

**KEJAHATAN MELALUI MEDIA SOSIAL ELEKTRONIK DI INDONESIA  
BERDASARKAN PERATURAN PERUNDANG-UNDANGAN SAAT INI**

<sup>1</sup>Prima Angkupi. SH.,MH.,MKn

<sup>1</sup>Fakultas Hukum Universitas Muhammadiyah Metro  
Jalan Ki Hajar Dewantara No. 116 Kota Metro

**Abstract** - *Internet creates new opportunities in public life, the internet also while creating new opportunities for crime. In the virtual world of people doing evil deeds (crime) that it can not be done in the real world. Kejahatan is done by using the computer as a means of actions. Crimes committed in the virtual world using the kom-puter called "computer crime" or "cyber crime". Computer crimes have created new problems for the task of inquiry, investigation, and prosecution by law negak oners. Consequently, electronic information and electronic transaction needs a strong protection against -upaya efforts made by parties who are not responsible for access to information stored in a computer system. While the response to cyber crime from the perspective of criminal law can be seen and various aspects, among other aspects of the criminalization policy (formulation criminal offense), aspects of criminal liability or punishment (including aspects of evidence / proof).*

**Keywords:** *Cyber, Computer, Cyber Crime*

**Abstrak** - Internet menciptakan berbagai peluang baru dalam kehidupan masyarakat, internet juga sekaligus menciptakan peluang-peluang baru bagi kejahatan. Di dunia virtual orang melakukan berbagai perbuatan jahat (kejahatan) yang justru tidak dapat dilakukan di dunia nyata. Kejahatan tersebut dilakukan dengan menggunakan komputer sebagai sarana perbuatannya. Kejahatan yang dilakukan di dunia virtual dengan menggunakan komputer itu disebut "kejahatan komputer" atau "cyber crime". Kejahatan-kejahatan komputer telah menciptakan masalah-masalah baru bagi tugas penyelidikan, penyidikan, dan penuntutan oleh para penegak hukum. Konsekuensinya, *electronic information* dan *electronic transaction* memerlukan adanya perlindungan yang kuat terhadap upaya-upaya yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab untuk dapat mengakses informasi yang tersimpan dalam sistem komputer. Sedangkan upaya penanggulangan cyber crime jika dilihat dari perspektif hukum pidana dapat dilihat dan berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian).

**Kata kunci :** *Cyber, Computer, Cyber Crime*

## I. PENDAHULUAN

Internet telah mempengaruhi pola hidup manusia atau masyarakat, ternyata ada masalah serius yang dihadapi oleh masyarakat berkenaan dengan maraknya Internet. Masalah itu adalah masalah hukum. Akan tetapi, masalah hukum di dunia virtual tersebut belum banyak mendapat perhatian otoritas dan pengguna Internet karena pemahaman yang masih dangkal mengenai aspek-aspek hukum dari Internet atau dari transaksi yang dilakukan dengan menggunakan sarana Internet.

Semua perbuatan hukum di dunia virtual, yang dilakukan oleh manusia-manusia yang berada di dunia nyata. Perbuatan-perbuatan hukum tersebut dilakukan menggunakan media atau sarana Internet (yaitu menggunakan komputer yang berada di dunia nyata). Jasmani manusia yang melakukan perbuatan-perbuatan hukum tersebut tidak berada dan tidak hidup di dunia virtual. Hanya sekadar berkhayal, mungkin saja kelak teknologi akan benar-benar dapat menciptakan makhluk-makhluk maya, yaitu manusia-manusia maya dan binatang-binatang maya, sebagaimana yang sering kita lihat di film-film, dan manusia-manusia maya ini yang nantinya melakukan sendiri perbuatan-perbuatan hukum itu tanpa perintah dan kendali manusia yang berada di dunia nyata.

Perkembangan yang pesat dalam pemanfaatan jasa internet tersebut ternyata menimbulkan dampak negatif lain, ialah dalam bentuk perbuatan kejahatan dari pelanggaran, yang kemudian muncul istilah *cybercrime*, yang merupakan perkembangan lebih lanjut dari *computercrime*. Dalam menjelaskan tantangan perkembangan *cyberlaw* ini, Rene L. Pattiradjawane menyebutkan konsep hukum *cyberspace*, *cyberlaw*, dan *cyberline* yang dapat menciptakan komunitas pengguna jaringan internet yang luas (60 juta), yang melibatkan 160 negara menimbulkan kekusaran para praktisi hukum untuk menciptakan pengamanan melalui regulasi, khususnya perlindungan terhadap milik pribadi (Ninieck Suparni, 2009: 9).

Sebagian besar anak muda dan para remaja memiliki dan/atau dapat menggunakan komputer. Hal ini tidak terkecuali pula dengan Indonesia. Di Amerika Serikat terdapat 80 juta orang dewasa dan 10 juta anak-anak yang mampu mengakses Internet. Keadaan ini tentu

saja telah memaraskan terjadinya kejahatan computer (Sutan Remy Syahdeini, 2009: 8)

Terdapat beberapa kasus kejahatan komputer yang telah diajukan ke pengadilan. Mungkin hal ini agak lain dibandingkan dengan perbuatan pidana siber, namun mengingat sarana yang digunakan dapat masuk di bidang komputer, telekomunikasi, dan informasi maka dapat dijadikan contoh yang termasuk segolongan. Adapun kasus-kasus tersebut adalah sebagai berikut.

Putusan Mahkamah Agung No. 363 K/Pid/1984 tanggal 25 Juni 1984 mengenai penggelapan uang di bank melalui komputer. Perbuatan pidana ini merupakan kerja sama antar orang luar dengan oknum pegawai BRI Cabang Brigjen Katamso Yogyakarta dari tanggal 15 September sampai dengan 12 Desember 1982, yaitu dengan cara mentransfer uang melalui kliring kemudian warkat kliring yang diterima dari kliring tersebut oleh oknum pegawai BRI secara melawan hukum dan tanpa sepengetahuan bagian kartu dibebankan kepada rekening orang lain, bukan rekening yang tertulis pada warkat kliring dengan cara membukukan melalui komputer tanpa kartu atau struk mesin.

Perbuatan ini berlangsung sampai 44 kali mencapai jumlah Rp815 juta serta Rp10 juta melalui validasi tunai tanpa dilakukan mutasi atas kartu nasabah Ny. Karlina. Atas perbuatan tersebut, Pengadilan Negeri Yogyakarta dengan keputusannya No. 33/1983/Pid/PN, tanggal 20 September 1983 menjatuhkan hukuman atas terdakwa bersalah melakukan perbuatan korupsi dan menghukum pidana penjara 10 tahun dipotong masa tahanan, harus membayar biaya perkara Rp100 ribu.

Keputusan ini diperkuat oleh keputusan Pengadilan Tinggi Yogyakarta No. 41/1983/Pid/PTY, tanggal 6 Maret 1984, dan Mahkamah Agung dengan keputusan No. 363/K/Pid/1984 tanggal 25 Juni 1984 menolak permohonan kasasi yang diajukan jaksa, karena hak permohonan kasasi telah gugur, disebabkan tidak ada memori kasasi. Adapun landasan hukum penuntutan adalah Pasal 55 ayat (1) jo. Pasal 64 ayat (1) KUH Pidana jo. Pasal 1 ayat (1) sub a Undang-Undang Nomor 3 Tahun 1971 tentang pemberantasan Tindak Pidana Korupsi, yang pada intinya perbuatan tersebut dilakukan

bersama-sama antara terdakwa dan oknum pegawai BRI dan merugikan negara.

Berikutnya kasus pembobolan BNI Cabang New York, ialah kasus seorang pegawai yang pernah bekerja di BNI Cabang New York sejak tahun 1980 sampai dengan September 1985.

Pada waktu masih bekerja, yang bersangkutan bertugas sebagai operator komputer untuk mengakses *Citybank New York* atau *Mantrust New York*, oleh karenanya yang bersangkutan memegang *password* dengan kode tertentu. Pada tanggal 31 Desember 1986, yang bersangkutan bekerja sama dengan orang lain berhasil mengoperasikan komputer di sebuah hotel untuk melakukan transfer ke rekening bank tertentu, yaitu dengan menggunakan *USER ID* dan *password* dengan melawan hukum. Proses tersebut dimulai dengan memerintahkan *Citybank New York* untuk mentransfer dana atas beban rekening BNI kepada rekening BNI di *Mantrust*. Dari sini kemudian yang bersangkutan mentransfer dana ke beberapa bank lainnya untuk keuntungan sendiri.

Penggunaan landasan hukum mengenai pasal pencurian (Pasal 363 KUH Pidana) tidak dapat diterima, demikian juga Undang-Undang Pemberantasan Tindak Pidana Korupsi tidak dapat diterapkan karena unsur melawan hukum yang dituduhkan tidak termasuk kriterium undang-undang tersebut. Hal ini karena tidak terbukti adanya kerja sama dengan pegawai negeri, atau lebih tepatnya tidak terbukti adanya penggunaan kekuasaan atau pengaruh yang melekat pada seorang pegawai negeri. Andi Hamzah, berpendapat bahwa pertimbangan hakim untuk membebaskan terdakwa dari dakwaan primer, subsidair, lebih subsidair tidak tepat, karena korupsi yang memakai penggunaan kekuasaan atau pengaruh yang melekat justru terdapat pada rumusan Pasal 1 ayat (1) sub b Undang-Undang Pemberantasan Tindak Pidana Korupsi, yang justru oleh jaksa tidak digunakan dalam menyusun dakwaan (Andi Hamzah, 1993 : 63).

Jadi aspek hukum pidana yang digunakan untuk dakwaan primer adalah Pasal 1 ayat (1) sub a jo. Pasal 28 Undang-Undang Nomor 3 Tahun 1971 jo. Pasal 55 ayat (1) ke-1 KUH Pidana. Dakwaan subsidair adalah Pasal 1 ayat (2) jo. Pasal 1 ayat (1) sub a jo. Pasal 28 Undang-Undang Nomor 3 Tahun 1971 jo. Pasal 55 ayat (1) ke-1 KUH Pidana. Dakwaan lebih subsidair lagi adalah Pasal 363 ayat (1) KUH Pidana, dan

yang lebih subsidair lagi adalah Pasal 363 ayat (1) ke-4 jo. Pasal 53 KUH Pidana.

Kasus ini menyebabkan kerugian BNI yang cukup besar (US\$9.100.000) dan dilakukan oleh orang-orang yang cukup ahli di bidang komputer, yaitu pembobolannya dilakukan dengan menggunakan Personal Komputer *Apple IIC*, *Keyboard*, dan *Smart Modem*, dan berbekal *password* dan *code* yang pernah diketahui. Ini suatu peringatan jika suatu perusahaan melakukan mutasi pada petugas operator komputer yang rawan terhadap terjadinya penyalahgunaan, harus diikuti dengan penggantian kode *password*, sehingga tidak ada pihak lain yang dapat mengakses. Kasus – kasus tersebut menunjukkan bahwa pada dasarnya kejahatan tersebut dilakukan dengan bantuan atau melalui peralatan komputer, telekomunikasi, dan informasi, baik berupa *hardware*, *software*, maupun *brainware*.

Sutan Remy Syahdeini berpendapat bahwa oleh karena interaksi dan perbuatan-perbuatan hukum yang terjadi melalui atau di dunia virtual adalah sesungguhnya interaksi antara sesama manusia dari dunia nyata, dan apabila terjadi pelanggaran hak atas perbuatan hukum melalui atau di dunia virtual itu adalah perbuatan hukum yang dilakukan oleh manusia dari dunia nyata dan hak yang dilanggar adalah hak dari manusia dari dunia nyata, maka hukum yang berlaku dan harus diterapkan adalah hukum dari dunia nyata bukan sama sekali tidak dapat digunakan. Namun karena peristiwanya berlangsung di atau melalui dunia virtual, maka tentulah tidak sepenuhnya hukum yang berlaku bagi dunia nyata dapat digunakan. Dengan demikian, bagi peristiwa-peristiwa dan perbuatan-perbuatan yang berdampak terhadap sistem komputer memerlukan pula hukum khusus. Hukum khusus tersebut dikenal sebagai *cyber law* (Sutan Remy Syahdeini, 2009: 15). Berdasarkan latar belakang di atas, maka judul dari penulisan karya ilmiah ini adalah ” **Analisis Bentuk-Bentuk Kejahatan Komputer Di Indonesia Berdasarkan Peraturan Perundang-Undang Saat ini** ”

### III. PERMASALAHAN DAN RUANG LINGKUP

#### 1. Permasalahan

Berdasarkan uraian dari latar belakang masalah tersebut diatas, maka yang menjadi permasalahan dalam karya ilmiah ini adalah apakah bentuk-bentuk kejahatan komputer di

Indonesia berdasarkan peraturan perundang-undangan saat ini ?

### C. Kerangka Teoretis

Kerangka Teoretis adalah konsep yang merupakan abstraksi dari hasil pemikiran atau kerangka acuan yang pada dasarnya bertujuan untuk mengadakan identifikasi terhadap dimensi sosial yang dianggap relevan (Soerjono Soekanto, 1986: 123).

Kejahatan terus berkembang seiring dengan perkembangan peradaban manusia, dengan kualitas dan kuantitasnya kompleks dengan variasi modus operandinya. J.E. Sahetapy telah menyatakan dalam tulisannya, kejahatan erat kaitannya dan bahkan menjadi bagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya (Abdul Wahid, 2002: 36).

Kejahatan adalah suatu nama atau cap yang diberikan orang untuk menilai perbuatan perbuatan tertentu, sebagai perbuatan jahat. Secara empiris menurut B. Simanjuntak definisi kejahatan dapat dilihat dari dua perspektif, pertama adalah kejahatan dalam perspektif yuridis, kejahatan dirumuskan sebagai perbuatan yang oleh negara diberi pidana untuk mengembalikan keseimbangan yang terganggu akibat perbuatan itu. Dalam hukum pidana disebut dengan tindak pidana. Kedua, kejahatan dalam arti sosiologis (kriminologis) merupakan kejahatan yang dari segi yuridis (hukum positif) bukan merupakan kejahatan. Artinya, perbuatan tersebut oleh negara tidak dipidana (Abdul Wahid, 2002: 38).

J.E. Sahetapy dan B. Marjono Reksodiputro dalam bukunya *Paradoks Dalam Kriminologi* menyatakan bahwa, kejahatan mengandung konotasi tertentu, merupakan suatu pengertian dan penamaan yang relatif, mengandung variabilitas dan dinamik serta bertalian dengan perbuatan atau tingkah laku (baik aktif maupun pasif), yang dinilai oleh sebagian mayoritas atau minoritas masyarakat sebagai suatu perbuatan anti sosial, suatu perkosaan terhadap skala nilai sosial dan atau perasaan hukum yang hidup dalam masyarakat sesuai dengan ruang dan waktu. (Abdul Wahid, 2002:39). Lemert mengemukakan bahwa kejahatan (deviance) terdiri atas devian primer dimaksudkan suatu perbuatan yang melawan hukum dan devian sekunder dimaksudkan suatu proses dimana orang lain beraksi terhadap akibat atau

implikasi dari devian primer. (J.E. Sahetapy, 2005: 32).

Edwin H. Sutherland dalam bukunya *Principles of Criminology* menyebutkan tujuh unsur kejahatan yang saling bergantung dan saling mempengaruhi. Suatu perbuatan tidak akan disebut kejahatan kecuali apabila memuat semua tujuh unsur tersebut. Unsur-unsur tersebut adalah :

1. Harus terdapat akibat-akibat tertentu yang nyata atau kerugian.
2. Kerugian tersebut harus dilarang oleh undang-undang, harus dikemukakan dengan jelas dalam hukum pidana.
3. Harus ada perbuatan atau sikap membiarkan sesuatu perbuatan yang disengaja atau sembrono yang menimbulkan akibat-akibat yang merugikan.
4. Harus ada maksud jahat (*mens rea*)
5. Harus ada hubungan kesatuan atau kesesuaian persamaan suatu hubungan kejadian diantara maksud jahat dengan perbuatan.
6. Harus ada hubungan sebab akibat diantara kerugian yang dilarang undang-undang dengan perbuatan yang disengaja atas keinginan sendiri.
7. Harus ada hukuman yang ditetapkan oleh undang-undang.

Hukum pidana membedakan antara kejahatan (deviance) dan tindak pidana (crime). Kejahatan tidak selalu tindak pidana. Kejahatan hanya merupakan tindak pidana apabila perilaku jahat tersebut telah ditetapkan sebagai tindak pidana (dikriminalisasi) oleh suatu undang-undang pidana. Tindak pidana adalah perilaku (commission dan omission) yang telah dinyatakan sebagai tindak pidana oleh undang-undang (Sutan Remy Syahdeini, 2009: 33)

Menurut Oemar Seno Adji (Andi Hamzah, 2004:88) tindak pidana (*starfbaarfeit*) merupakan padanan istilah delik yaitu kelakuan yang diancam dengan pidana, yang bersifat melawan hukum yang berhubungan dengan kesalahan dan dilakukan oleh orang yang mampu bertanggung jawab. Oleh karena itu perbuatan tertentu merupakan delik karena perbuatan tersebut membawa suatu sanksi, maka delik merupakan suatu kondisi atau syarat bagi diberlakukannya sanksi oleh norma hukum. (Hans Kelsen, 2006: 74)

Menurut Simon. (Andi Hamah, 2004:88) rumusan delik antara lain :

- a. Diancam dengan pidana oleh hukum.
- b. Bertentangan dengan hukum.

- c. Dilakukan oleh orang yang bersalah.
- d. Orang itu dipandang bertanggung jawab atas perbuatannya.

### III. HASIL DAN PEMBAHASAN

Terdapat undang-undang utama yang mengatur tentang informasi dan transaksi elektronik di Indonesia. Undang-undang yang pertama adalah Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang yang kedua adalah undang-undang yang telah dikeluarkan sebelum dikeluarkannya Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang tersebut adalah Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi. Di bawah ini diberikan penjelasan tentang beberapa hal yang menyangkut tindak-tindak pidana komputer dalam Undang-undang Informasi dan Transaksi Elektronik.

Akhir-akhir ini telah banyak bermunculan kejahatan-kejahatan komputer di Indonesia yang sangat merugikan perorangan maupun masyarakat luas. Di samping itu, akhir-akhir ini juga telah muncul berbagai *commercial website* milik orang/perusahaan Indonesia di Internet yang menawarkan berbagai barang dan jasa kepada masyarakat atau para konsumen. Berkaitan dengan perkembangan tersebut, pada 21 April 2008 Indonesia telah mengundangkan Undang-undang tentang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 (UU ITE). Dalam undang-undang tersebut terdapat beberapa pasal pidana yang merupakan ketentuan tindak pidana khusus di samping berlakunya KUHP sebagai Undang-undang tindak pidana umum. Selain pasal-pasal pidana, undang-undang tersebut sekaligus juga mengatur aspek-aspek keperdataan dari transaksi elektronik atau *e-commerce*.

Undang-undang tersebut memilih untuk mengacu model yang bersifat komprehensif. Artinya, materi muatan yang diatur dalam undang-undang tersebut mencakup hal yang luas disesuaikan dengan kebutuhan saat ini. Oleh karena sifatnya yang komprehensif itu, maka dalam undang-undang tersebut tercakup banyak aspek hukum, yaitu aspek hukum perdata materiil, hukum pidana materiil, hukum acara perdata, hukum acara pidana, dan hukum pembuktian. Dengan kata lain, yang dipilih bukan model pengaturan yang berpijak pada pemilahan materi hukum secara ketat sehingga

regulasi yang dibuat menjadi bersifat sangat sempit dan spesifik pada sektor tertentu saja.

UU ITE memuat ketentuan-ketentuan mengenai larangan melakukan perbuatan-perbuatan tertentu yang diancam dengan sanksi pidana bagi pelakunya. Tegasnya, Undang-undang tersebut menetapkan beberapa perbuatan yang dikriminalisasi sebagai tindak pidana komputer dengan sanksi-sanksinya. Tindak-tindak pidana yang dimaksud adalah sebagaimana yang diuraikan di bawah ini. Perbuatan-perbuatan yang dilarang dan bersanksi pidana itu merupakan tindak-tindak pidana komputer Indonesia. Tindak-tindak pidana komputer yang diatur oleh UU ITE tersebut adalah :

#### 1. Pornografi

##### a. Pornografi Pada Umumnya.

Larangan melakukan perbuatan yang bermuatan *melanggar kesusilaan* diatur dalam Pasal. 27 ayat (1) dan diancam sanksi pidana berdasarkan Pasal 45 ayat (1). Pasal 27 ayat (1) menentukan:

Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

Ancaman pidana terhadap pelaku yang melanggar Pasal 27 ayat (1) ditentukan dalam Pasal 45 ayat (1) yang berbunyi:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (5), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000.00 (satu miliar rupiah).

*Actus reus*, adalah "*conduct*" atau "perilaku" yang dapat berupa "melakukan perbuatan tertentu yang dilarang oleh undang-undang" atau "*commission*" atau "*act*" atau berupa "berdiam diri" atau "tidak melakukan perbuatan yang diwajibkan oleh hukum" atau "*omission*" yaitu berdiam diri tidak berbuat sesuatu. *Actus reus* dari tindak pidana Pasal 27 ayat (1) jo. Pasal 45 ayat (1) adalah:

- 1) mendistribusikan,
- 2) mentransmisikan, dan/atau
- 3) membuat dapat diakses

*Mens rea* ("sikap kalbu" atau unsur kesalahan) dari tindak pidana tersebut di atas adalah "dengan sengaja". Objek dari *actus reus* tindak pidana tersebut adalah "Informasi Elektronik

dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan".

#### b. Pornografi Anak

Pasal 52 ayat (1) mengancamkan sanksi pidana yang lebih berat apabila tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak. Lengkapnya bunyi Pasal 52 ayat (1) adalah:

Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.

Pasal 52 ayat (1) tidak berbicara apa-apa mengenai batasan umur. Seperti telah dikemukakan sebelumnya, di beberapa negara undang-undangnya memberikan batasan umur bagi mereka yang masih tergolong anak (*child*), yaitu di bawah umur 18 tahun atau sampai dengan 18 tahun. Dengan tidak adanya pembatasan umur oleh UU ITE, lalu undang-undang apa yang dapat dijadikan acuan untuk menentukan batasan umur tersebut? Ketiadaan batas umur menciptakan ketiadaan kepastian hukum bagi masyarakat.

#### 2. Perjudian *Online*

Larangan melakukan perjudian dengan menggunakan sistem elektronik atau dilakukan secara *online* (*e-gambling* atau *online gambling*) diatur dalam Pasal 27 ayat (2) dan diancam sanksi pidana berdasarkan Pasal 45 ayat (1). Pasal 27 ayat (2) menentukan:

Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

Ancaman pidana terhadap pelaku yang melanggar Pasal 27 ayat (2) ditentukan dalam Pasal 45 ayat (1) yang berbunyi:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

#### 3 Penghinaan dan atau Pencemaran Nama Baik

Larangan melakukan penghinaan dan atau pencemaran nama baik dengan menggunakan sistem komputer diatur dalam Pasal 27 ayat (3)

dan diancam sanksi pidana berdasarkan Pasal 45 ayat (1). Pasal 27 ayat (3) menentukan:

Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

Ancaman pidana terhadap pelaku yang melanggar Pasal 27 ayat (3) ditentukan dalam Pasal 45 ayat (1) yang berbunyi:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

#### 6. Penyebaran Informasi yang Bermuatan SARA

Larangan melakukan perbuatan menyebarkan informasi yang bermuatan SARA diatur dalam Pasal 28 ayat (2) dan diancam sanksi pidana berdasarkan Pasal 45 ayat (2). Pasal 28 ayat (2) menentukan:

Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/ atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).

Ancaman pidana terhadap pelaku yang melanggar Pasal 28 ayat (2) ditentukan dalam Pasal 45 ayat (2) yang berbunyi:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Perbuatan yang dilarang oleh Pasal 30 ayat (2) tersebut adalah apa yang kita kenal sebagai *cracking*. Menurut Penjelasan Pasal 30 ayat (2): Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:

- a. melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau
- b. sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima

oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

Ternyata kandungan penjelasan Pasal 30 ayat (2) tidak sesuai untuk menjelaskan Pasal 30 ayat (2); Penjelasan Pasal 30 ayat (2) itu lebih sesuai untuk menjelaskan Pasal 32 ayat (2), bukan untuk menjelaskan Pasal 30 ayat (2).

c. Membobol Komputer dan/atau Sistem Elektronik yang bertujuan selain untuk mengakses juga untuk menaklukkan sistem pengamanan dari sistem komputer yang diakses itu.

Larangan melakukan perbuatan tersebut diatur dalam Pasal 30 ayat (3) yang berbunyi:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Melanggar larangan Pasal 30 ayat (3) dipidana berdasarkan Pasal 46 ayat (3) yang berbunyi:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

*Actus reus* dari tindak pidana tersebut di atas adalah "mengakses". *Mens rea* dari tindak pidana tersebut di atas adalah "dengan sengaja". Objek dari *actus reus* tindak pidana tersebut adalah sama saja dengan objek dari *actus reus* dalam Pasal 30 ayat (1) dan ayat (2), yaitu "Komputer dan/atau Sistem Elektronik". Namun yang berbeda adalah tujuan pelakunya.

#### IV. KESIMPULAN

Bentuk-bentuk kejahatan komputer yang telah muncul sejak diperkenalkannya Internet berkaitan dengan pengembangan dan perkembangan teknologi informasi tersebut dilakukan dengan berbagai metode dan varian yaitu kejahatan terhadap harta kekayaan, kejahatan yang menyangkut identitas, kejahatan terhadap privasi, kejahatan terhadap sistem komputer serta kejahatan terhadap ketertiban umum. Mengingat perangkat teknologi dan kompetensi penegak hukum kita yang sangat terbatas. Pencegahannya lebih kepada upaya memasyarakatkan internal security (pengamanan

pribadi) dari pengguna layanan jaringan komputer. Penulis berpendapat bahwa tindakan pencegahan kejahatan komputer dapat dilakukan dengan meningkatkan sistem pengamanan komputer, Khususnya pada serangan hacker atau pun virus. Secara umum kejahatan komputer dapat dicegah melalui faktor-faktor lingkungan yaitu:

- a. Pendidikan komputer sejak dini yang dimulai dari bangku sekolah, sehingga dapat meningkatkan pengetahuan dan kesadaran atas bentuk-bentuk perbuatan dalam menggunakan sarana komputer yang salah.
- b. Pengawasan terhadap warnet-warnet yang ada di masyarakat, untuk mencegah warnet sebagai sarang penggunaan situs yang melanggar hukum..
- c. Pengawasan orang tua terhadap anak pengguna komputer dan internet.
- d. Membuat wadah bagi anak-anak yang memiliki kelebihan dibidang jaringan internet.
- e. Filterisasi situs-situs yang merusak norma anak muda oleh pemerintah.
- f. Sanksi yang tegas bagi pemilik warnet jika tidak menegur users nya yang sedang menggunakan situs cyber gambling, cyberporn, dll.
- g. Banyaknya komunitas black hat (hacker hitam) di Indonesia sebagai salah satu dampak penyebab maraknya terjadi kejahatan di dunia maya, lemahnya system computer, dan begitu kecilnya gaji para ahli IT di Indonesia menyebabkan para master computer berbuat criminal demi mencukupi kebutuhan finansialnya, jadi perlu peningkata taraf hidup bagi para ahli IT.

#### V. REFERENSI

- [1] Daliyo. 2001. Pengantar Hukum Indonesia. PT.Prehalindo
- [2] Hamzah, Andi. 2004. *Asas-Asas Hukum Pidana*. PT Rineka Cipta. Jakarta.
- [3] Heru Permana, Is. 2007. *Politik Kriminal*. Penerbit Universitas Atma Jaya Yogyakarta. Yogyakarta.
- [4] Kelsen, Hans. 2006. *Teori Umum Tentang Hukum dan Negara*. Penerbit Nusa Media dan Penerbit Nuansa. Bandung.

- [5] Laela Fakhriah. Efa, 2009. *Bukti Elektronik Dalam Sistem pembuktian perdata*. Alumni Bandung..
- [6] Merry, Magdalena, 2007. *Cyber Law, Siapa Takut*. Andi Yogyakarta.
- [7] Nawawi Arief, Barda. 2008. *Bunga Rampai Kebijakan Hukum Pidana*. Kencana Media Group. Jakarta.
- [8] Nawawi Arief, Barda, 2006. *Tindak Pidana Mayantara*. Raja Grafindo Persada. Jakarta
- [9] Partodihardji. Soemarno, 2009. *Tanya Jawab sekilas UU ITE*. Gramedia Pustaka Utama.
- [10] Rahardjo, Satjipto. 2008. *Membedah hukum Progresif*. KOMPAS. Jakarta.
- [11] Remy Syahdeini, Sutan. 2009. *Kejahatan & Tindak Pidana Komputer*. PT Pustaka Utama Grafiti. Jakarta.
- [12] Sehatapy, J.E. 2004. *Pisau Analisis Kriminologi*. PT Citra Aditya Bakti. Bandung.
- [13] Suparni, Niniek. 2009. *Cyber Space Problematika & Antisipasi Pengaturannya*. Sinar Grafika. Jakarta.
- [14] Wahid, Abdul. 2005. *Kejahatan Mayantara (Cyber Crime)*. PT Refika Aditama. Bandung.
- [15] Widodo. 2009. *Sistem Pidana Dalam Cyber Crime*. Laksbang Mediatama. Yogyakarta.
- [16] Waluyadi. 1999. *Pengetahuan dasar Hukum Pidana*. Mandar Maju
- [17] Anwar, Yesril. 2008. *Pembaharuan Hukum Pidana*, Kompas Gramedia.
- [18] KUHAP
- [19] Undang-Undang Nomor 11 Tahun 2008