Penegakan Hukum Terhadap Kejahatan Di Bidang Teknologi Informasi

Abdul Rauf[*1]
[1]Jurusan Sistem Informasi
Universitas Dipa Makassar
e-mail: *[1]abdulrauf.wa@gmail.com

Abstrak

Permasalahan dalam tulisan ini adalah tentang substansi hukum (legal substancy) di bidang teknologi informasi, khususnya kejelasan mengenai pasal-pasal maupun peraturan-peraturan lain yang mengatur tentang kejahatan di bidang teknologi informasi. Hal ini penting untuk menghindari timbulnya kesulitan bagi aparat penegak hukum dalam menerapkan pasal-pasal tersebut terhadap peristiwa konkrit yang timbul di masyarakat. Penelitian ini adalah penelitian hukum (legal research) yang mengkaji ketentuan-ketentuan dan prinsip-prinsip hukum yang mengatur tentang tindak pidana atau kejahatan di bidang teknologi informasi, baik melalui media internet maupun yang dikirim melalui fasilitas elektronik lainnya. 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.

Hasil pembahasan menunjukkan bahwa masih perlu pengaturan-pengaturan yang lebih jelas dan spesifik terkait dengan penegakan hukum terhadap kejahatan yang timbul di bidang teknologi Informasi, khususnya kejahatan-kejahatan yang timbul setelah adanya internet, dimana sistem komputer sebagai sasarannya, seperti hacking, cracking, viruses, booting, troyan horse, maupun spamming. Kejelasan ini sangat penting terutama berkaitan dengan substansi aturan atau ketentuan perundang-undangan yang mengatur tentang tindak pidana di bidang teknologi Informasi.Upaya penegakan hukum terhadap kejahatan di bidang teknologi Informasi tetap didasarkan pada hukum acara formal sebagaimana yang diatur dalam KUHAP. Hal ini sesuai pula dengan ketentuan Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kata kunci— Hukum, Kejahatan, Teknologi, Informasi, Cybercrime.

Abstract

The problem in this paper is about legal substance in the field of information technology, especially the clarity regarding the articles and other regulations that regulate crimes in the field of information technology. This is important to avoid the emergence of difficulties for law enforcement officials in applying these articles to concrete events that arise in society. This research is a legal research that examines the provisions and legal principles governing criminal acts or crimes in the field of information technology, both via the internet and sent via other electronic facilities. The approaches used in this research are: statutory approach, conceptual approach, and comparative approach. The analysis technique used is legal reasoning and argumentation to answer the proposed research issues according to the approach used.

The results of the discussion show that there is still a need for clearer and more specific regulations related to law enforcement against crimes that arise in the field of information technology, especially crimes that arise after the existence of the internet, where computer systems are the target, such as hacking, cracking, viruses, booting, trojan horses, and spamming. This clarity is very important, especially with regard to the substance of the rules or statutory provisions governing criminal acts in the field of information technology. Law enforcement efforts against crimes in the field of information technology are still based on formal procedural law as regulated in the Criminal Procedure Code. This is also in accordance with the provisions of Article 42 of Law Number 11 of 2008 concerning Information and Electronic Transactions.

Keywords— *Law, Crime, Technology, Information, Cybercrime.*

1. Pendahuluan

Hukum di bidang teknologi informasi termasuk dalam kerangka hukum telematika. Perkembangan aspek-aspek telematika bergerak begitu cepat mengikuti perubahan dunia. Aspek-aspek tersebut terus menyesuaikan diri dalam praktik secara substansial, sementara dari sisi aturan main cenderung kurang signifikan, sehingga peran pemerintah dalam hal ini menjadi sangat penting untuk merumuskan kerangka akomodatif terhadap setiap masalah yang dihadapi[1]. Aturan hukum tentang telematika atau sistem informasi pada umumnya akan menjadi landasan bagi para aparat penegak hukum dalam menjalankan tugasnya untuk menegakkan hukum di tengah-tengah masyarakat.

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 [2]. 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.

Kejahatan atau tindak pidana yang dilakukan melalui dunia maya atau internet disebut dengan istilah cyber crime. Dalam hal ini, cyber crime adalah bentuk perbuatan kriminal yang menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakannya[3]. Jadi, cybercrime merupakan bentuk kriminal yang menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakan kriminal. Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Bagi sebagian kalangan, kejahatan siber ini hanya dalam ruang lingkup kejahatan penipuan, hacker, penyebaran berita palsu maupun penyebaran suatu hal yang mengandung unsur pornografi, tetapi bukan hal tersebut saja yang dapat dikatakan sebagai Cybercrime, karena banyak sekali bentuk kejahatan lain yang masih asing dan termasuk dalam kategori Cyber Crime[4].

Istilah Cybercrime juga digunakan untuk jenis kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. Salah satu jenis kejahatan tersebut adalah penipuan yang dilakukan secara online. Penipuan online yang dimaksud adalah penipuan yang menggunakan media internet, baik untuk keperluan bisnis dan perdagangan sehingga tidak lagi mengandalkan basis perusahaan yang konvensional secara nyata[5], termasuk jenis penipuan lain yang umumnya berkedok undian berhadiah. Penipuan sendiri memiliki arti sebagai penyalahgunaan dalam pengiriman berita elektronik untuk menampilkan berita-berita tertentu, iklan atau informasi lainnya yang mengakibatkan ketidaknyamanan atau kerugian bagi pengguna web. Penipuan ini biasanya datang dengan cara bertubi-tubi tanpa diminta dan tidak dikehendaki oleh korbannnya.

Secara umum permasalahan yang timbul dalam upaya penegakan hukum di bidang komputer dapat dibagi atas tiga macam yaitu permasalahan pada aspek sustansi, struktur yang melibatkan aparatur penegak hukumnya dan permasalahan yang terkait dengan budaya hukum masyarakat Indonesia. Menurut Lawrence M.Friedman bahwa sistem hukum terdiri atas tiga komponen, yaitu struktur (legal structur), substansi (legal substancy), dan Budaya (legal cultur) [6].

Substansi hukum (legal substancy) adalah output dari sistem hukum, yang berupa peraturan-peraturan, keputusan-keputusan yang digunakan baik oleh pihak yang mengatur maupun yang diatur. Komponen berikutnya adalah struktur hukum (legal structur), merupakan kelembagaan yang diciptakan oleh sistem hukum itu dengan berbagai macam fungsi dalam rangka mendukung bekerjanya sistem tersebut. Komponen ini dimungkinkan untuk melihat bagaimana sistem hukum itu memberikan pelayanan terhadap penggarapan bahan-bahan hukum secara teratur. Sedangkan Budaya hukum (legal cultur) terdiri dari nilai-nilai dan sikap yang mempengaruhi bekerjanya hukum, atau oleh Friedman disebut sebagai kultur hukum. Kultur hukum inilah yang berfungsi sebagai jembatan yang menghubungkan antara peraturan hukum dengan tingkah laku hukum seluruh warga masyarakat.

Friedman mengungkapkan bahwa hukum harus diartikan sebagai suatu isi hukum (content of law), tata laksana hukum (structure of law) dan budaya hukum (culture of law). Sehingga, penegakan hukum tidak saja dilakukan melalui perundang-undangan, namun juga bagaimana memberdayakan aparat dan fasilitas hukum. Juga, yang tak kalah pentingnya adalah bagaimana menciptakan budaya hukum masyarakat yang kondusif untuk penegakan hukum.

Namun demikian, pokok permasalahan yang dibahas dalam tulisan ini terbatas pada permasalahan yang terkait dengan substansi hukum (legal substancy) khususnya menyangkut kejelasan rumusan pasal-pasal dalam undang-undang maupun peraturan-peraturan lain yang mengatur tentang kejahatan yang timbul di bidang teknologi informasi. Hal ini penting untuk menghindari adanya kesulitan bagi aparat penegak hukum dalam menerapkan pasal-pasal tersebut terhadap peristiwa konkrit yang timbul di masyarakat.

2. Metode Penelitian

Penelitian ini adalah penelitian hukum (legal research) yang mengkaji ketentuan-ketentuan dan prinsip-prinsip hukum yang mengatur tentang tindak pidana atau kejahatan di bidang teknologi informasi, khususnya yang dilakukan secara online melalui media internet maupun yang dikirim melalui fasilitas elektronik lainnya. Dalam penelitian ini akan dikaji dan dianalisis tentang teori yang melandasi prinsip-prinsip penegakan hukum terhadap kejahatan di bidang teknologi informasi yang dihubungkan dengan ketentuan-ketentuan sebagaimana yang diatur dalam undang-undang, baik berdasarkan KUHP maupun berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Data yang digunakan dalam penelitian ini dikumpulkan secara daring (online library research). Penelitian ini termasuk dalam kategori tipe penelitian normatif 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.

3. Hasil dan Pembahasan

Teknologi informasi adalah suatu teknologi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan pemerintahan dan juga merupakan informasi yang strategis untuk pengambilan keputusan. Teknologi ini menggunakan seperangkat komputer untuk mengolah data, sistem jaringan untuk menghubungkan satu komputer dengan komputer yang lainnya sesuai dengan kebutuhan dan teknologi telekomunikasi digunakan agar data dapat disebar dan diakses secara global.[7]

Di era globalisasi, perkembangan teknologi informasi dan komunikasi telah mengakibatkan semakin derasnya lalu lintas informasi. Akibatnya, akses terhadap informasi dan komunikasi semakin mudah didapatkan oleh setiap orang tanpa ada hambatan ruang dan waktu. Globalisasi dalam dunia ekonomi khususnya dunia perdagangan adalah salah satu aspek kehidupan yang mendapatkan imbas dari kehadiran media komunikasi yang cepat dan handal sehingga aktifitas bisnis diberbagai negara cenderung meningkat.[8] Penggunaan Teknologi informasi inilah yang kemudian menjadi sarana bagi timbulnya berbagai macam kejahatan yang disebut dengan istilah *cybercrime* yaitu suatu bentuk kejahatan yang timbul di bidang teknologi informasi.

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 dan operandinya dari semula menggunakan peralatan biasa, sekarang telah memanfaatkan teknologi informasi. Dampak dari kejahatan biasa yang telah menggunakan teknologi informasi ternyata berdampak cukup serius, terutama jika dilihat dari 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.[9]

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.

Internet merupakan sebuah ruang informasi dan komunikasi yang menembus batas-batas yurisdiksi antar Negara. Sebuah media yang menawarkan beragam kemudahan-kemudahan bertransaksi tanpa mempertemukan para pihak secara fisik atau materiil. Internet telah membawa kita ke dalam dunia baru yang disebut *cyberspace*, yang dalam perkembangannya tidak hanya membawa efek positif tetapi juga sarat dampak negatif.

Cyberspace sebagai wahana komunikasi yang berbasis computer (*computer mediated communication*), banyak menawarkan realitas baru dalam berinteraksi dalam dunia maya. Adanya interaksi antar pengguna *cyberspace* telah banyak terseret ke arah terjadinya penyelewengan hubungan sosial berupa kejahatan yang khas yang memiliki karakteristik berbeda dengan tindak pidana konvensional yang selama ini sudah dikenal. Namun ada juga yang berpandangan bahwa kejahatan melalui internet (*cybercrime*) memiliki kesamaan bentuk dengan kejahatan yang ada di dunia nyata.[10]

Namun demikian, belum ada definisi yang seragam mengenai istilah *cybercrime*[11], 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 lain sebagainya.

3.1. Jenis-Jenis Kejahatan di Bidang Komputer

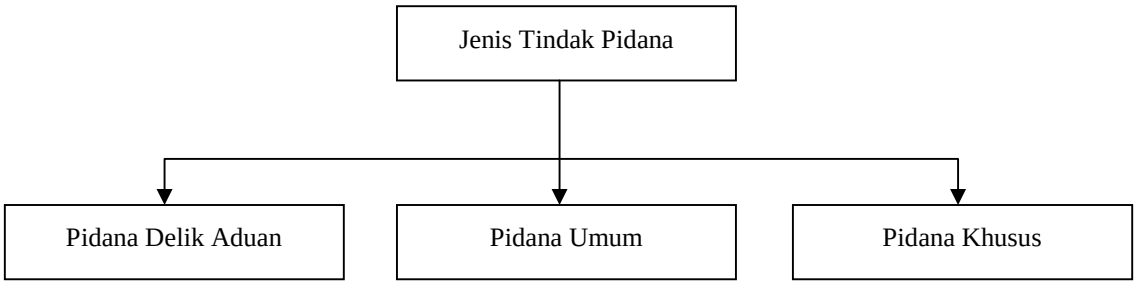
Kejahatan komputer dan siber bukanlah kejahatan yang sederhana. Jika dilihat dalam peraturan perundang-undangan yang konvensional, maka perbuatan pidana yang dapat digunakan di bidang komputer dan siber adalah penipuan, kecurangan, pencurian dan perusakan, yang pada pokoknya dilakukan secara langsung (dengan menggunakan bagian tubuh secara phisik dan pikiran) oleh si pelaku, dan jika hal tersebut dikaji dengan menggunakan kriteria peraturan hukum pidana konvensional, maka kejahatan komputer atau kejaatan siber secara substansial dapat berupa:

1) Penipuan komputer (*computer fraud*) yang mencakup :
   a. Bentuk dan jenis penipuan adalah berupa pencurian uang atau harta benda dengan menggunakan sarana komputer/siber dengan melawan hukum, ialah dalam bentuk penipuan data dan penipuan program, yang secara terinci adalah:
      i. Memasukkan instruksi yang tidak sah, ialah dilakukan oleh seorang yang berwenang atau tidak, yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (misalnya transfer).
      ii. 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).
      iii. Merusak data, ialah dilakukan seseorang untuk merusak print-out atau output dengan maksud untuk mengaburkan, menyembunyikan data atau informasi dengan itikad tidak baik.
      iv. Penggunaan komputer untuk sarana melakukan perbuatan pidana, ialah dalam pemecahan informasi melalui komputer yang hasilnya digunakan untuk melakukan kejahatan, atau mengubah program.
   b. Perbuatan pidana penipuan, yang sesungguhnya dapat 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 bersama-sama untuk melakukan penipuan dengan sarana komputer.
e. Pencurian ialah dengan sengaja mengambil dengan 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 komunikasi, ialah 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 sengaja menyebarkan virus yang dapat merusak program dan sistem komputer, atau pemerasan dengan meng-gunakan sarana komputer/telekomunikasi.
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 kejahatan tersebut pada dasarnya dapat berlaku jika komputer dihubungkan dengan teknologi telekomunikasi dan informasi, sehingga menjadi kejahatan siber, terutama dengan berkembangnya teknologi internet.



Bagan 1. Jenis Tindak Pidana

Mengingat bahwa karena karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja, maka dalam rangka melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik, diperlukan penegasan mengenai peran Pemerintah.

Peran pemerintah ini dimaksudkan untuk mencegah penyebarluasan konten illegal dengan melakukan tindakan pemutusan akses terhadap Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum agar tidak dapat diakses dari yurisdiksi Indonesia serta dibutuhkan kewenangan bagi penyidik untuk meminta informasi yang terdapat dalam Penyelenggara Sistem Elektronik untuk kepentingan penegakan hukum tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

3.2. Dasar Hukum Dalam Menangani Kejahatan di Bidang Komputer

Ketentuan-ketentuan mengenai *cybercrime* dalam KUHP masih bersifat global, namun berdasarkan tingkat kemungkinan terjadinya kasus dalam dunia maya (*cyberspace*) dan kategorisasi kejahatan *cyber* menurut *draft convention on cyber crime* maupun pendapat para ahli. Beberapa bentuk perbuatan pidana terkait bidang teknologi informasi yang diatur dalam KUHP, antara lain:

1) Ketentuan yang berkaitan dengan delik pencurian;
2) Ketentuan yang berkaitan dengan perusakan/ penghancuran barang;
3) Ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain;

a. Ketentuan yang Berkaitan dengan Delik Pencurian

Delik tentang pencurian dalam dunia maya termasuk salah satu delik yang paling sering diberitakan di media masa. Pencurian disini tidak diartikan secara konvensional karena barang yang dicuri adalah berupa data digital, baik yang berisikan data transaksi keuangan milik orang lain maupun data yang menyangkut *software* (program) ataupun data yang menyangkut hal-hal yang bersifat rahasia.Delik pencurian di atur dalam Pasal 362 KUHP dan variasinya diatur dalam Pasal 363 KUHP, yakni tentang pencurian dengan pemberatan; Pasal 364 KUHP tentang pencurian ringan, Pasal 365, tentang pencurian yang disertai dengan kekerasan; Pasal 367 KUHP, tentang pencurian di lingkungan keluarga. Pasal 362 KUHP menyatakan bahwa :

"Barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak Sembilan ratus rupiah".

Menurut hukum pidana, pengertian benda diambil dari penjelasan Pasal 362 KUHP yaitu segala sesuatu yang berwujud atau tidak berwujud seperti listrik, dan mempunyai nilai di dalam kehidupan ekonomi dari seseorang. Data atau program yang tersimpan di dalam media penyimpanan disket atau sejenisnya yang tidak dapat diketahui wujudnya dapat berwujud dengan cara menampilkan pada layar penampil komputer (*screen*) atau dengan cara mencetak pada alat pencetak (printer). Dengan demikian data atau program komputer yang tersimpan dapat dikategorikan sebagai benda seperti pada penjelasan Pasal 362 KUHP.

Menurut pengertian *computer related crime*, pengertian mengambil adalah dalam arti meng-copy data atau program yang tersimpan di dalam suatu disket dan sejenisnya ke disket lain dengan cara memberikan instruksi-instruksi tertentu pada komputer sehingga data atau program yang asli masih utuh dan tidak berubah dalam posisi semula. Menurut penjelasan pasal 362 KUHP, barang yang sudah diambil dari kekuasaan pemiliknya itu, juga harus berindah dari tempat asalnya, padahal dengan mengambil adalah melepaskan kekuasaan atas benda itu dari pemiliknya untuk kemudian dikuasai dan perbuatan itu dilakukan dengan sengaja dengan maksud untuk dimiliki sendiri, sehingga perbuatan mengcopy yang dilakukan dengan sengaja tanpa ijin dari pemiliknya dapat dikategorikan sebagai perbuatan "mengambil" sebagaimana yan dimaksud dengan penjelasan Pasal 362 KUHP.Dalam sistem jaringan (*network*), peng-copy-an data dapat dilakukan secara mudah tanpa harus melalui izin dari pemilik data. Hanya sebagian kecil saja dari data internet yang tidak dapat "diambil" oleh para pengguna internet. Pencurian bukan lagi hanya berupa pengambilan barang/benda berwujud saja, tetapi juga termasuk pengambilan data secara tidak sah. Penggunaan fasilitas *Internet Service Provider* (ISP) untuk melakukan kegiatan *hacking* erat kaitannya dengan delik pencurian yang diatur dalam Pasal 362 KUHP. Pencuri biasanya lebih mengutamakan memasuki sistem jaringan perusahaan financial, misalnya: penyimpanan data kartu kredit, situs-situs belanja *on-line* yang ditawarkan di media internet dan data yang didapatkan secara melawan hukum itu diharapkan memberi keuntungan bagi pelaku.

b. Ketentuan yang Berkaitan dengan Kejahatan Perusakan dan Penghancuran Barang

Ketentuan ini erat dengan kejahatan *hacking*. Dalam kejahatan mayantara (*cybercrime*) perbuatan perusakan dan penghancuran barang ini tidak hanya ditujukan untuk merusak/menghancurkan media disket atau media penyimpan sejenis lainnya, namun juga merusak dan menghancurkan suatu data, *web site* ataupun *homepage*. Delik ini juga termasuk di dalamnya perbuatan merusak barang-barang milik publik (*crime against public property*). Ketentuan mengenai perbuatan perusakan, penghancuran barang diatur dalam Pasal 406-412 KUHP. Pasal 406 KUHP mengatur bahwa :

(1) Barangsiapa dengan sengaja melawan hukum menghancurkan, merusakkn, membikin tidak dapat dipakai lagi atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana dipenjara paling lama dua tahun delapan bulan atau denda paling banyak empat ribu lima ratus rupiah;

(2) Dijatuhkan pidana yang sama terhadap orang, yang dengan sengaja dan melawan hukum membunuh, merusakkan, membuat tidak dapat digunakan atau menghilangkan hewan yang seluruhnya atau sebagian adalah kepunyaan orang lain. Pengertian-pengertian dalam Pasal 406 KUHP dapat dijelaskan sebagai berikut:

Pengertian "menghancurkan" (*vermielen*) atau membinasakan dimaksudkan sebagai merusak sama sekali sehingga suatu barang tidak dapat berfungsi sebagaimana mestinya. Pengertian "merusakkan" dimaksudkan sebagai memperlakukan suatu barang sedemikian rupa namun kurang dan membinasakan (*beschacdingen*). Misalnya: perbuatan merusak data atau program komputer yang terdapat di internet dengan cara menghapus data atau program, membuat cacat data atau program, menambahkan data baru ke dalam suatu situs (*web*) atau sejenisnya secara acak. Dengan kata lan, perbuatan tersebut mengacaukan isi media penyimpannnya.

Pengertian "membikin/membuat tidak dapat dipakai lagi". Tindakan itu harus sedemikian rupa, sehingga barang itu tidak dapat diperbaiki lagi. Kaitannya dengan *cybercrime* adalah perbuatan yang dilakukan tersebut menyebabkan data atau program yang tersimpan dalam media penyimpan (*data base*) atau sejenisnya menjadi tidak dapat dimanfaatkan (tidak berguna lagi). Hal ini disebabkan oleh data atau program telah dirubah sebagian atau seluruhnya, atau dirusak pada suatu bagian atau seluruhnya, atau dihapus pada sebagian atau seluruhnya. Pengertian "menghilangkan" Adalah membuat barang itu tidak ada lagi. Kaitannya dengan *cybercrime* yakni perbuatan mengilangkan atau menghapus data yang tersimpan pada data base –bisa juga tersimpan dalam suatu web- atau sejenisnya sehingga mengakibatkan semua atau sebagian dari data atau program menjadi hapus sama sekali.

Berdasarkan pengertian-pengertian tersebut di atas, dapat dipahami bahwa makna dalam perbuatan-perbuatan tersebut tedapat kesesuaian yang pada intinya menyebabkan fungsi data atau program dalam suatu jaringan menjadi berubah/berkurang. Perbuatan penghancuran atau perusakan barang yang dilakukan *cracker* dengan kemampuan *hacking*-nya bukanlah perbuatan yang bisa dilakukan oleh semua orang awam. Kemampuan tersebut dimiliki secara khusus oleh orang-orang yang mempunyai keahlian dan kreatifitas dalam memanfaatkan sistem, program, maupn jaringan. Motif untuk kejahatan ini sangat beragam yakni misalnya motif ekonomi, politik, pribadi atau motif kesenangan semata.

c. Ketentuan yang Berkaitan dengan Perbuatan Memasuki atau Melintasi Wilayah Orang Lain

Kehadiran internet tidak dapat dielakkan lagi dapat menunjang kerja dari komputer sehingga dapat mengolah data yang bersifat umum melalui suatu *terminal system*. Apabila ada orang asing yang masuk ke dalam jaringan komputer tersebut tanpa ijin dari pemilik terminal ataupun penanggung jawab sistem jaringan komputer, maka perbuatan ini dikategorikan sebagai *hacking*. Kejahatan komputer jenis *hacking* sangat berbahaya karena apabila seseorang berhasil masuk ke dalam sistem jaringan orang lain, maka implikasi hukumnya ia mungkin saja membaca dan menyalin informasi yang mungkin sangat rahasia, atau mungkin pula menghapus atau mengubah informasi atau program-program yang tersimpan pada sistem komputer. Ada pula kemungkinan ia mencuri dengan memerintahkan komputer untuk mengirimkan barang kepadanya. Perbuatan mengakses ke suatu sistem jaringan tanpa ijin tersebut dapat dikategorikan sebagai perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan tanpa haknya berjalan di atas tanah milik orang lain, sehingga pelaku dapat diancam idana berdasarkan Pasal 167 KUHP dan Pasal KUHP. Pasal 167 KUHP mengatur bahwa :

(1) Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum atau berada di situ dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama Sembilan bulan atau denda paling banyak empat ribu lima ratus rupiah;

(2) Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu atau barang siapa tidak setahu yang berhak lebih dulu bukan karen kekhilafan masuk dan kedapatan di situ pada waktu malam, dianggap memaksa masuk;

(3) Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, diancam dengan pidana penjara paling lama satu tahun empat bulan;

(4) Pidana tersebut dalam ayat (1) dan (3) ditambah sepertiga jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu.

Berdasarkan Pasal 167 KUHP tersebut, ada beberapa hal yang menyulitkan aparat penegak hukum dalam upaya penanganan kejahatan komputer, antara lain:

- Apakah komputer dapat disamakan dengan rumah, ruangan atau pekarangan tertutup;

- Berkaitan dengan cara masuk ke rumah atau ruangan tetutup, apakah test *key* atau *password* yang digunakan oleh seseorang untuk berusaha masuk ke dalam suatu sistem jaringan dapat dikategorikan sebagai kunci palsu, perintah palsu atau pakaian palsu.

Pasal yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain adalah Pasal 551 KUHP yang menyatakan bahwa:

"Barang siapa tanpa wewenang berjalan atau berkendaraan di atas tanah yang oleh pemiliknya dengan cara jelas di larang memasukinya, diancam dengan pidana denda paling banyak dua ratus dua puluh lima rupiah".

Berkaitan dengan pasal di atas, ada beberapa hal yang tidak sesuai lagi untuk diterapkan dalam upaya penanggulangan kejahatan *hacking*, yaitu pidana denda yang sangat ringan padahal hacking dapat merugikan finansial yang tidak sedikit bahkan mampu melumpuhkan kegiatan dari pemilik suatu jaringan yang berhasil dimasuki oleh pelaku.

d. Kejahatan sebagaimana yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik.

Beberapa bentuk tindak pidana yang diatur dalam UU ITE antara lain : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan dan/atau pencemaran nama baik, pemerasan dan/atau pengancaman. Menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik atau menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

3.3 Upaya Penegakan Hukum Terhadap Kejahatan di Bidang Komputer

Penanganan suatu tindak pidana akan dilakukan oleh penyidik. Penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang. Menurut ketentuan Pasal 7 KUHAP wewenang penyidik yaitu :

a) Menerima laporan atau pengaduan dari seorang tentang adanya tindak pidana;
b) Melakukan tindakan pertama pada saat di tempat kejadian;
c) Menyuruh berhenti seorang tersangka dan memeriksa tanda pengenal dari tersangka;
d) Melakukan penangkapan, penahanan, penggeledahan dan penyitaan;
e) Melakukan pemeriksaan dan penyitaan surat;
f) Mengambil sidik jari dan memotret seorang;
g) Memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
h) Mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara;
i) Mengadakan penghentian penyidikan;
j) Mengadakan tindakan lain menurut hukum yang bertanggung jawab.

Berdasarkan ketentuan Pasal 15, Peraturan Kepala Kepolisian Negara Republik Indonesia No. 14 Tahun 2012, kegiatan penyidikan dilaksanakan secara bertahap meliputi: penyelidikan; pengiriman SPDP; upaya paksa; pemeriksaan; gelar perkara; penyelesaian berkas perkara; penyerahan berkas perkara ke penuntut umum; penyerahan tersangka dan barang bukti; dan penghentian penyidikan. Secara rinci kegiatan tersebut terjabar dalam uraian berikut:

1) Penyelidikan

Berdasarkan ketentuan Pasal 1 angaka 5 KUHAP, pengertian penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang ini. Merujuk pada ketentuan Pasal 1 angka 4 KUHAP, maka penyelidikan perbuatan yang diduga *cybercrime* dilakukan pejabat Polri dan PNS sebagaimana yang diatur dalam undang-undang.

2) Pengiriman Surat Pemberitahuan Dimulainya Penyidikan (SPDP)

Pasal 109 ayat (1) KUHAP mengatur bahwa dalam hal penyidik telah memulai melakukan penyidikan suatu peristiwa yang merupakan tindak pidana, penyidik memberitahukan hal itu kepada penuntut umum. Kerena itu, berdasarkan Perkap No 14 tahun 2012 Pasal 1 angka 17, ditentukan bahwa Surat Pemberitahuan Dimulainya Penyidikan adalah surat pemberitahuan kepada Kepala kejaksaan tentang dimulainya penyidikan yang dilakukan oleh penyidik Polri.

3) Upaya Paksa

Merujuk pada ketentuan Pasal 26 Perkap No 14 Tahun 2012, upaya paksa meliputi: a.pemanggilan; b. penangkapan; c. penahanan; d. penggeledahan; e. penyitaan, dan f. pmeriksaan surat. Berdasarkan ketentuan Pasal 43 ayat (6) diatur bahwa dalam hal melakukan penangkapan dan penahanan,

penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

4) Pemeriksaan

Pasal 63 Perkap No 14 Tahun 2012, bahwa pemeriksaan dilakukan oleh penyidik atau penyidik pembantu terhadap saksi, ahli, dan tersangka yang dituangkan dalam berita acara pemeriksaan yang ditandatangani oleh penyidik/penyidik pembantu yang melakukan pemeriksaan dan orang yang diperiksa. Tujuannya untuk mendapatkan keterangan saksi, ahli dan tersangka yang dituangkan dalam berita acara pemeriksaan, guna membuat terang perkara sehingga peran seseorang maupun barang bukti dalam peristiwa pidana yang terjadi dapat diketahui secara jelas. Penyidik/ penyidik pembantu yang melakukan pemeriksaan wajib memiliki kompetensi sebagai pemeriksa.

Berkaitan dengan proses pemeriksaan barang bukti digital baik pada saat penyidikan maupun pemeriksaan di pengadilan, perlu ada kemampuan yang memadai dari penegak hukum. Dalam penanganan data elektronik diperlukan langkah-langkah khusus agar bukti digitalnya tidak berubah. Karena itu, penyidik harus memahami penanganan awal barang bukti elektronik pada komputer di tempat kejadian perkara, penggandaan secara Physical sektor per sektor (forensic imaging), analisis sistem file (file system) dari Program Microsoft Windows, mencari dan memunculkan file walaupun sudah dihapus dan diformat, atau data yang tidak pernah disimpan dan hanya di print (files recovery), analisis telepon seluler (mobile forensic), analisis rekaman suara (audio forensic), analisis rekaman video (video forensic), dan analisis gambar digital (image forensic).

Perkara *cybercime* merupakan perkara khusus yang cara penyidikannya dapat berbeda sebagaimana penyidikan dalam perkara umum. Dalam melaksanakan tugas dan peranannya maka fungsi reserse khususnya satuan *cybercrime* mendasarkan pada beberapa undang-undang yang terkait dengan tindak pidana *cybercrime* yang terjadi. Salah satunya sebagai pedoman alat bukti yaitu ketentuan dalam Pasal 184 KUHAP, dimana yang dimaksud alat-alat bukti adalah keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Selain itu penyidik dapat menggunakan penyidik *cybercrime* menggunakan alat bukti yaitu Informasi Elektronik dan atau Dokumen Elektronik dan/atau hasil cetaknya. Namun informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE.

Selanjutnya Menurut ketentuan Pasal 6 UU No.11 tahun 2008, diatur pula bahwa dalam hal terdapat ketentuan lain yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, infromasi elektronik dan/atau dokumen elektronik, maka akan dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan seuatu keadaan. Dalam ketentuan Pasal 44 UU ITE diatur bahwa, alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut: a. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3). Berdasarkan ketentuan tersebut, maka alat bukti dalam *cybercrime* adalah sebagai berikut :

a) Informasi Elektronik yaitu satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (electronic mail), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, symbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Hal ini sesuai dengan ketentuan Pasal 1 angka 1 UU No.11 Tahun 2008.
b) Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, symbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Hal ini didasarakan pada ketentuan Pasal 1 angka 4 UU No.11 Tahun 2008.

Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Informasi Elektronik dan/atau Dokumen Elektronik ataupun hasil cetaknya merupakan bentuk perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Namun demikian, hasil cetak dokumen elektronik tidak berlaku untuk: a). surat yang menurut

Undang-Undang harus dibuat dalam bentuk tertulis; dan b). surat beserta dokumennya yang menurut Undang-Undang harus dalam bentuk akta notaries atau akta yang dibuat oleh pejabat pembuat akta. Dalam hal terdapat ketentuan lain yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

5) Gelar Perkara

Merujuk pada ketentuan Pasal 72 Perkap No. 14 Tahun 2012, penyelenggaraan gelar perkara meliputi 3 tahapan berikut:

a) Persiapan

Tahap perisiapan meliputi:a. penyiapan bahan paparan gelar perkara oleh tim penyidik; b. panyiapan sarana dan prasarana gelar perkara; dan c. pengiriman surat undangan gelar perkara.

b) Pelaksanaan

Tahap pelaksanaan gelar meliputi: a. pembukaan gelar perkara oleh pimpinan gelar perkara; b. paparan tim penyidik tentang pokok perkara, pelaksanaan penyidikan, dan hasil penyidikan yang telah dilaksanan; c. tanggapan para peserta gelar perkara; d. diskusi permasalahan yang terkait dalam penyidikan perkara; dan e. kesimpulan gelar perkara.

c) Kelanjutan Hasil Gelar Perkara

Tahap kelanjutan hasil gelar perkara meliputi: a. pembuatan laporan hasil gelar perkara; b. penyampaian laporan kepada pejabat yang berwenang; c. tindak lanjut hasil gelar perkara oleh penyidik dan melaporkan perkembangannya kepada atasan penyidik; dan.d. pengecekan pelaksanaan hasil gelar perkara oleh pengawasan penyidikan.

6) Penyelesaian Berkas Perkara;

Berdasarkan ketentuan Pasal 73 Perkap No. 14 Tahun 2012, penyelesaian berkas perkara meliputi tahapan berikut:

a) Pembuatan resume berkas perkara

Pembuatan resume berkas perkara sekurang-kurangnya memuat: a. dasar penyidikan; b. uraian singkat perkara; c. uraian tentang fakta-fakta; d. analisis yuridis; dan e. kesimpulan.

b) Pemberkasan

Pemberkasan, sekurang-kurangnya memuat : a. sampul berkas perkara; b. daftar isi; c. berita acara pendapat/resume; d. laporan polisi; e. berita acara setiap tindakan penyidik/penyidik pembantu; f.administrasi penyidikan; g. daftar saksi; h. daftar tersangka; dan i. daftar barang bukti.

Setelah dilakukan pemberkasan, diserahkan kepada atasan penyidik selaku penyidik untuk dilakukan penelitian dan selanjutnya jika memenuhi syarat segera dilakukan penjilidan dan penyegelan.

6. Penyerahan Berkas Perkara Ke Penuntut Umum

Sesuai dengan ketentuan Pasal 110 KUHAP diatur bahwa dalam hal penyidik telah selesai melakukan penyidikan, penyidik wajib segera menyerahkan berkas perkara itu kepada penuntut umum. Dalam hal penuntut umum berpendapat bahwa hasil penyidikan tersebut ternyata masih kurang lengkap, maka penuntut umum segera mengembalikan berkas perkara itu kepada penyidik disertai petunjuk untuk dilengkapi. Dalam hal penuntut umum mengembalikan hasil penyidikan untuk dilengkapi, penyidik wajib segera melakukan penyidikan tambahan sesuai dengan petunjuk dari penuntut umum. Penyidik dianggap telah selesai apabila dalam waktu empat belas hari penuntut umum tidak mengembalikan hasil penyidikan atau apabila sebelum batas waktu tersebut berakhir telah ada pemberitahuan tentang hal itu dari penuntut umum kepada penyidik.

Pada prinsipnya, ketentuan tentang Penyidikan dan Penuntutan dalam KUHAP di atas menunjukkan hubungan yang erat antara penyidikan dengan penuntutan. Secara ringkas dapat dikatakan bahwa penyidikan merupakan kegiatan untuk mengumpulkan alat bukti mengenai adanya satu tindak pidana beserta pelaku tindak pidana tersebut, sementara penuntutan merupakan kegiatan yang ditujukan untuk mempertanggungjawabkan hasil dari kegiatan penyidikan di forum pengadilan. Dalam hal ini, pelaksanaan dari *integrated criminal justice system* sebetulnya adalah untuk melaksanakan penegakan hukum yang terpadu dan berkesinambungan untuk mendapatkan *out put* yang maksimal. Penyidikan haruslah diarahkan kepada pembuktian di persidangan, sehingga tersangka (pelaku tindak pidana) dapat dituntut dan diadili di persidangan. Penyidikan yang berakhir dengan putusan (*vrisjpraak*) ataupun lepas dari segala tuntutan (*onslag van alle rechtsvervolging*) dari Pengadilan terhadap pelaku tindak pidana akan merugikan masyarakat dan lembaga penegak hukum itu sendiri.

Terkait dengan subjek pelaku tindak pidana, maka 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.

Bagan 2. Alur Penanganan Tindak Pidana

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,-

4. Kesimpulan

Berdasarkan hasil pembahasan di atas, maka dapat disimpulkan bahwa masih perlu pengaturan-pengaturan yang lebih jelas dan spesifik terkait dengan penegakan hukum terhadap kejahatan yang timbul di bidang teknologi Informasi, khususnya kejahatan-kejahatan yang timbul setelah adanya internet, dimana sistem komputer sebagai korbannya, seperti hacking, cracking, viruses, booting, troyan horse,

maupun spamming. Kejelasan ini sangat penting terutama berkaitan dengan substansi aturan atau ketentuan perundang-undangan yang mengatur tentang tindak pidana di bidang teknologi Informasi.
Upaya penegakan hukum terhadap kejahatan di bidang teknologi Informasi tetap didasarkan pada hukum acara formal sebagaimana yang diatur dalam KUHAP. Hal ini sesuai pula dengan ketentuan Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

5. Saran

Penelitian ini tentu masih memiliki kekurangan. Harapan peneliti ke pada peneliti selanjutnya agar dapat mengembangkan penelitian ini agar untuk menyelesaikan kekurangan dari penelitian ini.

Daftar Pustaka

[1] Maskun, 2013. Kejahatan Siber; Cybercrime Suatu Pengantar, Kencana, Makassar.
[2] Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
[3] Widodo, 2011. Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law); Telaah Teoritik dan Bedah Kasus, Aswaja Presindo, Yogyakarta.
[4] Josua Sitompul, 2012. Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana, Tatanusa, Jakarta.
[5] Asril Sitompul, 2001. Hukum Internet: Pengenalan Mengenai Masalah Hukum di Cyberspace, Citra Aditya Bakti, Bandung.
[6] Lawrence M. Friedman, 1975. The Legal System: A Social Science Perspective, New York: Russell Sage Foundation.
[7] Pristika Handayani, 2020. Penegakan Hukum Terhadap Kejahatan Teknologi Informasi. Jurnal Dimensi.Vol.2 No.2 Universias Riau, Kepulauan Batam.
[8] Dikdik M. Arief Mansur dan Elisatris Gultom, Cyber Law Aspek Hukum Teknologi Informasi", Refika Aditama, Bandung,2005.
[9] Heru Sutadi, 2013. Cybercrime, Apa Yang Bisa Diperbuat?,http://www.sinarharapan.co.id/berita
[10] Tubagus Ronny Rahman Nitibaskara, 2001. Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi. Peradaban, Jakarta.
[11] Barda Nawawi Arif,2001. Tindak Pidana Mayantara, Bandung, 9 April 2001