CYBERCRIME DI INDONESIA

A. Latar Belakang

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user*) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.[1]

Pada tahun 1982 telah terjadi penggelapan uang di bank melalui komputer sebagaimana dapat dilihat dalam Putusan Mahkamah Agung Nomor 363 K/Pid/1984 tanggal 25 Juni 1984 mengenai. “Suara Pembaharuan” edisi 10 Januari 1991 memberitakan tentang dua orang mahasiswa yang membobol uang dari sebuah bank swasta di Jakarta sebanyak Rp. 372.100.000,00 dengan menggunakan sarana komputer.

Perkembangan lebih lanjut dari teknologi komputer adalah berupa *computer network* yang kemudian melahirkan suatu ruang komunikasi dan informasi global yang dikenal dengan internet.

Penggunaan teknologi komputer, telekomunikasi, dan informasi tersebut mendorong berkembangnya transaksi melalui internet di dunia. Perusahaan-perusahaan berskala dunia semakin banyak memanfaatkan fasilitas internet. Sementara itu tumbuh transaksi-transaksi melalui elektronik atau on-line dari berbagai sektor, yang kemudian memunculkan istilah *e-banking, e-commerce, e-trade,e-business, e-retailing*.

---

[1] **Andi Hamzah**, 1990, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, hal. 23-24.

Perkembangan yang pesat dalam pemanfaatan jasa internet juga mengundang terjadinya kejahatan. C*ybercrime* merupakan perkembangan dari *computer crime*.

Rene L. Pattiradjawane menyebutkan bahwa konsep hukum *cyberspace*, *cyberlaw* dan *cyberline* yang dapat menciptakan komunitas pengguna jaringan internet yang luas (60 juta), yang melibatkan 160 negara telah menimbulkan kegusaran para praktisi hukum untuk menciptakan pengamanan melalui regulasi, khususnya perlindungan terhadap milik pribadi.[2] John Spiropoulos mengungkapkan bahwa cybercrime memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya.[3]

Hukum yang salah satu fungsinya menjamin kelancaran proses pembangunan nasional sekaligus mengamankan hasil-hasil yang telah dicapai harus dapat melindungi hak para pemakai jasa internet sekaligus menindak tegas para pelaku cybercrime.

Penelitian ini merupakan kajian terhadap bentuk-bentuk cybercrime sebagai sebuah kejahatan, pengaturannya dalam sistem perundang-undangan Indonesia dan hambatan-hambatan yang ditemukan dalam penyidikan.

B. Perumusan Masalah

Berdasarkan latar belakang tersebut yang telah diuraikan maka dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana hubungan antara bentuk-bentuk Cybercrime dengan kejahatan?
2. Apakah undang-undang yang berlaku di Indonesia dapat diterapkan terhadap semua bentuk *Cybercrime* tersebut?

---

[2] **Rene L. Pattiradjawane**, "*Media Konverjensi dan Tantangan Masa Depan*", Kompas, 21 Juli 2000.
[3] **Jhon Sipropoulus**, 1999, "*Cyber Crime Fighting*, The Law Enforcement Officer's Guide to Online Crime", The Natinal Cybercrime Training Partnership, Introduction.

3. Masalah-masalah apa saja yang ditemukan dalam proses penyidikan terhadap *Cybercrime* dan bagaimana cara pemecahannya?

C. Tujuan Penelitian

1. Untuk mengetahui hubungan antara bentuk-bentuk *cybercrime* dengan kejahatan.
2. Untuk mengetahui bagaimana pengaturan *cybercrime* dalam sistem perundang-undangan Indonesia.
3. Untuk mengetahui masalah-masalah yang dihadapi dalam penyidikan *cybercrime*.

D. Manfaat Penelitian

1. Secara teoretis, hasil penelitian ini dapat dijadikan bahan kajian lebih lanjut untuk melahirkan beberapa konsep ilmiah yang pada gilirannya memberikan sumbangan bagi perkembangan hukum komputer.
2. Secara praktis, hasil penelitian ini dapat digunakan sebagai pedoman dan masukan bagi pemerintah, peradilan, dan praktisi hukum dalam menentukan kebijakan dan langkah-langkah untuk menyelesaikan perkara yang sedang dihadapi.

E. Komputer, Internet, dan Cybercrime

1. Komputer

Institut Komputer Indonesia mendefinisikan komputer sebagai berikut:

> "Suatu rangkaian peralatan-peralatan dan fasilitas yang bekerja secara elektronis, bekerja dibawah kontrol suatu *operating system*, melaksanakan pekerjaan berdasarkan rangkaian instruksi-instruksi yang disebut program serta mempunyai internal storage yang digunakan untuk menyimpan *operating system*, program dan data yang diolah." [4]

[4] **Institut Komputer Indonesia (IKI), 1981**, *Pengenalan Komputer (Introduction to Computer)*, hal. 1, dikutip dari Andi Hamzah, Loc. cit..

Operating system berfungsi untuk mengatur dan mengkontrol sumber daya yang ada, baik dari hardware berupa komputer, *Central Processing Unit* (CPU) dan *memory/storage* serta *software* komputer yang berupa program-program komputer yang dibuat oleh *programmer*. Jenis-jenis *Operating System* antara lain PC-DOS (Personal Computer Disk Operating System), MS-DOS (Microsoft Disk Operating System), Unix, Microsoft Windows, dan lain-lain.

2. Internet

Internet adalah jaringan luas dari komputer yang lazim disebut dengan *Worldwide network*. Internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik, satelit ataupun gelombang frekuensi. Jaringan komputer ini dapat berukuran kecil seperti *Lokal Area Network* (LAN) yang biasa dipakai secara intern di kantor-kantor, bank atau perusahaan atau biasa disebut dengan intranet, dapat juga berukuran superbesar seperti internet.[5]

The Federal Networking Council (FNC) memberikan definisi mengenai internet dalam resolusinya tanggal 24 Oktober 1995 sebagai berikut:

> *"Internet refers to the global information system that –*
> *(i) is logically linked together by a globally unique address space based in the Internet Protocol (IP) or its subsequent extensions/follow-ons;*
> *(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extension/follow-ons, and/or other Internet Protocol)IP)-compatible protocols; and*
> *(iii) Providers, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein."* [6]

[5] **Agus Raharjo**, 2002, *Cybercrime*, PT Citra Aditya Bakti, Bandung, hal. 59.

[6] *Ibid.*, hal. 60

3. Cyber Crime

Perkembangan teknologi jaringan komputer global atau Internet telah menciptakan dunia baru yang dinamakan *cyberspace*, sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru, yaitu realitas virtual.

Istilah *cyberspace* muncul pertama kali dari novel William Gibson berjudul Neuromancer pada tahun 1984.[7]

Istilah *cyberspace* pertama kali digunakan untuk menjelaskan dunia yang terhubung langsung *(online)* ke internet oleh Jhon Perry Barlow pada tahun 1990.

Secara etimologis, *istilah cyberspace* sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir. Cambridge Advanced Learner's Dictionary memberikan definisi *cyberspace* sebagai *"the Internet considered as an imaginary area without limits where you can meet people and discover information about any subject"*.[8] *The American Heritage Dictionary of English Language Fourth Edition* mendefinisikan cyberspace sebagai *"the electronic medium of computer networks, in which online communication takes place*".[9]

Pengertian *cyberspace* tidak terbatas pada dunia yang tercipta ketika terjadi hubungan melalui internet. Bruce Sterling mendefinisikan *cyberspace* sebagai *the 'place' where a telephone conversation appears to occur.*[10]

---

[7] **William Gibson**, 1984, *Neuromancer*, New York:Ace, hal. 51, dikutip dari Agus Raharjo, op.cit., hal. 92-93.

[8] http://dictionary.cambridge.org

[9] http://www.bartleby.com.

[10] **Bruce Sterling, 1990**, *The Hacker Crackdown, Law and Disorder on the electronic Frontier*, Massmarket Paperback, electronic version available at http://www.lysator.liu.se/etexts/hacker.

Perkembangan teknologi komputer juga menghasilkan berbagai bentuk kejahatan komputer di lingkungan *cyberspace* yang kemudian melahirkan istilah baru yang dikenal dengan *Cybercrime, Internet Fraud*, dan lain-lain.

Collin Barry C. menjelaskan istilah *cybercrime* sebagai berikut :

> *"Term "cyber-crime" is young and created by combination of two words: cyber and crime. The term "cyber" means the cyber-space (terms "virtual space", "virtual world" are used more often in literature) and means (according to the definition in "New hacker vocabulary" by Eric S. Raymond) the informational space modeled through computer, in which defined types of objects or symbol images of information exist – the place where computer programs work and data is processed."* [11]

Computer crime dan *cybercrime* merupakan 2 (dua) istilah yang berbeda sebagaimana dikatakan oleh Nazura Abdul Manap sebagai berikut:

> *"Defined broadly, "computer crime" could reasonably include a wide variety of criminal offences, activities or issues. It also known as a crime committed using a computer as a tool and it involves direct contact between the criminal and the computer…..There is no Internet line involved, or only limited networking used such as the Local Area Network (LAN). Whereas, cyber-crimes are crimes committed virtually through Internet online. This means that the crimes committed could extend to other countries… Anyway, it causes no harm to refer computer crimes as cyber-crimes or vise versa, since they have same impact in law."* [12]

Sebagian besar dari perbuatan *Cybercrime* dilakukan oleh seseorang yang sering disebut dengan *cracker*. Berdasarkan catatan Robert H'obbes'Zakon, seorang internet Evangelist, *hacking* yang dilakukan oleh *cracker* pertama kali terjadi pada tanggal 12 Juni 1995 terhadap The Spot dan tanggal 12 Agustus 1995 terhadap

---

[11] **Collin Barry C.**, 1996, *The Future of CyberTerrorism*, Proceedings of 11th Annual International Symposium on Criminal Justice Issues. The University of Illinois at Chicago, dikutip dari makalah Vladimir Golubev, cyber-crime and legal problems of usage network the INTERNET.

[12] **Nazura Abdul Manap**, *Cyber-crimes: Problems and Solutions Under Malaysian Law*, makalah pada seminar nasional Money Laundering dan Cybercrime dalam Perspektif Penegakan Hukum di Indonesia, diselenggarakan oleh Lab. Hukum Pidana FH Univ. Surabaya, 24 Februari 2001, hal.3.

Crackers Move Page. Berdasarkan catatan itu pula, situs pemerintah Indonesia pertama kali mengalami serangan *cracker* pada tahun 1997 sebanyak 5 (lima) kali.[13]

Kegiatan *hacking* atau *cracking* yang merupakan salah satu bentuk cybercrime tersebut telah membentuk opini umum para pemakai jasa internet bahwa Cybercrime merupakan suatu perbuatan yang merugikan bahkan amoral. Para korban menganggap atau memberi stigma bahwa *cracker* adalah penjahat. Perbuatan *cracker* juga telah melanggar hak-hak pengguna jasa internet sebagaimana digariskan dalam The Declaration of the Rights of Netizens yang disusun oleh Ronda Hauben.[14]

Berdasarkan pemikiran JoAnn L. Miller yang membagi kategori *white collar crime* menjadi empat kategori, yaitu meliputi *organizational occupational crime, government occupational crime, profesional occupational crime,* dan *individual occupatinal crime*, maka Agus Raharjo berpendapat bahwa Cybercrime dapat dikatakan sebagai *white collar crime* dengan kriteria berdasarkan kemampuan profesionalnya.[15]

David I. Bainbridge mengingatkan bahwa pada saat memperluas hukum pidana, harus ada kejelasan tentang batas-batas pengertian dari suatu perbuatan baru yang dilarang sehingga dapat dinyatakan sebagai perbuatan pidana dan juga dapat dibedakan dengan misalnya sebagai suatu perbuatan perdata. [16]

---

[13] **Agus Raharjo**, op. cit., hal. 35-39.
[14] *Ibid*, hal. 44.
[15] *Ibid*, hal. 50-51.
[16] **David I. Bainbridge**, 1993, *Komputer dan Hukum*, Sinar Grafika, Jakarta, hal. 155.

F. Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif yang ditujukan terhadap sistematika hukum[17] khususnya mengenai peristiwa hukum berupa perilaku atau sikap tindak dalam hukum yang digolongkan sebagai perbuatan pidana *(strafbaarfeit)*[18] yang dikenal dengan *cybercrime.*

Penelitian ini bersifat deskriptif analitis, yaitu ditujukan untuk memecahkan masalah cybercrime yang merupakan masalah aktual. Penelitian ini akan menggambarkan bentuk-bentuk cybercrime dan modus operandinya, selanjutnya bentuk-bentuk cybercrime tersebut dianalisa untuk dikualifikasikan dan sedapat mungkin dicari pengaturannya di dalam sistem perundang-undangan Indonesia. Penelitian ini juga berusaha untuk mencari hambatan-hambatan yang terdapat di dalam penyidikan cybercrime dan selanjutnya dianalisa untuk memecahkan masalah.

Data dalam penelitian ini diperoleh dari sumber:

1) Data primer, diperoleh dari wawancara kepada responden yang pernah menangani kasus Cybercrime serta jawaban responden dari angket quesioner yang disebarkan kepada penyidik di wilayah hukum Polda Sumatera Utara.
2) Data sekunder, meliputi bahan hukum primer mencakup buku, kertas kerja konperensi atau seminar, laporan penelitian, majalah, dan lain-lain, bahan hukum sekunder mencakup bibliografi dan penerbitan pemerintah, dan bahan hukum tersier mencakup abstrak perundang-udangan, ensiklopedia hukum, dan lain-lain.[19]

---

[17] **Soerjono Soekanto**, 1986, *"Pengantar Penelitian Hukum"*, cetakan ketiga, Penerbit Universitas Indonesia, Jakarta, hal: 51

[18] **Soerjono Soekanto & Sri Mamudji**, 1995, *"Penelitian Hukum Normatif"*, cetakan keempat, PT RajaGrafindo, Jakarta, hal: 72

[19] **Soerjono Soekanto & Sri Mamudji**, hal: 29-33

G. Peristilahan Operasional

1. Cybercrime

   Setiap bentuk kejahatan yang berkaitan langsung dengan Cyberspace.

   Cyberspace

   Media elektronik yang dihasilkan oleh jaringan komputer yang digunakan sebagai tempat melakukan komunikasi sambungan langsung (*on-line*).

2. Internet

   Sistem informasi global yang menghubungan berbagai jaringan komputer secara bersama-sama dalam suatu ruang global berbasis Internet Protocol ;

H. Hasil Penelitian dan Pembahasan

1. Kualifikasi dan Modus Operandi Cybercrime

Natalie D. Voos di dalam "Crime on The Internet" menguraikan beberapa jenis Cybercrime berdasarkan beberapa issu yang menjadi bahan studi atau penyelidikan pihak FBI dan National White Collar Crime Center sebagai berikut :

a. Computer network break-ins,
b. Industrial espionage,
c. Software piracy,
d. Child pornography,
e. E-mail bombings,
f. Password sniffers,
g. Spoofing,
h. Credit card fraud.[20]

---

[20] **Natalie D Voss**, Copyright © 1994-99 Jones International and Jones Digital Century, "*Crime on The Internet*", Jones Telecommunications & Multimedia Encyclopedia, hal. 1-2, http://www.digitalcentury.com/encyclo/*update/articles.html*..

Pengaturan cybercrime di Amerika Serikat antara lain tercantum dalam Computer Fraud and Abuse Act (Title 18 Part I Chapter 47 Section 1030 dengan judul "Fraud and related activity in connection with computers"). Bentuk-bentuk cybercrime yang diatur dalam ketentuan Section 1030 tersebut adalah sebagai berikut:

"Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -
   (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
   (B) information from any department or agency of the United States; or
   (C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029)[21] in any password or similar information through which a computer may be accessed without authorization, if -
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; "or".

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;"

Selain Computer Fraud and Abuse Act, terdapat berbagai peraturan perundang-undangan yang mengatur perbuatan-perbuatan pidana yang juga dapat menjadi suatu perbuatan "Cybercrime", seperti Access Device Fraud Act (Title 18 USC Section 1029), Wire Fraud Statute (Title 18 USC Section 1343), The Copyright Act of 1976 (Title 18 USC Section 2319), The Trademarks Counterfeit Act of 1984 (Title 18 USC Section 2320), Mail Fraud (Title 18 USC Section 1341), Identity Theft and Assumption Deterrence Act of 1998 (Title 18 USC Section 1028), Unlawful Access to Stored Communications (Title 18 USC Section 2701), dan lain-lain.

Convention on Cybercrime yang diadakan oleh Council of Europe dan terbuka untuk ditandatangani mulai tanggal 23 November 2001 di Budapest menguraikan jenis-jenis kejahatan yang harus diatur dalam hukum pidana substantif oleh negara-negara pesertanya, terdiri dari:

[21] Section 1029 mengatur tentang "Fraud and related activity in connection with access devices".

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems (Tindak pidana yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer):

Article 2 – *Illegal access* (melakukan akses tidak sah)

Article 3 – *Illegal interception* (intersepsi secara tidak sah)

Article 4 – *Data interference* (menggangu data)

Article 5 – *System interference* (mengganggu pada sistem)

Article 6 – *Misuse of devices* (menyalahgunakan alat)

Title 2 – Computer-related offences (Tindak pidana yang berkaitan dengan komputer):

Article 7 – *Computer-related forgery* (pemalsuan melalui komputer)

Article 8 – *Computer-related fraud* (penipuan melalui komputer)

Title 3 – Content-related offences (Tindak pidana yang berhubungan dengan isi atau muatan data atau sistem komputer)

Article 9 – *Offences related to child pornography* (Tindak pidana yang berkaitan dengan pornografi anak)

Title 4 – Offences related to infringements of copyrightand related rights (Tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak-hak terkait).

Kejahatan *fraud* sedang menjadi trend bagi beberapa kalangan pengguna jasa internet. Channel #cc, #ccs, #cchome atau #cvv2 pada server-server IRC favorit, seperti: DALnet, UnderNet dan Efnet banyak dikunjungi orang dari seluruh dunia untuk mencari kartu-kartu kredit bajakan dengan harapan dapat digunakan sebagai alat pembayaran ketika mereka berbelanja lewat Internet.

Dalam dunia Internet, kegiatan ilegal tersebut dikenal dengan istilah *carding*, sedangkan orang yang membajak kartu kredit disebut sebagai *carder* atau *frauder*.

Modus Kejahatan Kartu Kredit (Carding) umumnya berupa :

1) Mendapatkan nomor kartu kredit (CC) dari tamu hotel.
2) Mendapatkan nomor kartu kredit melalui kegiatan *chatting* di Internet.
3) Melakukan pemesanan barang ke perusahaan di luar negeri dengan menggunakan Jasa Internet.
4) Mengambil dan memanipulasi data di Internet.
5) Memberikan keterangan palsu, baik pada waktu pemesanan maupun pada saat pengambilan barang di Jasa Pengiriman (kantor pos, UPS, Fedex, DHL, TNT, dsb.).

Contoh kasus kejahatan kartu kredit melalui internet dapat dikemukakan dari suatu hasil penyidikan pihak Korps Reserse POLRI Bidang Tindak Pidana Tertentu di Jakarta terhadap tersangka berinisial BRS, seorang Warga Negara Indonesia yang masih berstatus sebagai mahasiswa Computer Science di Oklahoma City University USA. Ia disangka melakukan tindak pidana penipuan dengan menggunakan sarana internet, menggunakan nomor dan kartu kredit milik orang lain secara tidak sah untuk mendapatkan alat-alat musik, komputer dan Digital Konverter serta menjualnya, sebagaimana diatur dan diancam pidana dalam Pasal 378 atau 263 atau 480 KUHP.

Tersangka mendapatkan nomor-nomor kartu kredit secara acak melalui Search Engine mencari “Program Card Generator” di Internet. Tersangka menggunakan Program Card Generator versi IV, kemudian hasil dari generator tersebut disimpan Tersangka dalam file di “My Document” dan sebagian dari nomor-nomor itu digunakan Tersangka untuk melakukan transaksi di Internet. Selain itu Tersangka mendapatkan nomor-nomor kartu kredit dari saluran MIRC “JOGYA CARDING “.

Cara Tersangka menggunakan kartu kredit secara tidak sah sehingga mendapatkan barang yang diinginkannya adalah sebagai berikut:

Pertama, Tersangka Online menggunakan internet, kemudian Tersangka membuka situs : www.PCVideoOnline.com lalu memilih komputer laptop yang akan dibeli dan dimasukan ke *Shoping Bag*.

Kedua, setelah barang-barang yang diperlukan atau yang akan dibeli dirasa cukup, kemudian Tersangka menekan (klik) tombol Checkout dan selanjutnya mengisi formulir tentang informasi pembayaran dan informasi tujuan pengiriman. Dalam informasi pembayaran Tersangka mengetikkan nama, alamat tempat tinggal, dan alamat email. Dalam informasi tujuan tersangka mengetikkan data yang sama.

Ketiga, Tersangka memilih metode pengiriman barang dengan menggunakan perusahaan jasa pengriman ***UPS*** (United Parcel Service).

Keempat, Tersangka melakukan pembayaran dengan cara memasukkan atau mengetikkan nomor kartu kredit, mengetikan data Expire Date (masa berlakunya), kemudian menekan tombol (klik) Submit.

Terakhir, Tersangka mendapatkan email/invoice konfirmasi dari pedagang tersebut ke email Tersangka bahwa kartu kredit yang digunakan valid dan dapat diterima, email tersebut disimpan Tersangka di salah satu file di komputer Tersangka.

Cara Tersangka mengambil barang dari perusahaan jasa pengiriman adalah melalui seseorang berinisial PE yang berdasarkan referensi dari seorang karyawan perusahaan jasa pengiriman AIRBORNE EXPRESS dapat memperlancar pengeluaran paket kiriman. Tersangka memberi Tracking Number kepada PE, kemudian PE yang mengeluarkan paket kiriman tersebut dan mengantarnya ke rumah Tersangka.

Contoh modus operandi pelanggaran atau kejahatan terhadap hak milik intelektual dengan menggunakan komputer sebagai alat dapat dilihat dari *press realease* yang dikeluarkan oleh U.S. Department of Justice United States Attorney Western District of Washington pada tanggal 1 Maret 2001. Jaksa Wilayah Barat Washington Katrina C. Pflaumer dan Agen Khusus Federal Bureau of Investigation (FBI) Divisi Seattle Charles Mandigo mengajukan tuntutan kepada RYAN M. CAREY dengan tuduhan melakukan "*criminal copyright offense*" melanggar Pasal 18 United States Code, ayat 2319 dan Pasal 17 United States Code ayat 506(a)(2) karena diduga keras pada kurun waktu 30 Maret 2000 sampai dengan 31 Mei 2000 telah mengoperasikan situs "maccarey.com" yang menggandakan secara ilegal salinan (copies) video game produksi Nintendo Game Boy, NES dan Super NES yang dapat di-*download* secara gratis melalui Internet dan dapat dimainkan oleh orang yang telah men-*download*-nya di PC mereka masing-masing.

Berdasarkan bentuk-bentuk kejahatan sebagaimana telah dikemukakan oleh beberapa penulis serta memperhatikan kasus-kasus cybercrime yang sering terjadi, maka Peneliti mencoba membuat sendiri kualifikasi cybercrime sebagai berikut:

1) Tindak pidana yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer:
    a) **Illegal access** (akses secara tidak sah terhadap sistem komputer), yaitu dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain. *Hacking* merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi.

b) **Data interference** (mengganggu data komputer), yaitu dengan sengaja melakukan perbuatan merusak, menghapus, memerosotkan (*deterioration*), mengubah atau menyembunyikan (*suppression*) data komputer tanpa hak. Perbuatan menyebarkan virus komputer merupakan salah satu dari jenis kejahatan ini yang sering terjadi.

c) **System interference** (mengganggu sistem komputer), yaitu dengan sengaja dan tanpa hak melakukan gangguan terhadap fungsi sistem komputer dengan cara memasukkan, memancarkan, merusak, menghapus, memerosotkan, mengubah, atau menyembunyikan data komputer. Perbuatan menyebarkan program virus komputer dan *E-mail bombings* (surat elektronik berantai) merupakan bagian dari jenis kejahatan ini yang sangat sering terjadi.

d) **Illegal interception in the computers, systems and computer networks operation** (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer), yaitu dengan sengaja melakukan intersepsi tanpa hak, dengan menggunakan peralatan teknik, terhadap data komputer, sistem komputer, dan atau jaringan operasional komputer yang bukan diperuntukkan bagi kalangan umum, dari atau melalui sistem komputer, termasuk didalamnya gelombang elektromagnetik yang dipancarkan dari suatu sistem komputer yang membawa sejumlah data. Perbuatan dilakukan dengan maksud tidak baik, atau berkaitan dengan suatu sistem komputer yang dihubungkan dengan sistem komputer lainnya.

e) **Data Theft** (mencuri data), yaitu kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. *Identity theft* merupakan salah satu dari jenis kejahatan ini yang sering

diikuti dengan kejahatan penipuan *(fraud)*. Kejahatan ini juga sering diikuti dengan kejahatan *data leakage*.

f) **Data leakage and espionage** (membocorkan data dan memata-matai), yaitu kegiatan memata-matai dan atau membocorkan data rahasia baik berupa rahasia negara, rahasia perusahaan, atau data lainnya yang tidak diperuntukkan bagi umum, kepada orang lain, suatu badan atau perusahaan lain, atau negara asing."

g) **Misuse of devices** (menyalahgunakan peralatan komputer), yaitu dengan sengaja dan tanpa hak, memproduksi, menjual, berusaha memperoleh untuk digunakan, diimpor, diedarkan atau cara lain untuk kepentingan itu, peralatan, termasuk program komputer, password komputer, kode akses, atau data semacam itu, sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan digunakan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain.

2) Tindak pidana yang menggunakan komputer sebagai alat kejahatan:

a) **Credit card fraud** (penipuan kartu kredit);

b) **Bank fraud** (penipuan terhadap bank);

c) **Service Offered fraud** (penipuan melalui penawaran suatu jasa);

d) **Identity Theft and fraud** (pencurian identitas dan penipuan);

e) **Computer-related fraud** (penipuan melalui komputer);

f) **Computer-related forgery** (pemalsuan melalui komputer);

g) **Computer-related betting** (perjudian melalui komputer);

h) **Computer-related Extortion and Threats** (pemerasan dan pengancaman melalui komputer).

3) Tindak pidana yang berkaitan dengan isi atau muatan data atau sistem komputer:
   a) **child pornography** (pornografi anak);
   b) **infringements of copyright and related rights** (pelanggaran terhadap hak cipta dan hak-hak terkait);
   c) drug traffickers (peredaran narkoba), dan lain-lain.

2. Pengaturan Cybercrime dalam Perundang-undangan Indonesia

Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer termasuk cybercrime. Mengingat terus meningkatnya kasus-kasus cybercrime di Indonesia yang harus segera dicari pemecahan masalahnya maka beberapa peraturan baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan berikut ini:

1) **Illegal access** (akses secara tidak sah terhadap sistem komputer)

Perbuatan melakukan akses secara tidak sah terhadap sistem komputer belum ada diatur secara jelas di dalam sistem perundang-undangan di Indonesia. Untuk sementara waktu, Pasal 22 Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi dapat diterapkan.

Pasal 22 Undang-Undang Telekomunikasi menyatakan:

> "Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:
> a. akses ke jaringan telekomunikasi; dan/atau
> b. akses ke jasa telekomunikasi; dan/atau
> c. akses ke jaringan telekomunikasi khusus."

Pasal 50 Undang-Undang Telekomunikasi memberikan ancaman pidana terhadap barang siapa yang melanggar ketentuan Pasal 22 Undang-Undang

Telekomunikasi dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

2) **Data interference** (mengganggu data komputer) dan **System interference** (mengganggu sistem komputer)

Pasal 38 Undang-Undang Telekomunikasi belum dapat menjangkau perbuatan *data interference* maupun *system interference* yang dikenal di dalam Cybercrime.

Jika perbuatan *data interference* dan *system interference* tersebut mengakibatkan kerusakan pada komputer, maka Pasal 406 ayat (1) KUHP dapat diterapkan terhadap perbuatan tersebut.

3) **Illegal interception in the computers, systems and computer networks operation** (intersepsi secara tidak sah terhadap operasional komputer, sistem, dan jaringan komputer)

Pasal 40 Undang-Undang Telekomunikasi dapat diterapkan terhadap jenis perbuatan intersepsi ini. Pasal 56 Undang-Undang Telekomunikasi memberikan ancaman pidana terhadap barang siapa yang melanggar ketentuan Pasal 40 tersebut dengan pidana penjara paling lama 15 (lima belas) tahun.

4) **Data Theft** (mencuri data)

Perbuatan melakukan pencurian data sampai saat ini tidak ada diatur secara khusus, bahkan di Amerika Serikat sekalipun. Pada kenyataannya, perbuatan *Illegal access* yang mendahului perbuatan *data theft* yang dilarang, atau jika *data thef* diikuti dengan kejahatan lainnya, barulah ia menjadi suatu kejahatan bentuk lainnya, misalnya *data leakage and espionage* dan *identity theft and fraud*.

Pencurian data merupakan suatu perbuatan yang telah mengganggu hak pribadi seseorang, terutama jika si pemiik data tidak menghendaki ada orang lain yang mengambil atau bahkan sekedar membaca datanya tersebut. Jika para ahli hukum sepakat menganggap bahwa perbuatan ini dapat dimasukkan sebagai perbuatan pidana, maka untuk sementara waktu Pasal 362 KUHP dapat diterapkan.

5) **Data leakage and espionage** (membocorkan data dan memata-matai)

Perbuatan membocorkan dan memata-matai data atau informasi yang berisi tentang rahasia negara diatur di dalam Pasal 112, 113, 114, 115 dan 116 KUHP.

Pasal 323 KUHP mengatur tentang pembukaan rahasia perusahaan yang dilakukan oleh orang dalam (*insider*). Sedangkan perbuatan membocorkan data rahasia perusahaan dan memata-matai yang dilakukan oleh orang luar perusahaan dapat dikenakan Pasal 50 jo. Pasal 22, Pasal 51 jo. Pasal 29 ayat (1), dan Pasal 57 jo. Pasal 42 ayat (1) Undang-Undang Telekomunikasi.

6) **Misuse of devices** (menyalahgunakan peralatan komputer),

Perbuatan Misuse of devices pada dasarnya bukanlah merupakan suatu perbuatan yang berdiri sendiri, sebab biasanya perbuatan ini akan diikuti dengan perbuatan melawan hukum lainnya.

Sistem perundang-undangan di Indonesia belum ada secara khusus mengatur dan mengancam perbuatan ini dengan pidana. Hal ini tidak menjadi persoalan, sebab yang perlu diselidiki adalah perbuatan melawan hukum apa yang mengikuti perbuatan ini. Ketentuan yang dikenakan bisa berupa penyertaan (Pasal 55 KUHP), pembantuan (Pasal 56 KUHP) ataupun langsung diancam dengan ketentuan yang mengatur tentang perbuatan melawan hukum yang menyertainya.

7) **Credit card fraud** (penipuan kartu kredit)

Penipuan kartu kredit merupakan perbuatan penipuan biasa yang menggunakan komputer dan kartu kredit yang tidak sah sebagai alat dalam melakukan kejahatannya sehingga perbuatan tersebut dapat diancam dengan Pasal 378 KUHP.

8) **Bank fraud** (penipuan bank)

Penipuan bank dengan menggunakan komputer sebagai alat melakukan kejahatan dapat diancam dengan Pasal 362 KUHP atau Pasal 378 KUHP, tergantung dari modus operandi perbuatan yang dilakukannya.

9) **Service Offered fraud** (penipuan melalui penawaran suatu jasa)

Penipuan melalui penawaran jasa merupakan perbuatan penipuan biasa yang menggunakan komputer sebagai salah satu alat dalam melakukan kejahatannya sehingga dapat diancam dengan Pasal 378 KUHP.

10) **Identity Theft and fraud** (pencurian identitas dan penipuan)

Pencurian identitas yang diikuti dengan melakukan kejahatan penipuan dapat diancam dengan Pasal 362 KUHP atau Pasal 378 KUHP, tergantung dari modus operandi perbuatan yang dilakukannya.

11) **Computer-related fraud** (penipuan melalui komputer)

Penipuan melalui komputer juga merupakan perbuatan penipuan biasa yang menggunakan komputer sebagai alat dalam melakukan kejahatannya sehingga perbuatan tersebut dapat diancam pidana dengan Pasal 378 KUHP.

12) **Computer-related forgery** (pemalsuan melalui komputer)

Pemalsuan melalui komputer dapat dikenakan Pasal 378 KUHP atau Undang-Undang tentang Hak Cipta, Paten, dan Merk. Hal ini disesuaikan dengan modus operandi kejahatan yang terjadi.

13) **Computer-related betting** (perjudian melalui komputer)

Perjudian melalui komputer merupakan perbuatan melakukan perjudian biasa yang menggunakan komputer sebagai alat dalam operasinalisasinya sehingga perbuatan tersebut dapat diancam dengan Pasal 303 KUHP.

14) **Computer-related Extortion and Threats** (pemerasan dan pengancaman melalui komputer).

Pemerasan dan pengancaman melalui komputer merupakan perbuatan pemerasan biasa yang menggunakan komputer sebagai alat dalam operasinalisasinya sehingga perbuatan tersebut dapat diancam dengan Pasal 368 KUHP.

15) **Child pornography** (pornografi anak)

Perbuatan memproduksi, menawarkan, dan menyebarkan pornografi anak melalui sistem komputer dapat diancam dengan Pasal 282 KUHP. Perbuatan mendapatkan pornografi anak belum ada diatur di dalam undang-undang dan perlu segera diatur mengingat semakin banyaknya peminat pornografi anak akan memacu semakin meningkatnya pula produksi, penawaran, dan peredaran pornografi anak.

16) **Infringements of copyright and related rights** (pelanggaran terhadap hak cipta dan hak-hak terkait)

Pelanggaran hak cipta dan hak-hak terkait dapat diancam dengan ketentuan pidana yang terdapat di dalam Undang-Undang Hak Cipta dan hak-hak terkait.

Kejahatan ini bisa tergolong menjadi cybercrime disebabkan perbuatan yang secara insidental melibatkan penggunaan komputer dalam pelaksanaannya.

17) **drug traffickers** (peredaran narkoba);

Peredaran narkotika dan obat-obatan terlarang juga merupakan suatu perbuatan biasa yang disebabkan secara insidental melibatkan penggunaan komputer dalam pelaksanaannya sehingga digolongkan pula sebagai cybercrime. Oleh karena itu, perbuatan *drug traffickers* dapat diancam pidana sesuai dengan ketentuan yang diatur dalam Undang-Undang No. 5 Tahun 1997 tentang Psikotropika dan Undang-Undang Nomor 22 Tahun 1997 tentang Narkotika.

3. Permasalahan dalam Penyidikan terhadap Cybercrime

Berdasarkan hasil penelitian yang dilakukan, hambatan-hambatan yang ditemukan di dalam proses penyidikan antara lain adalah sebagai berikut:

1) Perangkat hukum yang belum memadai

Penulis telah menyebarkan tiga puluh angket kepada 30 orang responden yang bertugas sebagai penyidik di lingkungan unit tugas Serse POLDA Sumatera Utara. Seluruh responden mengaku telah mengetahui tentang cybercrime dan yakin bahwa cybercrime telah terjadi di Sumatera Utara, namun para responden masih menganggap lemahnya peraturan perundang-undangan yang dapat diterapkan terhadap pelaku cybercrime, sedangkan penggunaan pasal-pasal yang terdapat di dalam KUHP seringkali masih cukup meragukan bagi penyidik. 2 orang responden yang menganggap telah ada Undang-Undang yang mengatur tentang cybercrime merujuk kepada Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi. Seluruh responden sependapat bahwa perlu dibuat undang-undang yang khusus mengatur cybercrime.

2) Kemampuan penyidik

Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (determinan) adalah:

a. Kurangnya pengetahuan tentang komputer.
b. Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus cybercrime masih terbatas.
c. Faktor sistem pembuktian yang menyulitkan para penyidik.

Dari penelitian dilakukan, ternyata masih sangat kurang jumlah penyidik yang pernah terlibat dalam penanganan kasus cybercrime (10%), bahkan dari 30 orang responden yang ada, tidak ada satu orang pun yang pernah mendapat pendidikan khusus untuk melakukan penyidikan terhadap kasus cybercrime.

Dalam hal menangani kasus cybercrime diperlukan penyidik yang cukup berpengalaman (bukan penyidik pemula), pendidikannya diarahkan untuk menguasai teknis penyidikan dan menguasai administrasi penyidikan serta dasar-dasar pengetahuan di bidang komputer dan profil hacker.

3) Alat Bukti

Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap Cybercrime antara lain berkaitan dengan karakteristik kejahatan *cybercrime* itu sendiri, yaitu:

a. Sasaran atau media *cybercrime* adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya. Oleh karena itu, data atau sistem komputer atau internet yang berhubungan dengan

kejahatan tersebut harus direkam sebagai bukti dari kejahatan yang telah dilakukan. Permasalahan timbul berkaitan dengan kedudukan media alat rekaman (*recorder*) yang belum diakui KUHAP sebagai alat bukti yang sah.

b. Kedudukan saksi korban dalam *cybercrime* sangat penting disebabkan cybercrime seringkali dilakukan hampir-hampir tanpa saksi. Di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.[22] Penuntut umum juga tidak mau menerima berkas perkara yang tidak dilengkapi Berita Acara Pemeriksaan Saksi khususnya saksi korban dan harus dilengkapi dengan Berita Acara Penyumpahan Saksi disebabkan kemungkinan besar saksi tidak dapat hadir di persidangan mengingat jauhnya tempat kediaman saksi. Hal ini mengakibatkan kurangnya alat bukti yang sah jika berkas perkara tersebut dilimpahkan ke pengadilan untuk disidangkan sehingga beresiko terdakwa akan dinyatakan bebas. [23]

Mengingat karakteristik cybercrime, diperlukan aturan khusus terhadap beberapa ketentuan hukum acara untuk cybercrime. Pada saat ini, yang dianggap paling mendesak oleh Peneliti adalah pengaturan tentang kedudukan alat bukti yang sah bagi beberapa alat bukti yang sering ditemukan di dalam Cybercrime seperti data atau sistem program yang disimpan di dalam disket, hard disk, chip, atau media recorder lainnya.

4) Fasilitas komputer forensik

---

[22] Hasil wawancara dengan **S. Sinurat**, penyidik pada Resum Unit Bunuh & Culik pada Direktorat Reserse POLDA Sumut yang saat ini sedang menangani sebuah kasus Cybercrime di daerah hukum POLDA-SU Medan.

[23] Hasil wawancara dengan **Tommy Kristanto, S.H., M.Hum**, Jaksa Penuntut Umum yang pernah menangani berkas perkara hasil penyidikan Cybercrime ketika bertugas di Seksi Tindak Pidana Khusus pada Kejaksaan Tinggi Yogyakarta pada tahun 2002.

Untuk membuktikan jejak-jejak para *hacker*, *cracker* dan *phreacker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa soft copy (image, program, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas forensic computing yang memadai.

Fasilitas *forensic computing* yang akan didirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu *evidence collection, forensic analysis, expert witness*.[24]

[24] Makalah Drs. Rusbagio Ishak (Kombes Pol/49120373), Kadit Serse Polda Jateng, pada seminar tentang Hacking yang diadakan oleh Majalah NeoTek pada bulan Agustus 2002 di Semarang.

I. Kesimpulan dan Saran

Kesimpulan yang diperoleh dari penelitian terhadap 3 masalah pokok yang dibahas di dalam penelitian ini adalah :

1) Opini umum yang terbentuk bagi para pemakai jasa internet adalah bahwa cybercrime merupakan perbuatan yang merugikan. Para korban menganggap atau memberi stigma bahwa pelaku cybercrime adalah penjahat.

   Modus operandi cybercrime sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi, tetapi jika diperhatikan lebih seksama akan terlihat bahwa banyak di antara kegiatan-kegiatan tersebut memiliki sifat yang sama dengan kejahatan-kejahatan konvensional. Perbedaan utamanya adalah bahwa cybercrime melibatkan komputer dalam pelaksanaannya. Kejahatan-kejahatan yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer perlu mendapat perhatian khusus, sebab kejahatan-kejahatan ini memiliki karakter yang berbeda dari kejahatan-kejahatan konvensional.

2) Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer melalui media internet. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh undang-undang yang saat ini berlaku.

3) Hambatan-hambatan yang ditemukan dalam upaya melakukan penyidikan terhadap cybercrime antara lain berkaitan dengan masalah perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Upaya-upaya yang dapat dilakukan untuk mengatasi hambatan yang ditemukan di dalam melakukan penyidikan terhadap cybercrime antara lain berupa penyempurnaan

perangkat hukum, mendidik para penyidik, membangun fasilitas forensic computing, meningkatkan upaya penyidikan dan kerja sama internasional, serta melakukan upaya penanggulangan pencegahan.

Beberapa hal yang dapat dijadikan sebagai saran sehubungan dengan hasil penelitian terhadap cybercrime adalah sebagai berikut :

1) Undang-undang tentang cybercrime perlu dibuat secara khusus sebagai *lex-spesialis* untuk memudahkan penegakan hukum terhadap kejahatan tersebut.
2) Kualifikasi perbuatan yang berkaitan dengan cybercrime harus dibuat secara jelas agar tercipta kepastian hukum bagi masyarakat khususnya pengguna jasa internet.
3) Perlu hukum acara khusus yang dapat mengatur seperti misalnya berkaitan dengan jenis-jenis alat bukti yang sah dalam kasus cybercrime, pemberian wewenang khusus kepada penyidik dalam melakukan beberapa tindakan yang diperlukan dalam rangka penyidikan kasus cybercrime, dan lain-lain.
4) Spesialisasi terhadap aparat penyidik maupun penuntut umum dapat dipertimbangkan sebagai salah satu cara untuk melaksanakan penegakan hukum terhadap cybercrime.

DAFTAR PUSTAKA

1. Buku

Agus Raharjo, 2002, "Cybercrime", cetakan pertama, PT. Citra Aditya Bakti, Bandung.

Andi Hamzah, 1990, "Aspek-aspek Pidana di Bidang Komputer", cetakan kedua, Sinar Grafika, Jakarta.

----------, 1993, "Hukum Pidana yang Berkaitan dengan Komputer", cetakan pertama, Sinar Grafika, Jakarta.

Asril Sitompul, 2001, "Hukum Internet", cetakan pertama, PT. Citra Aditya Bakti, Bandung.

Bambang Sunggono, 2001, "Metodologi Penelitian Hukum", cetakan ketiga, PT RajaGrafindo Persada,Jakarta.

David I. Bainbridge, 1993, "Komputer dan Hukum", cetakan pertama, Sinar Grafika, Jakarta.

Harahap, M. Yahya, 1988, "Pembahasan Permasalahan dan Penerapan KUHAP", Jilid I dan II ,Pustaka Kartini, Jakarta.

Jhon M. Echols dan Hassan Shadily, 1996, "Kamus Inggeris Indonesia", PT. Gramedia Pustaka Utama, Jakarta.

Jhon Sipropoulus, 1999, "Cyber Crime Fighting, The Law Enforcement Officer's Guide to Online Crime", The Natinal Cybercrime Training Partnership, Introduction.

Lamintang, P.A.F., 1984, "KUHAP dengan Pembahasan Secara Yuridis Menurut Yurisprodensi dan Ilmu Pengetahuan Hukum Pidana", Sinar Baru, Bandung.

Lexy J. Moleong, 1999, "Metode Penelitian Kualitatif, cetakan kesepuluh, Remaja Rosdakarya, Bandung.

Mico Pardosi, 1997, "Kamus Komputer (Standard)", Indah, Surabaya.

----------, 1996, "Pengenalan Komputer", Penerbit Indah, Surabaya.

----------, 2000, "Uraian Lengkap Internet", Penerbit Indah, Surabaya.

Niniek Suparni, 2001, "Masalah Cyberspace", cetakan pertama, Fortun Mandiri Karya, Jakarta.

Soedarto, 1983, "Hukum Pidana dan Perkembangan Masyarakat", Sinar Baru, Bandung.

Soerjono Soekanto, 1986, "Pengantar Penelitian Hukum", cetakan ketiga, Penerbit Universitas Indonesia, Jakarta.

---------- & Sri Mamudji, 1995, "Penelitian Hukum Normatif", cetakan keempat, PT RajaGrafindo, Jakarta.

Suheimi, 1995, "Kejahatan Komputer", cetakan kedua, Andi Offset, Yogyakarta.

"The American College Dictionary", 1961, House Inc., New York.

Van Bemmelen, 1953, "Strafvordering", Leerboek Van het Nederlandsche Strafrecht, Martinus Nykoff'S, Gravenhages.

Widyopramono, 1994, "Kejahatan di Bidang Komputer", cetakan pertama, Pustaka Sinar Harapan, Jakarta.

Winarno Surakhmad, 1990, "Pengantar Penelitian Ilmiah", Dasar, Metoda dan Teknik, Edisi ketujuh, cetakan keempat, Penerbit Tarsito, Bandung

3. Makalah

Heru Soepraptomo, 2001, "Kejahatan Komputer dan Siber serta Antisipasi Pengaturan dan Pencegahannya di Indonesia", makalah disajikan pada Seminar Nasional tentang Cyber Law "Antisipasi Hukum terhadap Transaksi Bisnis melalui Cyber Network" yang diselenggarakan oleh Pusat Studi Hukum dan Kemasyarakatan Graha Kirana bekerjasama dengan Partnership for Economic Growth (PEG) di Hotel Danau Toba International tanggal 30 Januari 20001, Medan.

James K. Robinson, "Internet as the Scene of Crime", makalah disajikan dalam "International Computer Crime Conference", Oslo, 29-31 May 2000.

Mariam Darus Badrulzaman, 2001, "E-Commerce, Tinjauan dari Aspek Keperdataan", makalah disajikan pada Seminar Nasional tentang Cyber Law "Antisipasi Hukum terhadap Transaksi Bisnis melalui Cyber Network" yang diselenggarakan oleh Pusat Studi Hukum dan Kemasyarakatan Graha Kirana bekerjasama dengan Partnership for Economic Growth (PEG) di Hotel Danau Toba International tanggal 30 Januari 20001, Medan.

Himpunan Tata Naskah dan Petunjuk Teknis Penyelesaian Perkara Pidana Umum Kejaksaan Agung R.I, 1994, Buku I.

3. Koran, Majalah, Jurnal dan Publikasi lainnya

Carter, David L., July 1995, "Computer Crime Categories", *Law Enforcement Bulletin*, U. S. Department of Justice: Federal Bureau of Investigation.

Muladi, 22 Agustus 2002, "Kebijakan Kriminal terhadap Cybercrime", Media Hukum Vol. 1 No. 3, Persatuan Jaksa Republik Indonesia.

Natalie D Voss, Copyright © 1994-99 Jones International and Jones Digital Century , "Crime on The Internet", Jones Telecommunications & Multimedia Encyclopedia, *http//www.digitalcentury.com/encyclo/update/ articles.html.*

Pattiradjawane, Rene L., "Media Konverjensi dan Tantangan Masa Depan", Kompas, 21 Juli 2000.

Press Release, U.S. Department of Justice, United States Attorney, Western District of Washington, *http//www.usdoj.gov/usao/waw/press.html*.

US Code Collection, Legal Information Institute (LII), *http//www4.law.cornell. edu/ USCode/credit.html*.

Yosef Ardi, "Meroket, Bisnis E-Commerce", Kompas, 21 Juli 2000.

Rancangan Undang-Undang tentang Informasi dan Transaksi Elektronik (RUU ITE), 2003.

4. Peraturan Perundang-undangan

"Garis-garis Besar Haluan Negara GBHN 1999-2004 TAP MPR NO. IV/ MPR/1999", 1999, Sinar Grafika, Jakarta.

Kejaksaan Republik Indonesia, 1998, "Himpunan Peraturan tentang Tugas dan Wewenang Kejaksaaan", Buku II, diterbitkan oleh Kejaksaan Agung R.I., Jakarta.

Moeljatno, 1994, "Kitab Undang-undang Hukum Pidana", cetakan kesembilanbelas, Bumi Aksara, Jakarta.

Soenarto Soerodibroto, 2000, "KUHP dan KUHAP", Edisi keempat, cetakan kelima, PT RajaGrafindo Persada,Jakarta.

Undang-Undang Telekomunikasi 1999, 2000, cetakan pertama, Sinar Grafika, Jakarta.