BAB III

KEJAHATAN KOMPUTER DAN DELIK YANG DIGUNAKAN UNTUK MENJERATNYA (HASIL PENELITIAN DAN PEMBAHASAN)

Aktifitas teknologi tidak dapat diperkirakan perkembangannya karena perkembangan teknologi dapat terjadi setiap saat dan sangat cepat. Perkembangan teknologi tersebut diikuti dengan perkembangan akibat yang tidak diinginkan diantaranya adalah perbuatan menyimpang akibat dari perkembangan teknologi tersebut. Perkembangan hukum selalu tertinggal dalam rangka merespon perkembangan-perkembangan sosial, ekonomi, dan teknologi di masyarakat yang kemudian berpengaruh atau mengubah masyarakat secara dramatis.

3.1. KASUS-KASUS KEJAHATAN KOMPUTER DI INDONESIA.

Kejahatan-kejahatan yang berhubungan dengan komputer pertama ditemukan di Indonesia dan menjadi kasus yang penting atau *landmark case* adalah kasus manipulasi Bank Bank Rakyat Indonesia (BRI)Yogyakarta pada tahun 1983 dan pada Bank Negara Indonesia (BNI)46 New York pada tahun 1986. Sejak saat itu seiring dengan kemajuan teknologi informasi maka kejahatan komputer tersebut semakin banyak terjadi.

Sesuai dengan KUHAP, instansi penyidik yang menangani penyidikan tindak pidana secara umum adalah POLRI. Untuk menangani permasalahan kejahatan komputer POLRI telah membentuk sebuah unit khusus yaitu Unit V pada Direktorat II Ekonomi dan Khusus pada Bareskrim Mabes POLRI, yang berdiri sejak th 2001 dgn Keputusan Kapolri No. Kep/9/V/2001 tgl 5 Mei 2001. Namun unit tersebut baru berjalan secara maksimal menerima laporan dan menangani kejahatan komputer sejak tahun 2004.

Penyidik Polri dalam melakukan penyidikan menerima laporan dari masyarakat disamping penyidik menemukan sendiri peristiwa-peristiwa yang meresahkan masyarakat. Penuntut Umum dalam hal ini Kejaksaan menerima pelimpahan perkara dari penyidikan yang dilakukan oleh

penyidik Polri. Selama tahun 2005 hingga tahun 2007 Mabes Polri menangani kasus kejahatan komputer[100]:

1. Tahun 2005
    a. Jumlah laporan polisi yang diterima : 4
    b. Dinyatakan lengkap oleh Penuntut Umum : 2
    c. Dalam Proses penyidikan : 2
2. Tahun 2006
    a. Jumlah laporan polisi yang diterima : 23
    b. Telah dilimpahkan ke tahap penuntutan : 2
    c. Dalam proses penyidikan : 7
    d. Dinyatakan lengkap oleh Penuntut Umum : 10
    e. Dihentikan penyidikannya : 3
    f. Belum di proses : 3
3. Tahun 2007
    a. Jumlah laporan polisi yang diterima : 8
    b. Dinyatakan lengkap oleh Penuntut Umum : 2
    c. Dalam proses penyidikan : 6

Kejahatan-kejahatan komputer (*cyber crime)* dapat dikategorikan dengan beberapa cara. Pavan Duggal, Presiden dari *cyberlaws.net and consultant*, mendefinisikan dan mengkategorikan *cyber crime menjadi 3 jenis:*

Cybercrimes can be basically divided into 3 major categories:

1. *Cybercrimes against persons.*
2. *Cybercrimes against property.*
3. *Cybercrimes against government*[101].

Menurut Prof.Mardjono Reksodiputro, pada pembahasan RUU KUHP tahun 1993 mengenai kejahatan komputer terdapat 4 kategori yang dibahas, 3 diantaranya adalah:

1) Pencurian data komputer (mengenai data).
2) Merusak/memasuki komputer (hardware).
3) Permasalahan mengenai privasi.

[100] Data yang didapat pada Mabes Polri, perkara tersebut merupakan perkara yang ditangani oleh Mabes Polri berdasarkan laporan yang ditujukan kepada Mabes Polri.

[101] http://www.crime-research.org/analytics/702/, diakses tanggal 21 April 2008

Dalam kasus-kasus yang ditangani oleh penyidik Polri tersebut, termasuk didalamnya kejahatan yang berhubungan dengan komputer (*computer related crime*) serta kejahatan terhadap komputer. Kasus-kasus yang termasuk kejahatan yang berhubungan dengan komputer serta kejahatan terhadap komputer dapat dikelompokkan:

3.1.1. Pencurian data komputer (mengenai data/*software*)

Kejahatan terhadap harta yang dilakukan dengan menggunakan komputer dan teknologi informasi didominasi oleh kejahatan dengan menggunakan sarana kartu kredit. Dalam kasus-kasus tersebut pelaku menggunakan data atau informasi milik orang lain yang diperoleh dengan cara melawan hukum.

1) Kasus yang terjadi di Jawa Barat

Kasus posisi

Pelaku yang merupakan pegawai PT. NUSEX (perusahaan ekspedisi) pada sekitar bulan April 2003 telah memesan barang dari salah satu toko di Amerika dengan membuka situs MIRC dengan menggunakan kartu kredit. Pelaku mendapatkan nomor-nomor kartu kredit dari beberapa situs diantaranya *Indocarder* atau *Jogjacarding*. Setelah mendapatkan nomor-nomor kartu kredit milik orang lain pelaku masuk ke dalam situs Amazon.Com dan Ebay.com dan masuk menjadi anggota. Setelah itu pelaku melakukan transaksi pembelian barang dengan menggunakan nomor kartu kredit milik orang lain tersebut. Setelah disetujui barang tersebut dikirim ke Indonesia melalui Singapura. Setelah mendapat nomor pengiriman barang, pelaku memberi alamat pengiriman dengan memakai identitas palsu atas nama Jhony Wong dengan alamat di Singapura. Setelah barang sampai di Singapura dengan menggunakan Fedex, kemudian pelaku dapat mengambil barang kiriman dari Amerika melalui ekspedisi Fedex di Singapura, dan kemudian di Indonesia diterima oleh PT. Antar Benua Sukses Mandiri. Barang tersebut dikirim ke Indonesia dengan identitas palsu atas nama Andy Fong yang beralamat di Bandung melalui PT.

Antar Benua Sukses Mandiri. Pelaku menerima barang tersebut menggunakan identitas palsu yang didapat dari internet.

Terhadap perbuatan terdakwa tersebut Penuntut Umum melakukan penuntutan terhadap terdakwa dengan dakwaan:

Dakwaan kesatu

Primair : Pasal 263 ayat (1) KUHP

Subsidiair : Pasal 263 ayat (2) KUHP

Dakwaan kedua

Pasal 362 jo pasal 55 ayat (1) ke- 1c KUHAP

Pada proses persidangan perbuatan pelaku hanya dapat dibuktikan melanggar pasal 263 ayat (2) KUHP karena identitas terdakwa yang dipalsukan saat mengambil barang.

Dalam kasus ini hakim tidak sependapat mengenai pengenaan pasal 362 KUHP. Apabila dilihat dari kasus posisi dimana maksud dari pelaku adalah membeli barang dengan menggunakan identitas palsu milik orang lain, maka dalam kasus tersebut hanya identitas palsu yang digunakan oleh terdakwa saja yang dapat dibuktikan sedangkan esensi dari kasus ini yaitu menimbulkan kerugian bagi pemilik kartu kredit yang digunakan tidak dapat dibuktikan.

2) Kasus yang terjadi di Jogjakarta

Pada tanggal 3 Maret 2001, sekitar pukul 03.00 wib di warnet Naganet Jl Pringgodani Nomor 66 Depok, Sleman, **Petrus Pangkur** melakukan chatting (yaitu menggunakan fasilitas yang tersedia di internet yang memungkinkan seseorang berkomunikasi secara langsung dengan lawan bicara pada saat yang sama) dan minta kartu kredit pada seseorang di Bandung yang namanya sering berubah-ubah dan diberi dua nomor kartu kredit masing-masing :

(1) VISA 4388 5750 4013 6827 expiration date 06/03;

(2) VISA 4388 5750 4013 3003 expiration date 06/03.

Nomor kartu kredit tersebut adalah milik orang lain dan oleh **Petrus Pangkur** namanya telah diubah menjadi "Bony di Obok-obok", selanjutnya **Petrus Pangkur** berbelanja melalui website

http://www.agv.com. Sedangkan **Petrus Pangkur** menggunakan alamat email : kenny-JR@indonet.com dan bonz.2000@lycos.com, dengan alamat Gg. Ujung Brojo 009 Yogyakarta.

Terdakwa memesan helm sepeda motor merek AGV HDI sepeda motor X Vent dan 1 (satu) pasang sarung tangan merek AGV Y-402 putih biru hitam ukuran M seharga $ 365,93, (tiga ratus enam puluh lima koma sembilan tiga sent dollar Amerika) atau Rp 3.293.370,- (tiga juta dua ratus sembilan puluh tiga ribu tiga ratus tujuh puluh rupiah) (kurs 1 US $ = Rp 9.000,-) belum termasuk ongkos kirim. Selanjutnya barang pesanan oleh pihak Perusahaan AGV dikirimkan ke alamat tujuan di Yogyakarta melalui jasa pengiriman UPS. Paket tidak dapat dikirimkan ke alamat yang bersangkutan dengan alasan alamat penerima tidak jelas, sehingga kemudian terdakwa mengambil paket kiriman tersebut di kantor UPS Yogyakarta. Akibat perbuatan terdakwa, Perusahaan AGV di Amerika Serikat yang dalam hal ini diwakili oleh Gian Luca Manzo dirugikan sebesar US $ 499,00 (empat ratus sembilan puluh sembilan dollar Amerika) atau senilai kurang lebih Rp 4.491.000,00 (empat juta empat ratus sembilan puluh satu ribu rupiah)

Berdasarkan tuntutan Jaksa Penunutut Umum, Majelis Hakim memutuskan :

1. Menyatakan terdakwa Petrus Pangkur alias "Bonny Diobok-obok" tidak terbukti secara sah dan meyakinkan melakukan tindak pidana pencurian dalam keadaan yang memberatkan sebagaimana dakwaan kesatu penuntut umum,
2. Menyatakan terdakwa Petrus Pangkur alias "Bonny Diobok-obok" terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "PENIPUAN" sebagaimana dalam dakwaan kedua penuntut umum,

Perkara Petrus Pangkur ini merupakan perkara Cyber Crime dengan cara membeli barang melalui internet dengan menggunakan kartu kredit milik orang lain yang pertama kali terjadi di Indonesia dan berhasil

diungkap oleh jajaran Kepolisian dan diproses ke persidangan oleh Kejaksaan dan Pengadilan Negeri Sleman Yogyakarta

Pasal yang sering digunakan untuk menjerat pelaku dengan modus ini adalah dengan menggunakan pasal 263, 362, 372 dan 378 KUHP.

Pasal 362 KUHP berbunyi :

> "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."

Pasal 372 KUHP berbunyi:

> "Barang siapa dengan sengaja dan melawan hukum memiliki barang sesuatu yang seluruhnya atau sebagaian milik orang lain, tetapi yang ada dalam kekuasaannya bukan karena kejahatan diancam karena penggelapan, dengan pidana penjara paling lama empat tahun atau pidana denda paling banyak sembilan ratus rupiah."

Pasal 378 KUHP berbunyi:

> "Barang siapa dengan maksud menguntungka diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu padanya, atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun.

Dari delik-delik tersebut dapat disimpulkan bahwa perbuatan yang dikriminalisasi dalam KUHP adalah perbuatan melawan hukum terhadap **barang atau benda**. Pengertian benda pada saat Pasal 362 KUHP dibuat hanyalah benda yang berwujud, namun hal tersebut berubag sejak adanya *Electriciteits-arrest atau "arrest listrik"* tanggal 23 Mei 1921. Pada arrest Hoge Raad tersebut, orang juga telah

memasukkan "benda tidak berwujud", dalam hal ini "tenaga listrik" ke dalam pengertiannya[102]. Data atau program yang tersimpan di dalam media penyimpanan disket atau sejenisnya yang tidak dapat diketahui wujudnya, untuk dapat berwujud dapat dilakukan dengan cara menampilkan pada layar komputer atau dengan cara mencetak pada alat pencetak. Dengan demikian data atau program komputer yang tersimpan dapat dikategorikan sebagai benda.

Pengertian "mengambil" pada kejahatan komputer berbeda dengar arti mengambil dalam pengertian sehari-hari. Mengambil sebuah data/informasi dalam jaringan komputer atau biasa "*meng-copy*", adalah merekam data atau program yang tersimpan di dalam suatu media penyimpanan ke media penyimpanan lainnya dengan cara memberikan instruksi-instruksi tertentu pada komputer sehingga data atau program yang asli masih utuh dan tidak berubah dari posisi semula .

Undang-undang maupun pembentuk undang-undang ternyata tidak pernah memberikan suatu penjelasan tertentu yang dimaksud dengan perbuatan "mengambil"[103]. Sedangkan untuk kejahatan komputer (termasuk didalamnya cyber crime) di sini, pengertian mengambil adalah mengambil keuasaan atas benda itu dari pemiliknya untuk kemudian dikuasai dengan cara meng-copy. sehingga perbuatan mengcopy yang dilakukan dengan sengaja tanpa ijin dari pemiliknya dapat dikategorikan sebagai perbuatan "mengambil" sebagaimana yang 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 informasi dan data di internet yang tidak bisa "diambil" oleh para pengguna internet . Pencurian bukan lagi hanya berupa pengambilan barang / material berwujud saja, tetapi juga termasuk pengambilan data secara tidak sah.

---

[102] PAF. LAMINTANG, *Delik-delik Khusus Kejahatan-Kejahatan terhadap Kekayaan*, cetakan pertama (Bandung: Sinar Baru, 1989), hal. 18.

[103] Ibid, hal. 12.

Penggunaan fasilitas *Internet Service Provider* untuk melakukan kegiatan hacking dan cracking erat kaitannya dengan delik pencurian yang diatur dalam Pasal 362 KUHP. Pencuri biasanya lebih mengutamakan memasuki sistem jaringan perusahaan finansial seperti penyimpanan data kartu kredit, komputer-komputer di bank atau situs-situs belanja on-line yang ditawarkan di media internet dan data yang didapatkan secara melawan hukum itu diharapkan memberi keuntungan bagi si pelaku. Keuntungan ini dapat berupa keuntungan langsung (uang tunai) ataupun keuntungan yang didapat dari menjual data ke pihak ketiga (menjual data ke perusahaan pesaing).

Jenis kejahatan ini saat ini telah berubah dengan menggunakan modus operandi yang lainnya. Mabes Polri selama beberapa tahun terakhir menerima laporan adanya kejahatan yang diduga dilakukan dari negara Indonesia yaitu dengan cara menawarkan barang dengan membuka situs (website), sehingga dapat diakses dari hampir seluruh negara. Setelah mendapatkan pembeli pelaku akan meminta pembayaran dengan menggunkan kartu kredit. Pembeli yang telah menyerahkan nomor kartu kreditnya dan setuju untuk membeli sebuah barang akan didebet rekening kartu kreditnya dan akhirnya barang tersebut tidak pernah dikirim kepada pembeli. Beberapa laporan yang telah diterima oleh Mabes Polri mengenai peristiwa tersebut[104]:

TAHUN	NEGARA	JUMLAH KORBAN
2006	Inggris	1 orang
	Jerman	1 orang
	Singapura	2 orang
	Iran	2 orang
	Amerika	6 orang
	Australia	4 orang
	New zeland	3 orang

[104] Data yang didapat dari Unit V Direktorat Tindak Pidana Khusus dan Ekonomi Mabes Polri, dimana laporan tersebut dilaporkan oleh korban melalui perwakilan negaranya di Indonesia.

	Slovenia	1 orang
	Spanyol	1 orang
	Kenya	1 orang
2007	Yunani	2 orang
2008	Hungaria	2 orang
	Yunani	4 Orang

Peristiwa tersebut menimbulkan korban berupa materi milik orang lain, namun kasus-kasus tersebut belum dapat ditindaklanjuti oleh penyidik karena terdapat kesulitan untuk menghadirkan korban sebagai saksi dalam kasus ini. Selain itu kesulitan yang lain adalah belum adanya *single identity* di Indonesia, karena untuk membuka sebuah website dimana seseorang harus menyerahkan identitasnya kepada penyedia jasa website untuk mendapatkan sebuah IP address. Penyidik dalam melacak pemilik website berdasarkan identitas kependudukan akan mengalami kesulitan karena di Indonesia seseorang dapat mempunyai lebih dari satu identitas kependudukan.

Dengan demikian kasus-kasus yang terjadi tersebut berhubungan dengan materi milik orang lain yang dapat berupa materi yang berwujud maupun tidak berwujud (data atau *software*) dan dapat dimasukkan dalam kategori *Cybercrimes against property.*

3.1.2. Merusak/memasuki komputer (hardware).

Merusak atau memasuki komputer adalah persoalan mengenai kejahatan yang ditujukan kepada perangkat keras komputer (hardware). Ketentuan tersebut sangat berkaitan erat dengan kejahatan yang hacking dan craking . Dalam kejahatan komputer (cyber crime), perbuatan perusakan, penghancuran barang mempunyai pengertian suatu perbuatan yang dilakukan dengan suatu kesengajaan untuk merusak / menghancurkan sesuatu yaitu data atau program komputer yang disimpan dalam suatu media penyimpanan data elektronik sehingga akibat perbuatan tersebut data atau program yang dimaksud menjadi tidak dapat dipergunakan lagi. Selain data elektronik suatu web site ataupun hompe page juga dapat menjadi sasaran perusakan tersebut.

Kasus yang menjadi perhatian publik adalah kasus *cracking* website Komisi Pemilihan Umum yang terjadi pada masa Pemilu tahun 2004 serta terhadap website Partai Golkar pada tahun 2006.

1) Kasus cracking website KPU

Pada hari Sabtu (17/4/2004) sekitar pukul 16.30 WIB situs KPU tidak bisa menampilkan datanya mengenai hasil perhitungan suara hasil pemilu legislatif. Informasi ini awalnya datang dari kecamatan Sumbawa. Ternyata setelah dapat dibuka kembali ternyata nama-nama partai politik di Situs Tabulasi Nasional Pemilu 2004 menjadi nama-nama yang sudah diganti. Terdakwa berhasil merubah tabel nama partai yang lucu-lucu seperti Partai Jambu, Partai Kolor Ijo, Partai Dukun Beranak dan Partai Mbah Jambon. Lima hari setelah perbuatannya menembus situs TNP Legislatif, tepatnya Kamis, 22 April 2004, pelaku yang diketahui bernama Dani Firmansyah ditangkap polisi di Yogyakarta. Cara yang dilakukan Dani Firmansyah untuk mengetes tim keamanan server tnp.kpu.go.id dengan cara XSS (Cross Site Scripting) dan SQL Injection. Sedangkan sesuai dengan pembelaan yang diajukan oleh terdakwa bahwa motivasi Dani melakukan serangan ke situs KPU hanya untuk memperingatkan kepada tim TI KPU bahwa sistem TI yang berharga miliaran ternyata tidak secure.

Penuntut Umum melakukan penuntutan terhadap Dani Firmansyah dengan dakwaan alternatif:

Kesatu,

Pasal 22 huruf a Jo. Pasal 50 Undang-Undang No. 36 Tahun 1999 tentangTelekomunikasi,

Kedua,

Pasal 22 huruf b Jo. Pasal 50 Undang-Undang RI. No. 36 Tahun 1999 tentang Telekomunikasi.

Ketiga,

Pasal 22 huruf c Jo. Pasal 50 Undang-Undang UU RI. No. 36 Tahun 1999 tentang Telekomunikasi.

Keempat,

Pasal 38 jo. Pasal 55 Undang-Undang RI Nomor 36 Tahun 1999 tantang Telekomunikasi.

Terhadap dakwaan tersebut Penuntut Umum mengajukan tuntutan bahwa terdakwa terbukti melakukan perbuatan seperti yang didakwakan pada dakwaan ketiga melanggar pasal 22 butir c j.o pasal 50 Undang-Undang No 36 tahun 1999 tentang Telekomunikasi.

Kemudian Majelis Hakim Pengadilan Negeri Jakarta Pusat menjatuhkan vonis terhadap Dani Firmansyah yang diyatakan bersalah melanggar pasal 22 c j.o pasal 50 Undang-Undang No 36 tahun 1999 tentang Telekomunikasi.

Dengan demikian Hakim beranggapan semua unsur dakwaan Penuntut Umum terpenuhi, termasuk anggapan bahwa situs KPU merupakan jaringan telekomunikasi khusus. Hakim mempertimbangkan keterangan dari saksi-saksi ahli, meskipun hakim mencatat adanya keterangan salah satu saksi ahli yang bertentangan. Dalam sebuah persidangan, saksi ahli I Made Wiryana tidak menganggap situs KPU sebagai jaringan telekomunikasi khusus.

2) **Kasus cracking website Partai Golkar.**

Iqra Syafaat, tersangka pelaku *hacking* (*deface*) situs Partai Golkar yaitu dengan cara merubah tampilan situs *www.golkar.or.id*. Perusakan situs Golkar, *www.golkar.or.id*, pertama kali terjadi pada tanggal 9 Juli 2006. Iqra Syafaat seorang lulusan SMU yang sering berjualan buku elektronik (*ebook*) merubah foto beberapa tokoh Golkar pada situsnya menjadi foto gorila putih tersenyum. Pada 10 Juli 2006, tersangka melanjutkan aksinya yaitu halaman muka situs Golkar diisi dengan foto mesum aktris Hollywood dengan tulisan "bersatu untuk malu". Penyerangan situs Golkar itu dilakukan pada tanggal 9-13 Juli 2006. Kemudian, pada tanggal 17 Juli 2006, Partai Golkar melalui pengacaranya Zulhendri Hasan melaporkan hal tersebut ke Mabes Polri. Terhadap kasus tersebut Penuntut Umum melakukan penuntutan terhadap Iqra Syafaat dengan dakwaan alternatif:

Kesatu,

Pasal 22 huruf b jo. Pasal 50 UU RI No.36 Tahun 1999 tentang Telekomunikasi jo. Pasal 64 ayat (1) KUHP

Kedua,

Pasal 406 KUHP. jo Pasal 64 ayat (1) KUHP

Terhadap dakwaan tersebut Penuntut Umum mengajukan tuntutan bahwa terdakwa terbukti melakukan perbuatan seperti yang didakwakan pada dakwaan ketiga melanggar Pasal 22 huruf b jo. Pasal 50 UU RI No.36 Tahun 1999 tentang Telekomunikasi.

Kemudian Majelis Hakim Pengadilan Negeri Jakarta Pusat menjatuhkan vonis terhadap Iqra Syafaat yang diyatakan bersalah melanggar Pasal 22 huruf b jo. Pasal 50 UU RI No.36 Tahun 1999 tentang Telekomunikasi.

Seperti kasus di atas tersebut bahwa pelaku yang memasuki sebuah jaringan komputer dalam hal ini jaringan komputer Komisi Pemilihan Umum dan Partai Golkar dijerat dengan undang-undang mengenai telekomunikasi dimana dalam pasal 1 undang-undang nomor 36 tahun 1999 disebutkan bahwa yang dimaksud dengan telekomunikasi adalah

> *"setiap pemancaran, pengiriman dan atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan,gambar, suara dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya".*

Dalam kasus Dani Firmansyah dituntut dengan aturan pasal 22 huruf c undang-undang nomor 36 tahun 1999 yang berbunyi:

> *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.*

Penuntut Umum maupun Hakim dalam kasus sependapat bahwa jaringan internet yang digunakan oleh KPU adalah termasuk dalam

kategori "jaringan khusus". Pada pasal 1 ayat (15) undang-undang dimaksud disebutkan "Penyelenggaraan telekomunikasi khusus adalah penyelenggaraan telekomunikasi yang sifat, peruntukan, dan pengoperasiannya khusus" sedangkan dalam pasal 1 ayat (2) disebutkan bahwa "Alat telekomunikasi adalah setiap alat perlengkapan yang digunakan dalam bertelekomunikasi" bahwa yang dimaksud "setiap perlengkapan yang digunakan dalam bertelekomunikasi" dalam undang-undang ini adalah jaringan komunikasi secara umum dan bukan dikhususkan untuk jaringan internet. Dalam kasus ini website milik KPU dimasukkan ke dalam jaringan komunikasi khusus Sehingga dalam proses penuntutan dan persidangan kasus ini terjadi interpretasi pasal oleh Penuntut Umum dan Hakim.

Dalam pembelaan yang dilakukan oleh terdakwa disebutkan bahwa maksud terdakwa melakukan hal tersebut dapat diibaratkan situs KPU sebagai rumah yang terbakar. Dani Firmansyah menyebut tindakannya telah mencegah timbulnya 'kebakaran yang lebih besar'. Kebakaran tersebut, bisa terjadi karena adanya celah keamanan yang tidak ditutup yang tidak diketahui oleh KPU. Pelaku mengibaratkan perbuatannya tersebut adalah sebagai tindakan masuk lewat jendela untuk menyelamatkan rumah yang terbakar. Sehingga menurut Dani Firmansyah Akibat perbuatannya, KPU kemudian memperbaiki keamanan situs mereka. "Apa yang saya lakukan adalah kontribusi saya sebagai warga negara yang baik."

Dari dua kasus yang relatif sama diatas, baik Penuntut Umum maupun Hakim mempunyai penafsiran yang berbeda terhadap akses ke ke dalam website (situs). Pada kasus website KPU Penuntut Umum dan Hakim menginterpretasikan website KPU sebagai "Jaringan telekomunikasi khusus" dan di dalam kasus website Golkar Penuntut Umum dan Hakim menginterpretasikan website Golkar sebagai "jasa telekomunikasi".

Pada kasus hacking seperti yang terjadi pada situs KPU tersebut berbeda dengan kasus penipuan kartu kredit seperti yang telah dibahas

sebelumnya. Pada kasus ini kerugian yang diderita serta korbannya tidak dapat ditentukan secara pasti, menurut KPU mereka dirugikan dengan adanya perbuatan Dani Firmansyah tersebut sedangkan menurut Dani Firmansyah perbuatannya tersebut justru menyelamatkan situs KPU karena dapat diketahui kelemahan-kelamahan hingga dapat diperbaiki.

Perbuatan memasuki jaringan komputer pihak lain merupakan perbuatan yang dianggap oleh korban maupun penegak hukum sebagai perbuatan menyimpang namun belum terdapat aturan yang memadai untuk menjerat pelaku. Korban dalam hal ini pihak yang merasa daerah yang terbatas telah dimasuki oleh pihak yang tidak berhak untuk memasuki daerah tersebut. Sehingga aparat penegak hukum (Polisi, Jaksa dan Hakim) menggunakan cara menginterpretasikan pasal di dalam sebuah undang-undang untuk menjerat pelaku.

Selain ketentuan tersebut diatas yang dipergunakan oleh aparat penegak hukum, terdapat beberapa pasal dalam KUHP dapat diinterpretasikan guna menjerat pelaku seperti kasus DANI FIRMANSYAH yaitu Ketentuan mengenai perbuatan perusakan dan penghancuran suatu barang diatur di dalam pasal 406 sampai dengan pasal 412 KUHP.

Pasal 406 ayat (1) KUHP berbunyi :

(1). Barangsiapa dengan sengaja melawan hukum menghancurkan, merusakkan, 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.

Pengertian-pengertian dalam pasal 406 KUHP dapat dijelaskan diantaranya adalah sebagai berikut[105]:

(1). Pengertian "membuat tidak dapat dipakai lagi"

[105] PAF. LAMINTANG, op cit, hal. 296.

Unsur tersebut dapat diartikan sebagai "membuat sehingga tidak dapat dipakai sesuai kegunaannya".Kaitannya dengan kejahatan komputer (cyber crime) adalah perbuatan yang dilakukan tersebut menyebabkan data atau program yang tersimpan dalam media penyimpan menjadi tidak dapat digunakan. Hal ini disebabkan oleh data atau program telah dirubah atau dihapus sebagian atau seluruhnya.

(2). Pengertian menghilangkan

Pengertian menghilangkan adalah berbuat sesuatu sehingga barang itu tidak ada lagi. Dalam hal ini perbuatan menghilangkan atau menghapus data yang tersimpan pada media penyimpanan atau pada sebuah *web* atau sejenisnya sehingga mengakibatkan semua atau sebagian dari data atau program menjadi hilang.

Berdasarkan pengertian-pengertian mengenai perbuatan "membuat tidak dapat dipakai lagi" dan "menghilangkan" maka kriminalisasi tersebut mempunyai kesesuaian makna, yaitu pada intinya melarang melakukan perbuatan yang menyebabkan fungsi dari data atau program dalam suatu jaringan menjadi berubah / berkurang.

Perbuatan penghancuran atau perusakkan barang yang dilakukan *cracker* dengan kemampuan *hacking*-nya adalah perbuatan yang hanya bisa dilakukan oleh orang-orang tertentu. Kemampuan tersebut dimiliki secara khusus oleh orang yang mempunyai keahlian dan kreatifitas dalam memanfaatkan sistem, program, maupun jaringan. Motif untuk kejahatan ini sangat beragam; dalam kedua kasus di atas, motif yang terlihat hanyalah karena kesenangan saja.

3.1.3. Kejahatan terhadap privasi

Pada era teknologi informasi pada suatu saat seluruh informai dan data akan disimpan dan ditransfer melalui jaringan komputer. Jika hal tersebut terjadi maka privasi menjadi hal yang perlu diperhatikan. Privasi tersebut merupakan hak setiap orang dimana didalamnya terkandung beberapa aspek seperti terhadap personality, data dan

komunikasi. Aspek-apek tersebut hendaknya dapat dilindungi oleh hukum.

Terdapat sebuah kasus yang sampai saat ini Penuntut Umum (Kejaksaan Tinggi DKI) belum dapat menerima hasil penyidikan yang dilakukan oleh penyidik (Mabes Polri).

Kasus Posisi

Tersangka Joko (nama samaran) mempunyai hubungan khusus dengan seseorang yaitu saksi Bunga (nama samaran). Pada masa itu A dan B pernah menginap di sebuah hotel X pada tahun 2005. Pada saat menginap di hotel X tersebut Joko merayu Bunga untuk diambil foto dalam keadaan tanpa busana. Pada saat melakukan tersebut Joko berjanji tidak akan menyebarkan foto tersebut karena foto tersebut hanya untuk konsumsi pribadi Agus.Kemudian pada bulan Pebruari tahun 2006 hubungan antara Joko dan Bunga tersebut putus.

Beberapa waktu kemudian foto-foto Bunga yang diambil oleh Joko tersebut beredar di internet dan dapat diakses oelh siapa saja lewat situs www.kaskus.com serta www.image.com. Karena itu Bunga melaporkan peristiwa tersebut ke Polisi.

Berdasarkan laporan tersebut penyidik menemukan sebagai bukti awal, komputer (CPU), hard disk dan barang-barang lain milik tersangka. Setelah dilakukan analisa terhadap barang bukti dan keterangan yang diperoleh dari para saksi dan tersangka, penyidik menjerat Joko dengan sangkaan pasal 282 ayat (1) KUHP dan pasal 335 KUHP. Pasal 282 ayat (1) berbunyi:

> Barang siapa menyiarkan, mempertunjukkan atau menempelkan di muka umum tulisan, gambaran atau benda yang telah diketahui isinya melanggar kesusilaan, atau barang siapa dengan maksud untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membikin tulisan, gambaran atau benda tersebut, memasukkannya ke dalam negeri, meneruskannya, mengeluarkannya dari negeri, atau memiliki persediaan, ataupun barang siapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkannya atau

menunjukkannya sebagai bisa diperoleh, diancam dengan pidana penjara paling lama satu tahun enam bulan atau pidana denda paling tinggi empat ribu lima ratus rupiah.

Sedangkan pasal 335 berbunyi:

(1). Diancam dengan pidana penjara paling lama satu tahun atau denda paling banyak empat ribu lima ratus rupiah:

1. barang siapa secara melawan hukum memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu, dengan memakai kekerasan, sesuatu perbuatan lain maupun perlakuan yang tak menyenangkan, atau dengan memakai ancaman kekerasan, sesuatu perbuatan lain maupun perlakuan yang tak menyenangkan, baik terhadap orang itu sendiri maupun orang lain;
2. barang siapa memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu dengan ancaman pencemaran atau pencemaran tertulis.

(2). Dalam hal sebagaimana dirumuskan dalam butir 2, kejahatan hanya dituntut atas pengaduan orang yang terkena.

Penuntut Umum sependapat dengan penyidik pada penerapan pasal yang disngkakan kepada tersangka. Hal ini dapat dilihat dari petunjuk (P-19) yang diberikan kepada penyidik hanya terhadap permasalahan alat bukti yang digunakan seperti:

(1) Agar ditambahkan ahli dari external Polri (Perguruan Tinggi atau profesional pada teknologi informatika).

(2) Agar diambil keterangan pihak Star One dan pihak Kaskus.com untuk mengetahui apakah tersangka melakukan upload atau download.

(3) Agar ditanyakan kepada ahli tentang kegunaan dan cara kerja software komputer forensik EnCase versi 4 dan Forensik Tool Kit (FTK), Hardware Write Blocker, sebagaimana penjelasan ahli pada nomor 5.

Kasus-kasus yang diambil sebagai contoh tersebut diatas seluruhnya menggunakan interpretasi pasal-pasal yang ada dalam undang-undang. Interpretasi yang digunakan tersebut pada umumnya adalan penafsiran *ekstensif*, yakni menafsirkan dengan memperluas arti suatu istilah atau pengertian dalam (pasal) undang-undang[106]. Penafsiran secara ekstensif tersebut merupakan penafsiran pada tingkatan yang paling akhir[107]. Dengan penafsiran secara ekstensif tersebut maka dapat dikatakan terdapat perbuatan-perbuatan yang ditarik menjadi sebuah tindak pidana dengan rumusan pasal yang secara gramatikal, sistimatikal, historikal dan teleologikal bukan dimaksudkan untuk perbuatan tersebut. Namun berbeda dengan apa yang disampaikan oleh Prof. Jan Remmelink bahwa kita tidak akan menemukan urutan prioritas penggunaan pelbagai metode interpretasi. Paling jauh kita dapat mengatakan bahwa di dalam hukum pidana, metode gramatikal menempati urutan lebih penting dibandingkan dengan hukum keperdataan[108].

Untuk menentukan sebuah perbuatan menjadi sebuah perbuatan yang dapat dipidana terdapat berbagai pendapat para ahli. Seperti yang telah dikemukakan oleh Roeslan Saleh bahwa respon hukum pidana atas suatu fenomena dimaksudkan untuk melindungi kepentingan-kepentingan masyarakat, lebih lanjut Harkristuti Harkrisnowo menyatakan bahwa sesuai dengan pendapat Jeremy Bentham,

---

[106] Purnadi Purbacaraka dan Soerjono Soekanto, *Prundang-undangan dan Yurisprudensi*, cetakan ke-IV, Bandung, PT. Citra Aditya Bakti, hal.14.

[107] Menurut Purnadi Purbacaraka dan Soerjono Soekanto, cara-cara penafsiran yang disusun menurut tingkatannya adalah:

1) Penafsiran Gramatikal,
2) Penafsiran Sistimatikal,
3) Penafsiran Historikal, yang terdiri dari:
   a. Penafsiran dengan melihat perkembangan terjadinya undang-undang, melihat bahan-bahan perundingan/parlementer dan sebagainya (*wetshistorissch*).
   b. Penafsiran dengan melihat perkembangan lembaga hukum yang diatur dalam undang-undang (*rechtshistorisch*).
4) Penafsiran Teleologikal,
5) Penafsiran Ekstensif dan Restriktif.

[108] Jan Remmelink, *Hukum pidana, Komentar atas Pasal-Pasal terpenting dari Kitab Undang-undang Hukum Pidana Belanda dan Padanannya dalam Kitab Undang-undang Hukum Pidana Indonesia*, diterjemahkan oleh Tristam Pascal Moeliono dan Marjanne Termorshuizen, cet.I, Jakarta:Gramedia Pustaka Utama, 2003, hal. 56.

penentuan perilaku yang dirumuskan sebagai tindak pidana seharusnya diawali dengan pertanyaan: apakah suatu perilaku selayaknya diserahkan kepada *private etchics* ataukah ia telah menjadi bagian dari ranah (*domain*) publik?[109].

Sebuah perbuatan yang termasuk dalam ranah publik apabila perbuatan tersebut telah bersinggungan dengan kepentingan publik. Pada kejahatan komputer terdapat beberapa kepentingan yang harus dilindungi, yaitu kepentingan masyarakat untuk mendapatkan perlindungan baik terhadap *property* maupun *privacy*. Namun terhadap aparat penegak hukum khususnya penyidik juga harus diberikan akses untuk menemukan alat bukti yang diperlukan untuk melakukan proses penyidikan sebuah kasus tindak pidana.

Terhadap kejahatan seperti pada kasus pembelian barang yang menggunakan data kartu kredit milik orang lain menyangkut masalah hak milik (property) seseorang. Pada peristiwa ini perbuatan pelaku dapat dikatakan telah bersinggungan dengan kepentingan orang lain.Motif dari perbuatan pelaku dalam kasus tersebut adalah ingin memiliki barang milik orang lain secara melawan hukum. Namun dalam kasus yang terjadi di Jawa Barat tersebut di atas dimana pelaku membeli barang lewat sebuah situs dengan menggunakan nomor kartu kredit milik orang lain, Penuntut Umum tidak dapat membuktikan pasal 362 yang merupakan esensi dari peristiwa ini yaitu mengambil barang milik orang lain secara melawan hukum.

Pada kasus yang terjadi di Jawa Barat mengenai kejahatan terhadap property tersebut di atas Penuntut Umum dan Hakim hanya dapat menentukan pelaku bersalah menggunakan surat atau identitas palsu (pasal 263 ayat (2) KUHP) dimana perbuatan itu pada saat pelaku mengambil kiriman barang dengan menggunkan KTP palsu. Sedangkan dalam kasus yang terjadi di Jogjakarta, Hakim tidak sependapat dengan Penuntut Umum yang menuntut terdakwa dengan

---

[109] Harkristuti Harkrisnowo, *Rekonstruksi Konsep Pemidanaan: Suatu Gugatan terhadap Proses Legislasi dan Pemidanaan Indonesia*, Orasi Pada Upacara Pengukuhan Guru Besar Tetap dalam Ilmu Hukum Pidana FH UI, Depok, 8 Maret 2003, hal 20

pasal 362 KUHP pada dakwaan pertama namun Hakim sependapat dengan Penuntut Umum sesuai dengan dakwaan kedua yaitu melanggar pasal 378 KUHP.

Pada kasus-kasus mengenai kejahatan memasuki/ merusak komputer/jaringan komputer, Penuntut Umum pada kasus *cracking website* KPU hanya menggunakan undang-undang telekomunikasi sedangkan pada kasus *cracking website* Partai Golkar selain menggunakan undang-undang telekomunikasi, Penuntut Umum juga menggunakan pasal 406 KUHP walaupun pada akhirnya tidak dapat dibuktikan di pengadilan. Pada peristiwa-peristiwa tersebut belum dapat diketahui secara pasti apa motif para pelaku melakukan perbuatan tersebut. Seorang hacker adalah sebuah label bagi seseorang yang mahir menerobos jaringan milik pihak lain secara tidak sah. Para hacker saat ini telah mempunyai komunitas tersendiri dan bahkan mempunyai perspektif tersendiri terhadap perilakunya.

Menurut perspektif para hacker yang biasa disebut "underground" pada dunia maya yang tercermin pada banyak *blog* yang dijumpai di internet mereka mengklaim bahwa mereka tidaklah jahat. Perbuatan mereka justru berguna bagi pengguna jasa internet yaitu memberitahu kelemahan-kelemahan yang ada pada jaringan milik pengguna. Namun terdapat juga hacker yang menurut mereka jahat yaitu yang memanfaatkan ketrampilannya untuk mendapatkan keuntungan secara melawan hukum. Sehingga dalam kasus-kasus tersebut diatas beberapa kasus tidak menyentuh motif dari pelaku dan hanya menjelaskan perbuatan pelaku yang didakwa dengan delik formil. Pada blog atau website yang dijumpai di dunia maya yang merupakan komunitas para hacker mereka mempunyai manifesto yang biasa disebut *"Hacker's Manifesto"*. Manifesto tersebut berupa sebuah esai yang ditulis pada tanngal 8 Januari 1986 oleh seseorang yang mempunyai nama "The Mentor" di dunia *underground*. Tulisan

tersebut dibutan setelah ia tertangkap polisi karena kejahatan komputer[110]:

The following was written shortly after my arrest...

The Conscience of a Hacker

by

+++The Mentor+++

Written on January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...

Or feels threatened by me...

Or thinks I'm a smart ass...

Or doesn't like teaching and shouldn't be here...

---

[110] http://www.mithral.com/~beberg/manifesto.html diakses pada tanggal 6 Mei 2008.

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals.
We explore... and you call us criminals.
We seek after knowledge... and you call us criminals.
We exist without skin color, without nationality, without
religious bias... and you call us criminals.
You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

Dari pesan yang disampaikan kepada komunitas hacker tersebut dapat disimpulkan bahwa mereka telah mempunyai sebuah komunitas tersendiri dan bahkan seolah-olah mempunyai sebuah budaya

tersendiri di dalam dunia maya. Budaya tersebut terbentuk karena mereka merasa tidak puas dengan budaya pada main stream yaitu pada dunia dimana mereka hidup dan bersosialisasi. Pada peristiwa ini dapat dikatakan bahwa telah terbentuk sub budaya (*subculture*) yang terpecah dari *mainstream* yaitu budaya pada umumnya dan budaya pada dunia maya. Subculture dapat terjadi karena beberapa orang pada kultur yang dominan mempunyai norma-norma tersendiri,

A subculture is a subdivision within the dominant culture that has it own norms, belief, and values. Subculture typically emerge when people in similar circumstances find themselves isolated from the mainstream and band together for mutual support.

(terjemahan bebas penulis: Subkultur adalah sebuah subdivisi (bagian) dalam budaya yang dominan yang mempunyai norma-norma, keyakinan-keyakinan dan nilai-nilai tersendiri. Subkultur biasanya timbul karena orang-orang dalam keadaan yang sama mendapati diri mereka terpisah dari arus utama masyarakat dan mengikatkan diri bersama untuk saling mendukung)[111].

Komunitas para hacker ini membentuk kelompok tersendiri yang mempunyai pandangan bahwa di dunia maya terdapat nilai-nilai atau *conduct norms* yang berbeda dengan masyarakat pada umumnya. Sehingga terjadi persinggungan kepentingan-kepentingan antara kepentingan masyarakat akan privacy dan property dengan perbuatan para hacker tersebut.

Namun terhadap kejahatan yang ditujukan kepada property dan privacy motif pelaku berbeda dengan perbuatan yang hanya memasuki jaringan komputer orang lain (hacker). Khusus perbuatan memasuki jaringan komputer milik orang lain tersebut, apabila pemilik jaringan komputer merasa bahwa dengan diketahuinya kelemahan-kelamahan yang ada pada jaringannya itu menguntungkan dirinya, maka pemilik jaringan komputer tersebut tidak akan melaporkan peristiwa tersebut.

[111] Bahan kuliah kriminologi yang dikumpulkan oleh Prof. Harkristuti Harkrisnowo, SH, MA, Ph.D pada bagian Subculture Theories.

Pembahasan kasus-kasus tersebut diatas, menyimpulkan bahwa motif (maksud) dari pelaku penyimpangan dapat dikategorikan menjadi dua bagian:

- Pelaku yang mempunyai motif hanya untuk membuktikan bahwa ia dapat membobol sebuah situs karena ketrampilannya yang lebih dari yang lain dan agar mendapat pengakuan dari komunitasnya atau yang lain.
- Pelaku yang mempunyai motif selain tersebut di atas, yaitu juga untuk mencari keuntungan secara materi, seperti pada kasus-kasus pembelian barang dengan menggunakan kartu kredit milik orang lain lewat *online shopping* serta motif lainnya seperti untuk mempermalukan orang lain.

Kepentingan-kepentingan yang perlu dilindungi dalam hal ini[112]:

1) Melalui dunia maya dapat diakses berbagai macam informasi mengenai seseorang yang sebenarnya merupakan informasi rahasia, termasuk pemerintah (privacy). Pada era teknologi informasi, penggunaan komputer akan menyentuh seluruh aspek kehidupan. Sehingga identitas seseorang akan tersimpan di berbagai tempat seperti perbankan, pemerintah, dan lain-lain yang terhubung pada jaringan komunikasi. Dengan dapat diaksesnya data-data tersebut maka tidak tertutup kemungkinan akan terjadi penggunaan identitas atau data-lainnya secara melawan hukum. Hal ini dapat dilakukan oleh siapapun juga termasuk pemerintah.
2) Dunia bisnis mempunyai informasi yang perlu dilindungi. Dalam dunia bisnis terdapat informasi yang bernilai, yang perlu dirahasiakan sehingga perlu dilindungi.
3) Pada sisi lain penyidik diberikan akses untuk mengungkap kasus-kasus kriminal. Akses disini dapat diterjemahkan sebagai akses kepada wilayan pribadi masyarakat termasuk di dalamnya jaringan informasi.

Menurut Soerjono Soekanto, dalam penegakan hukum terdapat beberapa aspek yang mempengaruhinya, diantaranya *faktor hukumnya sendiri, yang dibatasi pada undang-undang saja.* Pada kasus-kasus kejahatan komputer seperti yang dibahas di atas, terdapat perbedaan penafsiran oleh penegak hukum pada beberapa kasus yang relatif sama. Sebagai contoh pada kasus pembelian barang

[112] Pendapat Prof. Mardjono Reksodiputro, SH, MA pada saat penulis melakukan bimbingan tesis ini.

dengan menggunakan kartu kredit orang lain, pada sebuah kasus Penuntut Umum dan Hakim sependapat menginterpretasikan perbuatan terdakwa membeli barang dengan menggunakan kartu kredit milik orang lain adalah termasuk pengertian "menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya". Sedangkan dalam kasus yang lainnya yang relatif sama, Penuntut Umum dan Hakim tidak menginterpretasikan perbuatan terdakwa membeli barang dengan menggunakan kartu kredit milik orang lain dengan pengertian yang sama, sehingga yang dapat dibuktikan hanya perbuatan terdakwa menggunakan identitas palsu dalam mengambil barang yang dikirim kepada terdakwa.

Terlihat bahwa pada keadaan tersebut faktor hukumnya (undang-undang) menjadi hambatan dalam proses penegakan hukumnya. Pasal-pasal di dalam undang-undang dimaksudkan untuk mengkriminalisasi perbuatan-perbuatan tertentu yang telah ada sebelumnya, sehingga penegak hukum akan kesulitan dalam melakukan proses peradilan dengan menggunakan pasal-pasal yang bukan dibuat untuk mengkriminalisasi perbuatan tersebut.

3.2. PROSES PENCARIAN FAKTA (*FACTUAL GUILT*) DALAM PENYIDIKAN TERHADAP KEJAHATAN KOMPUTER YANG MERUPAKAN BUKTI AWAL.

3.2.1. Bukti Elektronik dan Penggunaannya.

Dalam kasus-kasus *cyber crime*, disamping bukti keterangan saksi, alat bukti lain yang sangat menentukan adalah bukti elektronik. Menurut **Alan M Gahtan** bukti elektronik (*electronic evidence*) adalah *electronically stored information on any type of computer device that can be used as evidence in a legal action*[113] (informasi yang tersimpan secara elektronik dalam setiap bentuk komputer yang dapat digunakan sebagai buktidalam suatu tindakan hukum.

Sehingga yang dimaksud dengan bukti elektronik adalah bukti yang dibangun dari suatu data elektronik yang digunakan untuk kepentingan pembuktian terhadap tindak pidana yang disangkakan dan didakwakan.

---

[113] Alan M Gahtan, ***Electronic Evidence,*** Carswell:Toronto: 1999, hal 4

Bukti elektronik mempunyai karakteristik khusus yang berbeda dengan bukti konvensional (berbasis kertas). Bukti elektronik tersebut dapat berupa hardware dan software. Data elektronik mudah untuk diubah dan dirusak dan dengan kemampuan teknik yang memadai bahkan perubahan dan perusakan tersebut dapat tertutupi.[114]

Untuk memperoleh bukti permulaan penyidik harus mendapatkan sebuah alat bukti yang didapat dengan beberapa cara. Sesuai dengan Kitab Hukum Acara Pidana bahwa penyidik dapat melakukan penggeledahan dan penyitaan untuk menemukan barang bukti yang dapat menjadi bukti awal untuk menentukan perbuatan yang dilakukan oleh seseorang. Karena karakteristik alat bukti elektronik tersebut maka permasalahannya bagaimana penyidik dapat memastikan dan menemukan bukti tersebut yang biasanya notabene berada pada kekuasaan pelaku.

Selama ini penyidik Polri dalam melakukan penyidikan mempunyai "Pedoman penyitaan&penanganan barang bukti elektronik". Dalam pedoman tersebut barang bukti elektronik yang dapat disita untuk keperluan pembuktian kejahatan komputer adalah:

- Komputer
- Personal Data Asistance (PDA)
- Media penyimpanan data
- Back-up tape (pita back-up)

Menurut AKBP EDDY HARTONO, SIK Penyidik Madya pada Unit V IT & Cybercrime Mabes Polri selama ini memperoleh bukti permulaan terhadap dugaan tindak pidana komputer selain dari keterangan saksi dapat berupa *log file*. Log file tersebut tersimpan di dalam *hard disk* atau media penyimpanan lainnya yang berisi history. Selain log file tersebut beberapa contoh bukti digital hasil rekaman antara lain:

- E-mail dan alamat e-mail.
- Word processor.
- Pesan dari chat room di internet.

[114] Alan M Gahtan., *Op.cit* hal 7

- Source code dari software.
- Voice mail.
- File image digital.
- Web browser, book marks, cookies, dll.

Setelah mendapatkan log file tersebut maka penyidik akan meminta bantuan kepada forensik komputer untuk membaca data-data yang tersimpan dalam history. Dalam kejahatan yang menggunakan sarana komputer pelaku dapat melakukan sendiri dan dari tempat yang jauh dan tersembunyi misalnya di dalam rumah sehingga tidak ada saksi yang melihat kecuali pelaku sendiri, sehingga untuk membuktikan adanya perbuatan tersebut diperlukan alat bukti lain untuk membuktikan perbuatan dan kesalahan pelaku.

Komputer dapat menyimpan berbagai macam data baik data yang dibuat oleh operator maupun operasi yang dilakukan oleh komputer itu sendiri seperti waktu dilakukan input, waktu mengenai terakhir digunakan, program apa yang dipakai selama ini dan informasi lain diluar input dan pengolahan data. Catatan data dan operasi komputer tersebut dapat digunakan dalam membantu pembuktian kejahatan komputer. Bahkan dengan teknik tertentu didalam *forensic audit* data yang telah dihapus dapat dilakukan *recovery* hingga dapat ditampilkan kembali. *L Volonino* memberikan definisi mengenai forensik komputer,

Computer forensics is the science of retrieving and chronicling evidence located on a computer's hard drive so that it can be presented as evidence in a court of law.[115]

Pihak yang melakukan audit forensik merupakan lembaga yang telah terakreditasi sehingga hasil auditnya valid[116]. Dalam praktek peradilan seringkali kemampuan dan independensi lembaga audit

[115] L Volonino, ***Electronic Evidence and Computer Forensic*** , (Communication of AIS, Vol 12, October 2003) hal 7.

[116] Abu Bakar Munir, ***Cyber Law : Policies and Challenges***, (Butterworths Asia: Malaysia: 1999) hal 256

forensik tersebut dipertanyakan, yang dapat mengakibatkan keraguan hakim atas alat bukti yang disampaikan, saat ini di Indonesia belum terdapat aturan tentang akreditasi auditor komputer, namun di Indonesia telah ada Laboratorium Forensik Polri dan Badan Pengkajian dan Pengembangan Teknologi[117]. Saat ini yang melakukan audit forensik komputer adalah laboratorium forensik Polri dan Internal Audit instansi-instansi.

Setelah mendapatkan bukti digital tersebut, penyidik akan menyerahkannya kepada Penuntut Umum sebagai salah satu alat bukti yang digunakan di pengadilan. Pada tindak pidana yang melibatkan teknologi komputer dan informasi, karena dapat dilakukan di mana saja biasanya tidak ditemukan saksi seperti yang diharuskan dalam penjelasan pasal 185 ayat (1) KUHAP yaitu keterangan saksi yang mendengar dan atau melihat sendiri sebuah peristiwa pidana. Keterangan saksi yang diperoleh biasanya hanya keterangan yang diberikan oleh saksi yang diperoleh secara tidak langsung (testimonium de auditu). Sehingga bukti yang berbentuk elektronik memiliki peran yang sangat besar dalam membuktikan kejahatan komputer.

3.2.2. Autentikasi Bukti Elektronik

Penggunaan data komputer sebagai alat bukti seringkali mendapatkan keberatan dari pihak-pihak yang beracara di pengadilan. Keberatan-keberatan yang biasa diajukan tersebut adalah mengenai apakah data komputer tersebut layak dan validitasnya tinggi untuk dapat digunakan sebagai alat bukti.

Menurut Edmon Makarim, keberadaan alat bukti elektronik memang tidak dapat berdiri sendiri sebagai alat bukti (*real evidence*), karena alat bukti elektronik harus didukung oleh adanya alat bukti lain (misalnya didukung keterangan ahli)[118].

Kekhawatiran tentang validitas data komputer tersebut karena data komputer dapat diubah atau dimanipulasi, tetapi hal yang

[117] Hasil wawancara dengan AKBP EDDY HARTONO, SIK di Jakarta pada tanggal 15 April 2008

[118] Edmon Makarim, op cit hal 427.

terpenting dalam menjamin validitas data yang diautentifikasi adalah sistem keamanan yang tinggi. Dengan sistem keamanan yang tinggi komputer tersebut tidak mudah diubah oleh yang tidak berwenang mengakses ke dalam jaringan tersebut. Dengan demikian apapun data yang dibuat oleh komputer jika memiliki keamanan yang tinggi maka data yang didapat sebagai alat bukti mempuyai validitas yang tinggi.

Dengan demikian autentifikasi bukti elektronik sangat penting untuk menjamin validitas bukti elektronik. Untuk keperluan persidangan autentifikasi bukti tersebut haruslah didukung dengan identifikasi dan atau penjelasan dari saksi/terdakwa/ ahli. Selain itu cara penyitaan juga harus dilakukan tidak dengan cara melawan hukum. langkah-langkah yang dilakukan oleh Polri dalam menangani kasus *hacking* atau kasus-kasus perusakan terhadap komputer melalui jaringan,adalah sebagai berikut[119]:

1. Laporan Polisi, yang diikuti dengan pemeriksaan saksi dari pemilik ISP (*Internet Service Provider*) yang telah diketahui bahwa ISP tersebut digunakan oleh si pelaku (*hacker*);
2. Pemeriksaan di Tempat Kejadian Perkara (TKP) dan warnet yang digunakan pelaku, sekaligus untuk mengumpulkan, melacak dan/atau melakukan penyitaan terhadap bukti elektronik (*digital evidence*) yang ada di TKP, seperti *hard disk*;
3. Melakukan pemeriksaan terhadap ahli yang memiliki keahlian dibidang teknologi informasi, baik dari akademisi maupun lembaga-lembaga lainnya;
4. Pemeriksaan terhadap tersangka, setelah didahului dengan upaya paksa penangkapan dan/atau penahanan, berdasarkan bukti permulaan dan/atau alat bukti yang cukup;
5. Pemberkasan dan penerapan pasal-pasal pidana yang dapat disangkakan terhadap tersangka.

Dengan demikian penyidik dalam menentukan seorang tersangka dalam kasus-kasus kejahatan komputer (cyber crime) melalui tahapan-tahapan

[119] Hasil wawancara dengan AKBP EDDY HARTONO, SIK di Jakarta pada tanggal 15 April 2008

setelah menemukan bukti awal bukti tersebut terlebih dahulu dikonfirmasikan kepada ahli. Hal ini disebabkan karena sifat kejahatan komputer yang dapat dikatakan anonim atau hampir tanpa jejak dan adanya karateristik khusus yang mudah dilakukan perubahan-perubahan.

Audit Forensik Komputer termasuk didalamnya teknik-teknik dalam mendapatkan, menganalisa dan menampilkan data-data yang dicurigai di pengadilan merupakan cara yang utama dalam mencari bukti awal serta alat bukti yang digunakan di pengadilan untuk membuktikan perbuatan pelaku. Dalam melakukan Audit Forensik seorang auditor harus bertindak sesuai dengan hukum sehingga dapat diterima di pengadilan. Misalnya atas komputer yang akan dilakukan audit harus melalui prosedur penyitaan yang sah.

Seperti pada kasus yang disebutkan di atas yaitu atas nama tersangka Joko dimana Penuntut Umum memberikan petunjuk kepada Penyidik hampir seluruhnya merupakan cermin bahwa Penuntut Umum masih meragukan alat bukti elektronik yang didapat oleh Penyidik sehingga memerlukan seorang ahli yang independen untuk menjelaskan keabsahan alat bukti tersebut.

Dengan demikian belum terdapat peraturan yang mengatur tentang proses-proses yang harus dilakukan pada penggunaan sebuah bukti elektronik tersebut untuk dapat digunakan sebagai alat bukti di pengadilan.