud*);
3) Delik-delik yang bermuatan pornografi anak (*content-related offences, child pornography*);
4) Delik-delik yang berhubungan dengan hak cipta (*offences related of infringements of copyrights*).

Berbagai perbuatan di atas menjadi sandaran untuk menilai pengaturan dalam UU ITE dan menilai sejauhmana terdapat harmonisasi hukum dalam pengaturan tersebut.

## 3. Metode Penelitian

Penelitian ini adalah penelitian hukum (*legal research*) yang mengkaji ketentuan-ketentuan dan prinsip-prinsip hukum yang mengatur tentang Hak Cipta, khususnya yang terkait dengan karya cipta di bidang Komputer. Dalam penelitian ini akan dikaji dan dianalisis secara mendalam keterkaitan antara teori yang melandasi prinsip-prinsip perlindungan hukum, dihubungkan dengan ketentuan-ketentuan sebagaimana yang diatur dalam undang-undang hak cipta. Penelitian ini termasuk dalam kategori tipe penelitian normative atau *Normative Legal Research*. Pendekatan yang digunakan dalam penelitian ini adalah: *statuta approach, conseptual approach,* dan *comparative approach*. Teknik analisis yang digunakan adalah penalaran dan argumentasi hukum untuk menjawab isu-isu penelitian yang diajukan sesuai dengan pendekatan yang digunakan.

## 4. Hasil Penelitian dan Pembahasan

Upaya penanggulangan dan pencegahan kejahatan dapat dilakukan melalui suatu kebijakan kriminal (*criminal policy*) dengan menggunakan sarana “penal” (hukum pidana) dan sarana “non penal”. Sarana penal dikenal dengan kebijakan/politik hukum pidana (*penal policy*). Menurut Sudarto, politik hukum pidana adalah usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang [10]. Sementara menurut Marc Ancel, *penal policy* adalah suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik [11].

Terkait dengan upaya penanggulangan *cybercrime* dengan menggunakan hukum pidana, telah ada Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Tulisan ini akan melihat sejauhmana regulasi ini mampu memberikan peran dalam penanggulangan *cybercrime* di Indonesia. Mulai dari sistem perumusan tindak pidana sampai dengan sistem sanksi pidananya.

Undang-undang tentang Informasi dan Transaksi Elektronik (UU ITE) ini diundangkan pada tanggal 21 April 2008 dalam Lembaran Negara Nomor 58. Dalam sejarahnya, kebijakan hukum pidana sebagai sarana penanggulangan *cybercrime* selama ini masih tersebar diberbagai peraturan perundang-undangan yang lebih bersifat sektoral dan memiliki keterbatasan, misalnya dalam Undang-Undang Telekomunikasi dan Undang-Undang Pers. Keluarnya Undang-Undang Nomor 11 tahun 2008 ini diharapkan mampu menjawab segala tantangan hukum dalam penanggulangan *cybercrime* di Indonesia.

### 4.1 Jenis Kejahatan Komputer

Kejahatan komputer dan siber bukanlah kejahatan yang sederhana [12]. Jika dilihat dalam peraturan perundang-undangan yang konvensional, maka ketentuan pidana yang dapat digunakan di bidang komputer adalah ketentuan tentang penipuan, kecurangan, pencurian dan pengrusakan, yang pada pokoknya dilakukan secara langsung dengan menggunakan bagian tubuh secara phisik dan pikiran oleh si pelaku. Jika hal tersebut dikaji dengan menggunakan kriteria peraturan hukum pidana konvensional, maka kejahatan komputer dapat berbentuk sebagai berikut:

1. Penipuan komputer (*computer fraud*) yang mencakup :
    a. Bentuk dan jenis penipuan adalah berupa pencurian uang atau harta benda dengan menggunakan sarana computer yang dilakukan secara melawan hukum. Bentuk penipuan dalam hal ini biasanya dilakukan dengan cara:
        1) memasukkan instruksi yang tidak sah. Tindakan ini dapat dilakukan oleh seorang yang berwenang atau tidak, dengan mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri secara melawan hukum (misalnya transfer uang).
        2) Mengubah data input, yang dilakukan seseorang dengan cara memasukkan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum, misalnya memasukkan data gaji pegawai melebihi yang seharusnya.
        3) Merusak data, yaitu dilakukan oleh seseorang untuk merusak print-out atau output dengan maksud untuk mengaburkan, menyembunyikan data atau informasi dengan itikad tidak baik.
        4) Penggunaan komputer sebagai sarana untuk melakukan perbuatan pidana, yaitu dalam bentuk pemecahan informasi melalui komputer yang hasilnya digunakan untuk melakukan kejahatan, atau mengubah program.
    b. Perbuatan pidana penipuan, sesungguhnya dapat pula termasuk unsur perbuatan lain, yang pada pokoknya dimaksudkan menghindarkan diri dari kewajiban, misalnya pajak atau untuk memperoleh sesuatu yang bukan hak/miliknya melalui sarana komputer.
    c. Perbuatan curang untuk memperoleh secara tidak sah harta benda milik orang lain, misalnya seseorang yang dapat mengakses komputer mentransfer rekening orang ke rekeningnya sendiri, sehingga merugikan orang lain.
    d. Konspirasi penipuan, ialah perbuatan pidana yang dilakukan beberapa orang secara bersama-sama untuk melakukan penipuan dengan sarana komputer.
    e. Pencurian adalah perbuatan yang dengan sengaja mengambil secara melawan hukum hak atau milik orang lain dengan maksud untuk dimilikinya sendiri.
2. Perbuatan pidana penggelapan, pemalsuan pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri.
3. Hacking, ialah melakukan akses terhadap sistem komputer tanpa seizin atau dengan melawan hukum sehingga dapat menembus sistem pengamanan komputer yang dapat mengancam berbagai kepentingan.
4. Perbuatan pidana terkait dengan komunikasi, yaitu hacking yang dapat membobol sistem on-line komputer yang menggunakan sistem komunikasi.
5. Perbuatan pidana perusakan sistem komputer, baik merusak data atau menghapus kode-kode yang menimbulkan kerusakan dan kerugian. Termasuk dalam golongan perbuatan ini adalah berupa penambahan atau perubahan program, informasi, media, sehingga merusak sistem, demikian pula dengan sengaja menyebarkan virus yang dapat merusak program dan sistem komputer, atau pemerasan dengan menggunakan sarana komputer atau system telekomunikasi lainnya.

6. Perbuatan pidana yang berkaitan dengan hak milik intelektual, hak cipta, dan hak paten, ialah berupa pembajakan dengan memproduksi barang-barang tiruan untuk mendapatkan keuntungan melalui perdagangan.

Jenis perbuatan pidana tersebut pada dasarnya dapat berlaku jika komputer dihubungkan dengan teknologi telekomunikasi dan informasi, sehingga menjadi kejahatan siber, terutama dengan berkembangnya teknologi internet.

### 4.2 Tindak Pidana dalam UU ITE

Undang-Undang ITE berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan yang berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif untuk melakukan perbuatan melawan hukum.

Berdasarkan hal tersebut di atas, maka telah lahir suatu rezim hukum baru yang dikenal dengan istilah hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi *(law of information technology)*, hukum dunia maya *(virtual world law)*, dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik dan dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input, process, output, storage,* dan *communication*.

Sehubungan dengan itu, maka penting sekali artinya bagi dunia hukum untuk memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelanjaan di Internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia

dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit.

Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber *(cyber space)*, meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai Orang yang telah melakukan perbuatan hukum secara nyata. Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan di *cyber space*, yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

Ketentuan tindak pidana dalam UU ITE diatur dalam Bab XI dari Pasal 45 s/d Pasal 52. Adapun unsur-unsur tindak pidana dalam ketentuan pidana tersebut adalah :

1) Pasal 45 ayat (1) jo Pasal 27 ayat (1), (2), (3) atau (4) : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
2) Pasal 45 ayat (1) jo Pasal 27 ayat (2) : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian
3) Pasal 45 ayat (1) jo Pasal 27 ayat (3) : 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) Pasal 45 ayat (1) jo Pasal 27 ayat (4) : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.
5) Pasal 45 ayat (2) jo Pasal 28 ayat (1) : menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
6) Pasal 45 ayat (2) jo Pasal 28 ayat (2) : menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).
7) Pasal 45 ayat (3) jo Pasal 29 : mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
8) Pasal 46 ayat (1) jo Pasal 30 ayat (1) : mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun
9) Pasal 46 ayat (1) jo Pasal 30 ayat (2) : mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik
10) Pasal 46 ayat (1) jo Pasal 30 ayat (3) : mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.
11) Pasal 47 jo Pasal 31 ayat (1) : melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain.
12) Pasal 47 jo Pasal 31 ayat (2) : 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.
13) Pasal 48 ayat (1) jo Pasal 32 ayat (1) : 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.
14) Pasal 48 ayat (1) jo Pasal 32 ayat (2) : dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
15) Pasal 48 ayat (1) jo Pasal 32 ayat (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.

16) Pasal 49 ayat (1) jo Pasal 33 : melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.
17) Pasal 50 jo Pasal 34 ayat (1) : memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki :
    a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
    b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
18) Pasal 51 ayat (1) jo Pasal 35 : melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
19) Pasal 51 ayat (2) jo Pasal 36 : melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.
20) Pasal 52 ayat (1) : Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.
21) Pasal 52 ayat (2) : Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.
22) Pasal 52 ayat (3) : Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.
23) Pasal 52 ayat (4) : Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

Rumusan ketentuan pidana dalam undang-undang ITE menyebutkan secara tegas adanya unsur *"sifat melawan hukum"* yang terlihat pada rumusan "*tanpa hak atau melawan hukum*". Sebenarnya tanpa disebutkan/ditegaskan, pada prinsipnya setiap delik harus dianggap bertentangan dengan hukum, sebagaimana ide dasar yang terkandung dalam Pasal 11 ayat (3) Konsep KUHP 2005. Sementara rumusan '*dengan sengaja*' juga dicantumkan secara tegas, sehingga jelas ada unsur kesengajaan (*dolus*) yang berarti menganut asas kesalahan atau *asas culpabilitas*. Sama halnya dengan sifat melawan hukum, pada prinsipnya tindak pidana melalui unsur-unsurnya dilakukan dengan kesengajaan kecuali dinyatakan secara tegas sebagai kealpaan. Hal ini sebagaimana ide dasar yang terkandung dalam Konsep KUHP 2005 Pasal 39 ayat (2).

Beberapa bentuk kriminalisasi dalam ketentuan pidana di atas diantaranya melalui dunia maya melakukan tindak pidana kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan/pengancaman, menyebarkan berita bohong dan informasi yang bermuatan SARA, mengakses data orang lain tanpa hak, atau menjebol sistem keamanan pihak lain. Disamping itu ada pula kriminalisasi yang mengandung pemberatan pidana, seperti tindak pidana kesusilaan terhadap anak dalam Pasal 27 ayat (1) Pidananya ditambah sepertiga dari pidana pokoknya. Begitu pula bagi korporasi yang melakukan tindak pidana dalam Pasal 27 sampai dengan Pasal 37 pidana pokoknya ditambah dua pertiga.

Gambar 1. Alur Persidangan Perkara Pidana

### 4.3 Sistem Pertanggungjawaban Pidana

Pertanggungjawaban pidana dalam Undang-Undang ITE dapat dijatuhkan kepada *individu* dan *korporasi.* Hal ini terlihat dari subjek tindak pidana yang terkandung dalam ketentuan pidananya, yaitu setiap orang. Pengertian orang dalam Ketentuan Umum Pasal 1 ayat (21) adalah *orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum*. Bahkan secara eksplisit, pertanggungjawaban korporasi dalam tindak pidana UU ITE disebutkan secara tegas dalam Pasal 52 ayat(4).

Dalam Undang-Undang ITE, korporasi juga merupakan subjek tindak pidana. Maka seharusnya diatur pula sistem pertanggungjawaban korporasi yang jelas dan terperinci, khususnya berkaitan dengan kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggungjawab dan sanksi pidana yang dapat dijatuhkan. Namun dalam undang-undang ini justru tidak diatur mengenai tiga hal pokok tersebut. Terkait sanksi pidana misalnya, hanya disebutkan pidana pokoknya ditambah dua pertiga. Tidak diatur jenis sanksi lain yang lebih tepat bagi korporasi, seperti tindakan tata tertib penutupan sementara atau selamanya.

Ketentuan pidana dalam Undang-Undang ITE menganut sistem perumusan alternatif-kumulatif. Hal ini terlihat dengan digunakannya rumusan "*…dan/atau…*", kecuali pada Pasal 52 yang sifatnya mengandung pemberatan pidana. Sementara untuk jenis sanksi *(strafsoort)* pidananya ada 2 (dua) jenis, yaitu pidana penjara dan pidana denda. Kedua jenis sanksi tersebut diancamkan untuk semua jenis kejahatan, baik dilakukan oleh individu maupun korporasi. Padahal terhadap korporasi tentunya tidak dapat dikenakan pidana penjara. Ditetapkannya korporasi sebagai subjek tindak pidana, seyogyanya hanya diancam pidana denda dan pidana tambahan/administrasi/tindakan tata tertib. Adapun Sistem perumusan jumlah/lamanya pidana (*strafmaat*) dalam Undang-Undang ITE adalah sistem maksimum khusus, yaitu maksimum khusus untuk pidana penjara berkisar antara 6 tahun sampai dengan 12 tahun

dan maksimum khusus untuk pidana denda berkisar antara Rp 600.000.000,- sampai dengan Rp 12.000.000.000,-

## 5. Kesimpulan

Bentuk upaya penanggulangan cybercrime atau kejahatan di bidang computer dengan menggunakan sarana penal adalah dengan menggunakan kebijakan/politik hukum pidana (*penal policy*) yang lebih sesuai dengan keadaan dan situasi pada suatu saat sekarang dan untuk masa-masa yang akan datang. Oleh karena itu dibentuklah Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Hal ini dimaksudkan untuk mengatasi permasalahan sebelumnya terkait dengan pengaturan tentang penanggulangan *cybercrime* yang masih tersebar diberbagai peraturan perundang-undangan yang berlaku. Pengaturan tersebut lebih bersifat sektoral dan memiliki keterbatasan, misalnya dalam Undang-Undang Telekomunikasi dan Undang-Undang Pers. Pertanggungjawaban pidananya sebagaimana yang diatur dalam undang-undang informasi dan transaksi elektronik dapat dijatuhkan kepada *individu* dan *korporasi.* Namun demikian sistem pertanggungjawaban korporasi belum cukup jelas dan terperinci, khususnya berkaitan dengan kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggungjawab dan sanksi pidana yang dapat dijatuhkan.

## DAFTAR PUSTAKA


[1] Widodo, 2009. *Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime*, Laksbang Mediatama, Yogyakarta.

[2] Akbar Kurnia Putra, 2014. *Harmonisasi Konvensi Cybercrime dalam Hukum Nasional*. Jurnal Hukum Fakultas Hukum Universitas Jambi.

[3] Abdul Wahid dan Mohammad Labib, 2005. *Kejahatan Mayantara (Cybercrime)*, Refika Aditama, Bandung.

[4] Volodymyr Golubev, *Cyber-crime and legal problems of Internet usage*, p.1; Zaporizhia Law Institute, Ministry of Interior of Ukraine.

[5] Barda Nawawi Arief, 2006. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia.* PT. Rajagrafindo Persada, Jakarta.

[6] Council of Europe, *Explanatory Report To The Convention on Cybercrime* (ETS No 185), poin ke 44.

[7] Ilhamd Wahyudi (2006). *Kebijakan Pidana Terhadap Kejahatan Mayantara*. Tesis. Program Pascasarjana Unand-Unri. Padang, hlm 5.

[8] Widyopramono, 1994. *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta.

[9] Sutarman, 2007. *Cybercrime (Modus Operandi dan Penanggulangannya)*, LaksBang Pressindo, Yogyakarta.

[10] Sudarto, 1983. *Hukum Pidana dan Perkembangan Masyarakat "Kajian Terhadap Pembaharuan Hukum Pidana***.** Sinar Baru, Bandung.

[11] Barda Nawawi Arief, 1996. *Bunga Rampai Kebijakan Hukum Pidana*, PT Citra Aditya Bakti, Bandung.

[12] David I. Bainbridge, 1993. Komputer dan Hukum, terjemahan dari Computer and the Law, Cetakan I PT. Sinar Grafika. Jakarta.