



**PEMBOBOLAN KARTU KREDIT KAITANNYA DENGAN *CYBERCRIME*
DAN ALTERNATIF PENYELESAIANNYA**

SKRIPSI

**Diajukan guna melengkapi tugas akhir dan memenuhi syarat-syarat
untuk menyelesaikan Program Studi Ilmu Hukum (SI)
dan mencapai gelar Sarjana Hukum**

Asal :	Hadiah	Klasa
	Pembelian	396.08
tanggal :	16 NOV 2006	VAP
Oleh :		P
Disertifikasi :		C

BAGUS NUR JAKFAR ADI SAPUTRO
NIM. 020710101225

**DEPARTEMEN PENDIDIKAN NASIONAL RI
UNIVERSITAS JEMBER
FAKULTAS HUKUM
2006**

**PEMBOBOLAN KARTU KREDIT KAITANNYA DENGAN *CYBERCRIME*
DAN ALTERNATIF PENYELESAIANNYA**



**PEMBOBOLAN KARTU KREDIT KAITANNYA DENGAN *CYBERCRIME*
DAN ALTERNATIF PENYELESAIANNYA**

Oleh :

BAGUS NUR JAKFAR ADI SAPUTRO
NIM. 020710101225

PEMBIMBING :

Dr.J.J. SETYABUDHI, S.H., M.S.
NIP. 130 287 096

PEMBANTU PEMBIMBING

I GEDE WIDHIANA SUARDA, S.H., M.Hum.
NIP. 132 304 778

**DEPARTEMEN PENDIDIKAN NASIONAL RI
UNIVERSITAS JEMBER
FAKULTAS HUKUM
2006**

MOTTO

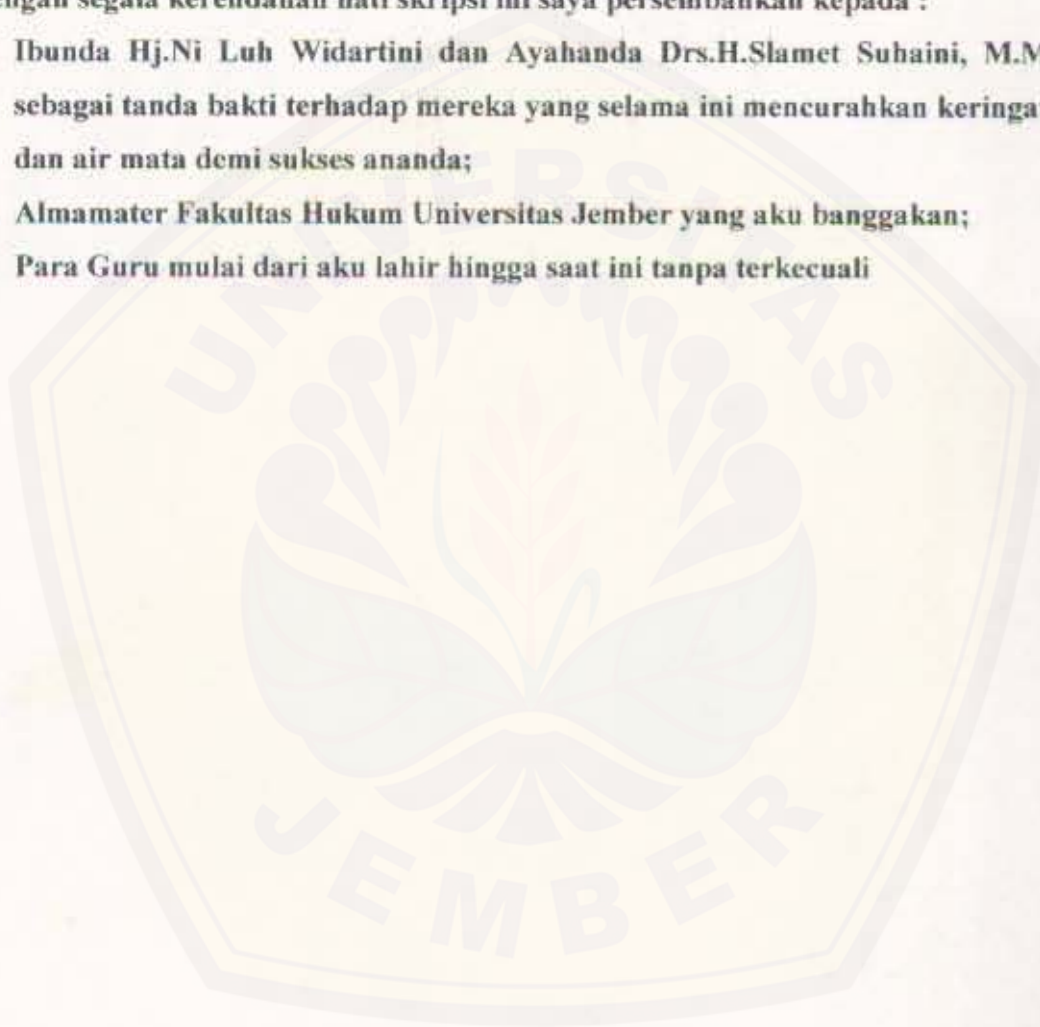
Hai orang-orang yang beriman, ta'atilah Allah dan ta'atilah Rasul (Nya), dan ulil amri di antara kamu. Kemudian jika kamu berlainan pendapat tentang sesuatu, maka kembalikanlah ia kepada Allah (Al Qur'an) dan Rasul (sunnahnya), jika kamu benar-benar beriman kepada Allah dan hari kemudian. Yang demikian itu lebih utama (bagimu) dan lebih baik akibatnya¹.

¹ Al Qur'anul Karim Surah An Nisaa' ayat 59. Ayat tersebut apabila dimaknai dalam konteks hukum positif di Indonesia, dapat diartikan ketika terjadi perbedaan pendapat mengenai sesuatu harus dikembalikan pada hukum (aturan) yang mengaturnya.

PERSEMBAHAN

Dengan segala kerendahan hati skripsi ini saya persembahkan kepada :

1. Ibunda Hj.Ni Luh Widartini dan Ayahanda Drs.H.Slamet Subaini, M.M sebagai tanda bakti terhadap mereka yang selama ini mencurahkan keringat dan air mata demi sukses ananda;
2. Almamater Fakultas Hukum Universitas Jember yang aku banggakan;
3. Para Guru mulai dari aku lahir hingga saat ini tanpa terkecuali



PERSETUJUAN

Dipertahankan di hadapan Panitia Penguji :

Hari : Sabtu
Tanggal : 4
Bulan : November
Tahun : 2006

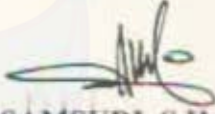
Diterima oleh Panitia Penguji Fakultas Hukum Universitas Jember.

PANITIA PENGUJI :

Ketua,


ECHWAN HRYANTO, S.H., M.H.
NIP. 131 832 334

Sekretaris,


SAMSUDI, S.H., M.H.
NIP. 131 577 298

ANGGOTA PANITIA PENGUJI :

1. **Dr.J.J. SETYABUDHI, S.H..M.S.**
NIP. 130 287 096


(.....)

2. **I GEDE WIDHIANA SUARDA, S.H., M.Hum.**
NIP. 132 304 778


(.....)

PENGESAHAN

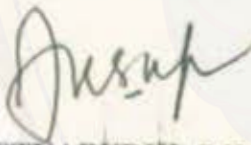
Disahkan skripsi dengan judul :

**PEMBOBOLAN KARTU KREDIT KAITANNYA DENGAN *CYBERCRIME*
DAN ALTERNATIF PENYELESAIANNYA**

Oleh :

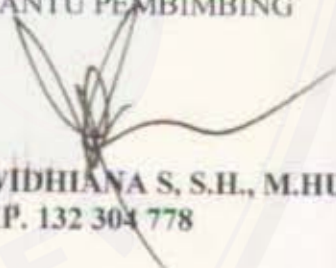
BAGUS NUR JAKFAR ADI SAPUTRO
NIM. 020710101225

PEMBIMBING



Dr.J.J. SETYABUDHI, S.H., M.S.
NIP. 130 287 096

PEMBANTU PEMBIMBING



I GEDE WIDHIANA S, S.H., M.HUM.
NIP. 132 304 778

Mengesahkan :

**DEPARTEMEN PENDIDIKAN NASIONAL RI
UNIVERSITAS JEMBER
FAKULTAS HUKUM**

Dekan,



KOPONG PARON PIUS, S.H., S.U.
NIP. 130 808 985

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Syukur Alhamdulillah penulis haturkan ke hadirat Allah Swt atas limpahan rahmat dan hidayah-Nya serta ridlo-Nya penulis dapat menyelesaikan skripsi dengan judul **"pembobolan kartu kredit kaitannya dengan *cybercrime* Dan alternatif penyelesaiannya "**. *Shalatan wa salaman* senantiasa tercurahkan kepada *rahmatan lil'alamin* Nabi Muhammad Saw karena berkat syafaatnya skripsi ini bisa terselesaikan.

Skripsi ini disusun dan ditulis sebagai salah satu syarat akademis guna mencapai gelar Sarjana Hukum pada Fakultas Hukum Universitas Jember. Pada kesempatan ini, penulis dengan segala kerendahan hati dan rasa hormat menyampaikan terimakasih dan penghargaan kepada para pihak yang telah membantu penulis dalam menyelesaikan penulisan skripsi, antara lain:

1. Bapak Dr.J.J. Setyabudhi, S.H., M.S. dan bapak I Gede Widhiana Suarda, S.H., M.Hum., selaku dosen pembimbing dan pembantu pembimbing skripsi yang telah banyak memberikan masukan dan pengarahan;
2. Bapak Echwan Iriyanto, S.H., M.H. dan bapak Samsudi, S.H., M.H., selaku ketua panitia dan sekretaris penguji skripsi ini;
3. Bapak Kopong Paron Pius, S.H., S.U., selaku Dekan Fakultas Hukum Universitas Jember;
4. Bapak Totok Sudaryanto, S.H., M.S., selaku Pembantu Dekan I dan juga sebagai Dosen Pembimbing Akademik (DPA) penulis, bapak I Ketut Suandra, S.H., selaku Pembantu Dekan II Fakultas Hukum Universitas Jember dan bapak Ida Bagus Oka Ana, S.H., M.M., selaku Pembantu Dekan III Fakultas Hukum Universitas Jember;
5. Bapak Echwan iriyanto. S.H., M.H., selaku Ketua Jurusan Hukum Pidana Fakultas Hukum Universitas Jember;

6. Almarhum Kakek tercinta yang telah sepenuh hati menjaga, merawat dan membesarkan (semoga tenang di alam kubur dan diterima disisi Allah Amin)
7. Keluarga besar di Banyuwangi, nenek, pamanku Agus Suhairi S.H dan mbak Irma, Lek Didi dan Bu Iin, keponaanku Reza, Vita, Didit dan Dinda dan juga adikku Vira semoga jadi anak yang shaleh dan shalehah serta seluruh keluarga besarku yang tidak dapat disebutkan satu persatu atas doa dan dukungannya selama ini;
8. Para Guru yang dengan tulus ikhlas menuntun pada kebenaran;
9. Bapak dan Ibu Dosen serta seluruh staf Fakultas Hukum Universitas Jember yang telah memberikan bantuan selama mengikuti pendidikan di Fakultas Hukum Universitas Jember;
10. Klub Karimata 111, Sever, Vicky, Jojon dan Pak Nugie, Jack, Bung Roma, Ricko, Arya atas persaudaraannya selama ini;
11. Sahabat Suhai, Windy, Yunus, Munib, Esti, Ichang, Salim, Daniel, Ady, Puput, Letda Inf Didik, Sugiharto, Bondan, Riyadi, Novan dan Nila, Prasetyo, Ajang, Kris dan sahabat-sahabat yang lain atas keakraban dan persaudaraan selama ini;
12. Keluarga Mbak Ana di Jember, terimakasih dukungannya selama ini dan;
13. Semua pihak yang telah memberi kontribusi kepada penulis baik secara moril maupun materiil.

Penulis sadar bahwa penulisan skripsi ini masih jauh dari kesempurnaan karena penulis hanyalah manusia biasa yang tidak lepas dari kesalahan. Harapan penulis semoga tulisan ini mampu memberikan manfaat bagi para pembaca.

Jember, November 2006

Penulis

DAFTAR ISI

	Halaman
HALAMAN COVER	i
HALAMAN JUDUL	ii
HALAMAN PEMBIMBING.....	iii
HALAMAN MOTTO	iv
HALAMAN PERSEMBAHAN	v
HALAMAN PERSETUJUAN.....	vi
HALAMAN PENGESAHAN	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR LAMPIRAN	xii
RINGKASAN	xiii
BAB I. PENDAHULUAN	
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian.....	4
1.4 Metode Penelitian	5
1.4.1 Pendekatan Masalah.....	5
1.4.2 Sumber Penelitian Hukum.	6
1.4.3 Metode Pengumpulan Bahan Hukum.	7
1.4.4 Analisis Bahan Hukum.	7
BAB II. FAKTA, DASAR HUKUM, DAN TINJAUAN PUSTAKA	
2.1 Fakta	9
2.2 Dasar Hukum	11

2.3	Tinjauan Pustaka	16
2.3.1	Pengertian Dan Jenis <i>cybercrime</i>	16
2.3.2	Yurisdiksi Hukum Pidana Di Dalam <i>Cybercrime</i>	18
2.3.3	Pembobolan Kartu Kredit Sebagai Salah Satu Bentuk <i>Cybercrime</i>	20

BAB III. PEMBAHASAN

3.1	Upaya Penanggulangan Kejahatan <i>Cybercrime</i> Dengan Hukum Pidana Sebelum Ada Aturan Yang Mengatur Secara Khusus	23
3.2	Alternatif penyelesaian Perkara Pembobolan Kartu Kredit Sebelum Diundangkannya Undang-Undang yang Mengatur	35

BAB IV KESIMPULAN DAN SARAN

4.1	Kesimpulan	44
4.2	Saran	45

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR LAMPIRAN

1. Undang-Undang No 36 Tahun 1999 Tentang TELEKOMUNIKASI



RINGKASAN

Terdapat beberapa kasus yang berkaitan dengan *cybercrime* yang marak akhir-akhir ini. Permasalahan dalam skripsi ini pertama, seiring berkembangnya kemajuan teknologi hal ini menimbulkan berbagai macam permasalahan baru di dalam perkembangan ilmu hukum yang menuntut adanya pembaharuan hukum karena ketiadaan peraturan yang mengatur tentang *cybercrime*, maka ada beberapa solusi yang ditawarkan sebagai jalan untuk menegakkan keadilan dan juga agar tidak terjadi kekosongan hukum.

Pendekatan masalah yang digunakan dalam skripsi ini adalah pendekatan yuridis normatif, sumber bahan hukum adalah bahan hukum primer dan bahan hukum sekunder, metode pengumpulan bahan hukum adalah studi kepustakaan dan analisis bahan hukum yang digunakan adalah analisis preskriptif normatif.

Fakta, dasar hukum dan tinjauan pustaka merupakan acuan bagi penulis dalam melakukan pembahasan. Dalam tinjauan pustaka penulis mengutip beberapa pendapat para sarjana hukum mengenai hal-hal yang berkaitan dengan *cybercrime*, baik itu berupa pernyataan di dalam persidangan, hasil diskusi dan seminar maupun kutipan dari beberapa hasil kongres PBB.

Perkembangan teknologi yang semakin pesat membawa manusia pada era baru di dalam pemenuhan kebutuhan akan informasi dan teknologi yaitu dengan hadirnya internet, internet di anggap sebagai dunia baru yang menawarkan segala kemudahan di dalamnya, tetapi tanpa disadari banyak kejahatan baru yang berkembang di dalamnya, kejahatan yang benar-benar merasahkan dengan berbagai bentuk dan fungsinya yang kesemuanya dilakukan dengan media komputer tanpa memperlihatkan sosok nyata dari pelakunya, hal ini memaksa para aparat untuk menemukan aturan baru sedangkan KUHP yang ada dinilai belum memenuhi tuntutan untuk menjerat pidana pelakunya.

Salah Satu bentuk dari *cybercrime* tersebut adalah Pembobolan Kartu Kredit, para aparat dihadapkan pada ketiadaan peraturan untuk menjerat pelaku tindak pidana

ini oleh karenanya beberapa diantaranya tidak dijerat pidana hanya dikenakan sanksi untuk mengembalikan barang yang telah dicurinya, hal ini menimbulkan beberapa kontroversi diantara beberapa kalangan praktisi hukum, untuk itulah diperlukan adanya suatu kejelasan untuk menggunakan KUHP dan Undang-Undang Nomor 36 Tahun 1999 Tentang telekomunikasi sebagai alternatif di dalam menjerat para pelaku kejahatan ini

Kesimpulannya, beberapa permasalahan tentang *cybercrime* sebenarnya masih dapat di selesaikan dengan alternatif penyelesaian yaitu dengan menggunakan KUHP dan Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi dengan disertai penafsiran dari hakim didalam memutus perkara

Fakultas Hukum, Universitas Jember.

BAB I PENDAHULUAN



1.1 Latar Belakang

Teknologi semakin menyediakan banyak kemudahan bagi penggunanya, selain membawa dampak positif juga mengundang berbagai bentuk tangan-tangan kriminal untuk beraksi, baik untuk mencari keuntungan materi ataupun sekedar iseng. Hal ini memunculkan fenomena khas yang sering disebut *Computercrime* atau *Cybercrime* atau kejahatan di dunia komputer¹.

Kejahatan *cyber* dalam perkembangannya mulai memprihatinkan banyak pihak yang merasa telah dirugikan hal ini juga dikarenakan arus globalisasi ini adalah suatu bentuk dari pada pemenuhan informasi yang merupakan inti dari globalisasi yaituperubahan yang cepat dan mendasar.

Kejahatan *Cybercrime* tersebut dapat disebut sebagai *cost* atau harga mahal dari suatu perubahan masyarakat global yang tingkat perkembangannya melebihi eksistensi hukum. Hal ini merupakan cermin dari suatu kondisi masyarakat yang selalu berkejaran antara keinginan dengan tarikan pengaruh global yang tidak sedikit memproduksi dan menawarkan perubahan bercorak sampah (merugikan).²

Dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan yang bersifat tidak berwujud, misalnya dalam kasus pencurian listrik yang pada awalnya sulit dikategorikan sebagai delik pencurian tetapi akhirnya dapat diterima sebagai tindak pidana.

¹ Teguh Wahyono, 2006. *Etika Komputer Dan Tanggung Jawab Profesional Di bidang Teknologi Informasi*. Yogyakarta: Andi. h. 30.

² Achmad Sodiki, 2005. dalam sebuah pengantar tentang kejahatan mayantara. Wahid & Mohammad Labib. *Kejahatan Mayantara*. Bandung: Reflika Aditama. h. vii

Kenyataan saat ini yang berkaitan dengan kegiatan *Cyber* tidak lagi sesederhana itu, mengingat kegiatannya tidak lagi bisa dibatasi oleh teritori suatu negara, aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun.

Kegiatan *cyber* meskipun bersifat *virtual* dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam ruang *cyber* sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi hukum konvensional untuk dapat dijadikan objek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan *cyber* adalah kegiatan *virtual* yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.³

Kejahatan komputer dapat diartikan sebagai kejahatan yang ditimbulkan karena penggunaan komputer secara *illegal*. Selanjutnya, seiring dengan perkembangan pesat teknologi komputer, kejahatan di bidang ini pun meningkat. Berbagai jenis kejahatan komputer yang terjadi mulai dari kategori ringan seperti *penyebaran virus, spam email, penyadapan transmisi* sampai pada kejahatan-kejahatan kategori berat seperti misalnya *Carding* (Pencurian Melalui Internet)⁴

Carding adalah sebuah ungkapan mengenai aktivitas berbelanja secara maya (lewat komputer), dengan menggunakan berbagai macam alat pembayaran yang tidak sah. Dalam kasus *carding* tercatat mendominasi kejahatan sejak 1999 hingga akhir Agustus 2004 dimana selama periode Januari–Agustus tahun ini, kerugian akibat *carding* dilaporkan telah mencapai US\$4.543.176,5.

Carding adalah suatu penipuan dengan berbasis pada perdagangan elektronik yang ditandai dengan pembayaran melalui kartu kredit. Didalam *carding*, penjahat memakai data kartu kredit asli milik orang lain atau memakai data kartu kredit palsu

³ Ahmad M. Ramli. 2004. *Prinsip-Prinsip Cyberlaw Dan Kendala Hukum Positif Dalam Menanggulangi Cybercrime*. Modul I e-Learning, Fakultas Hukum Universitas Padjadjaran

⁴ FN Jovan. 2006. *Pembobolan Kartu Kredit. "Menyingkap tehnik & cara kerja para carder internet*. Tangerang: Mediakita h.1

dan para pelaku dari *carding* ini disebut *carder*, dalam menjalankan aksinya *carder* mengenal dua modus kejahatan. Pertama, *carder* bertindak sebagai pembeli gadungan (*fraud buyer*). Sebagai pembeli, para *carder* memakai data kartu kredit milik orang lain untuk membeli barang dari toko *online* yang menerima pembayaran dengan kartu kredit. Modus kedua, *carder* bertindak sebagai penjual gadungan (*fraud seller*) dalam hal ini ia menipu konsumen dengan mendapatkan uang pembayaran atau data kartu kredit konsumen tanpa harus mengirim barang yang sudah dipesan oleh konsumen. Kalaupun penjual gadungan ini mengirimkan barang yang dipesan oleh pembeli, maka barang itu sebetulnya dibeli dari pihak lain dengan menggunakan kartu kredit orang lain⁵

Ketiadaan peraturan yang mengatur tentang *cybercrime* menyebabkan dengan mudahnya para pelaku dari pembobolan kartu kredit ini bebas memainkan perannya di dalam dunia maya. Banyaknya kejahatan *carding* karena banyak masyarakat senang mengakses website yang tidak bertanggungjawab. Di samping itu, banyak pula website yang menyediakan nomor-nomor kartu kredit banyaknya kejahatan *carding* karena pelaku menganggap kejahatan tersebut tidak akan dihukum dengan berat. Pelaku juga telah terpengaruh gaya hidup sehingga ingin mempunyai berbagai fasilitas meski tidak mempunyai cukup uang banyak pelaku kejahatan *carding* tidak tertangani dengan baik. Hanya satu dua orang pelaku saja yang bisa ditangkap oleh kepolisian.

Untuk mencegah menjadi korban kejahatan *carding*, berharap masyarakat tidak memberikan nomor kartu kredit pada orang dan tidak masuk ke website yang tidak dikenal keberadaannya serta tidak memberikan nomor 3 digit terakhir pada pihak lain.

Persamaan persepsi dari aparat penegak hukum tentang perlunya penanganan yang serius terhadap para pelaku penyalahgunaan kartu kredit karena hal itu akan

⁵ FN Jovan, *Op.cit*, hlm. 2.

berdampak kepada citra Indonesia di mata dunia internasional dan kenyamanan para pengguna kartu kredit.

Celah kecil ini nampaknya dimanfaatkan oleh sekelompok orang tertentu dengan mencari keuntungan baik secara pribadi ataupun korporasi, baik itu berupa *carding* (pembobolan kartu kredit). Dalam hal ini banyak tujuan yang dijadikan alasan bagi masing-masing perseorangan tersebut,

Dari uraian latar belakang di atas, saya tertarik untuk mengetahui lebih jauh hal-hal yang terkait dengan berbagai perkembangan dunia *Cyber* khususnya dalam hal pembobolan kartu kredit. Selanjutnya akan dicoba mengkaji dan membahas persoalan tersebut dalam skripsi ini dengan judul : **“PEMBOBOLAN KARTU KREDIT KAITANNYA DENGAN *CYBERCRIME* DAN ALTERNATIF PENYELESAIANNYA”**.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, permasalahan pokok dalam penulisan skripsi ini adalah sebagai berikut:

- 1). Upaya Penanggulangan *Cybercrime* Dengan Hukum Pidana Sebelum Ada Aturan Yang Mengatur Secara Khusus?;
- 2). Bagaimana Alternatif Penyelesaian kasus pembobolan kartu kredit sebelum diundangkannya aturan yang mengatur secara khusus?;

1.3 Tujuan Penelitian

Setiap penulisan suatu karya ilmiah, termasuk skripsi pasti ada tujuan yang hendak dicapai. Pada penulisan skripsi ini tujuan yang ingin dicapai, adalah sebagai berikut:

- 1). Upaya penanggulangan kejahatan *Cybercrime* sebelum ada aturan yang mengaturnya secara khusus?

- 2). Untuk mendapatkan solusi terbaik bagi kasus pembobolan kartu kredit sebelum diundangkannya aturan yang mengatur secara khusus?

1.4 Metode Penelitian

Pendekatan masalah yang digunakan dalam skripsi ini adalah pendekatan yang bersifat yuridis normatif. Pendekatan yuridis normatif adalah suatu pendekatan masalah dengan menelaah peraturan perundang-undangan, pendapat para sarjana hukum dan teori hukum yang berhubungan dengan permasalahan⁶.

Guna mencapai tujuan dalam penulisan skripsi ini, maka diperlukan suatu cara atau metode agar memudahkan dalam proses pengumpulan bahan hukum, menganalisis permasalahan dan perumusan kesimpulan atau memeriksa suatu kebenaran pernyataan. Metode dalam suatu karya ilmiah merupakan aspek epistemologis yang penting dan harus dikemukakan secara rinci dan jelas.

1.4.1 Pendekatan Masalah

Pendekatan masalah yang digunakan dalam skripsi ini adalah pendekatan dengan menelaah peraturan perundang-undangan, studi kasus, pendapat para sarjana hukum dan teori hukum yang berhubungan dengan permasalahan⁷.

Berbagai peraturan perundang-undangan, pendapat para sarjana hukum dan teori-teori hukum yang penulis anggap relevan dengan permasalahan yang diangkat, akan dijadikan sebagai pisau analisa untuk membedah dan memecahkan permasalahan tersebut.

⁶ Peter Mahmud Marzuki, *Penelitian Hukum*: ". Makalah (Belum Diterbitkan) Pada Lokakarya Technical Assistance dalam Kerangka TPSDP (September-Oktober), Fakultas Hukum Unej, Jember, 2004. h. 7

⁷ *ibid*

1.4.2 Sumber Penelitian Hukum

Suatu karya ilmiah agar memiliki kualitas yang berbobot dan dapat dipertanggungjawabkan secara ilmiah, memerlukan acuan berupa bahan hukum yang benar dan lengkap. Sumber bahan hukum dapat diklasifikasikan menjadi tiga (3) macam, yaitu bahan hukum primer, bahan hukum sekunder, dan bahan hukum tertier [sich]⁸. Dalam skripsi ini bahan hukum yang penulis gunakan adalah bahan hukum primer dan bahan hukum sekunder.

a. Bahan Hukum Primer

Bahan hukum primer adalah bahan-bahan hukum mengikat yang terdiri dari norma atau kaidah dasar yaitu Pembukaan Undang-Undang Dasar 1945 (UUD 1945); peraturan dasar meliputi batang tubuh UUD 1945 dan ketetapan-ketetapan MPR(S); peraturan perundang-undangan; bahan hukum yang tidak dikodifikasikan; yurisprudensi; traktat dan bahan hukum dari zaman penjajahan yang hingga kini masih berlaku⁹.

Bahan hukum primer yang digunakan dalam penulisan skripsi ini adalah batang tubuh UUD 1945 (amandemen), peraturan perundang-undangan yang meliputi U.U. No. 8 tahun 1981 tentang Hukum Acara Pidana (KUHP), Undang-Undang Hukum Pidana (KUHP), Undang-Undang Republik Indonesia No. 36 Tahun 1999 tentang Telekomunikasi

b. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan penjelasan dari bahan hukum primer semisal rancangan undang-undang, hasil penelitian dibidang hukum, karya ilmiah di bidang hukum dan sebagainya¹⁰. Dalam skripsi ini bahan hukum sekunder yang digunakan adalah bahan-bahan yang diperoleh penulis dari penelitian kepustakaan

⁸ Soerjono Soekanto, *Pengantar Penelitian Hukum*, UI Press, Jakarta, 1986. h. 51-52. lihat juga Bambang Sunggono, *Metodologi Penelitian Hukum*: Cetakan Keenam, Rajawali Press, Jakarta, 2003. h. 113-114.

⁹ Bambang Sunggono, *loc. cit.*

¹⁰ *Ibid.*, h. 114.

(*library reseach*), baik dalam bentuk Tulisan-tulisan tentang hukum, buku, majalah, jurnal (hukum), dan media massa dan Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana (RUUKUHP)

1.4.3 Metode Pengumpulan Bahan Hukum

Metode yang penulis gunakan dalam pengumpulan bahan hukum pada skripsi ini adalah studi kepustakaan. Sunggono¹¹, menyatakan bahwa studi kepustakaan merupakan metode yang digunakan dalam pencarian berbagai landasan teoritis dari permasalahan dalam penelitian sehingga penelitian yang dilakukan tidak bersifat "*trial and error*". Upaya pencarian yang dilakukan adalah dengan membaca berbagai buku/literatur yang terkait dengan permasalahan dan dilakukan pencatatan. Kemudian juga melakukan pengembangan dengan penelusuran informasi melalui internet yang selanjutnya dilakukan pencatatan guna mendapatkan bahan hukum yang diperlukan sebagai dasar penelitian.

1.4.4 Analisis Bahan Hukum

Analisis bahan hukum yang digunakan dalam skripsi ini adalah "preskriptif normatif". Menurut Marzuki¹² yang dimaksud dengan preskriptif normatif adalah:

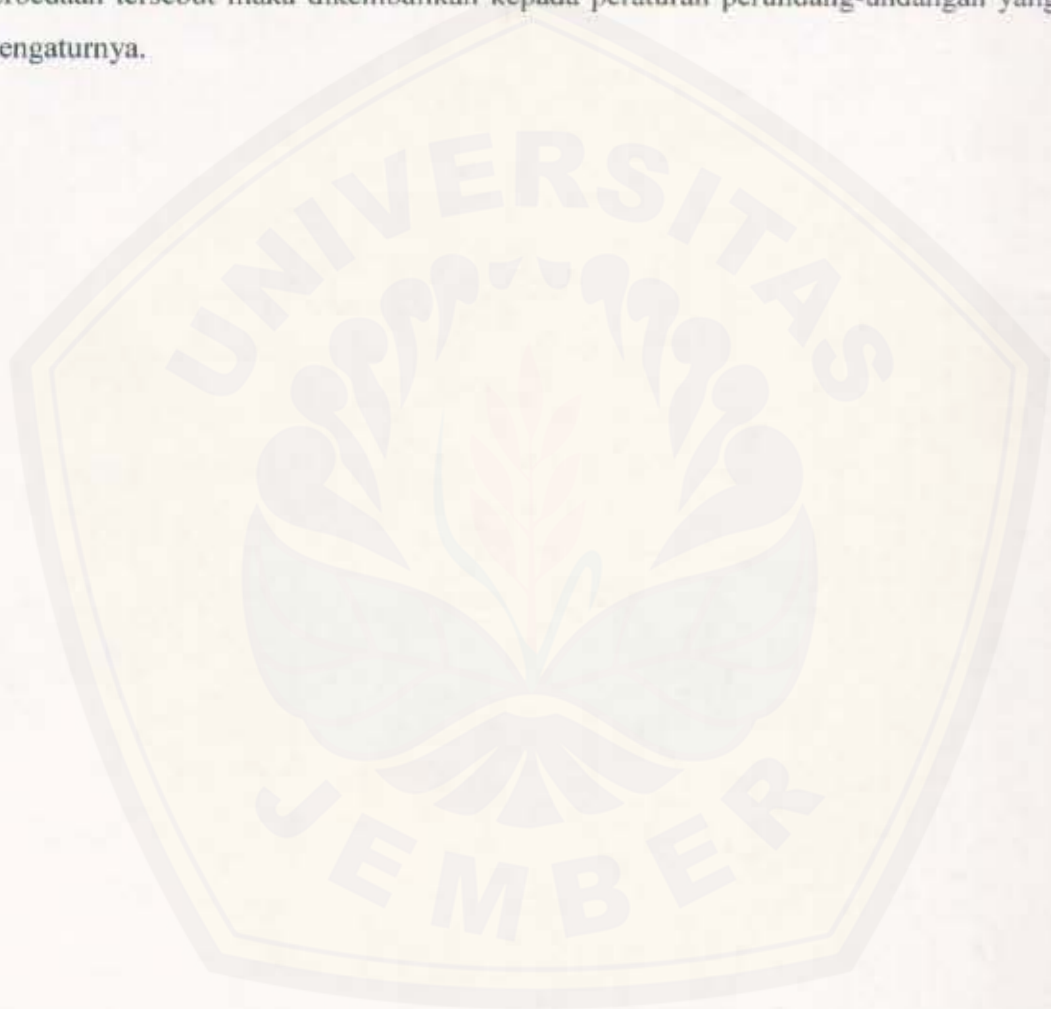
analisis yang dilakukan guna mencari pemecahan atas isu hukum yang timbul mengenai fakta dan gejala yang ditimbulkan dalam hubungannya antara ketentuan peraturan perundang-undangan yang berlaku dan selanjutnya dianalisis dengan memberikan preskripsi (petunjuk) mengenai apa yang seyogyanya atas isu hukum yang diajukan.

Analisis dalam skripsi ini didasarkan atas suatu isu hukum mengenai fakta bahwa telah terjadi perdebatan di kalangan akademisi dan praktisi hukum mengenai penegakkan hukum terhadap kejahatan *Cybercrime* khususnya dalam kasus pembobolan kartu kredit dan pengaturan *Cybercrime* dalam hukum positif, kemudian

¹¹ *Ibid.*, h. 112-113.

¹² P. M. Marzuki, "Penelitian Hukum". Makalah (Belum Diterbitkan) Pada Lokakarya Technical Assistance dalam Kerangka TPSDP (September-Oktober), Fakultas Hukum Unej, Jember, 2004, h.1.

memberikan preskripsi mengenai hal yang harus dilakukan dalam menyikapi isu hukum yang timbul tersebut, yaitu bahwa perbedaan tersebut harus tetap dilihat dalam kerangka normatif, artinya ketika tidak lagi ada titik temu antara berbagai perbedaan tersebut maka dikembalikan kepada peraturan perundang-undangan yang mengaturnya.



BAB II

FAKTA, DASAR HUKUM DAN TINJAUAN PUSTAKA



2.1 Fakta

Dua orang lagi tertangkap sebagai pembobol kartu kredit di Semarang, menyusul satu orang seprofesinya yang tertangkap beberapa bulan berselang, ironisnya *Cyberlaw* malah kesandung batu Kitab Undang-Undang Hukum Pidana (KUHP). Status mereka juga tidak beda yakni sama-sama mahasiswanya. Modus yang mereka lakukan juga sama yakni belanja produk komputer canggih dengan menggunakan kartu kredit milik orang lain (asing).¹³

Di Bandung, kasus *cybercrime* berhasil diungkap kepolisian daerah (Polda) Jawa Barat dalam sebuah operasi pekan lalu. Tujuh pelaku *carding*, pembobolan kartu kredit melalui *Internet*, berhasil diringkus polisi beserta penadahnya.

Para pelaku yang sebagian besar oknum mahasiswa universitas swasta di Bandung, kini ditahan di Markas Polda Jawa Barat beserta sejumlah barang bukti. Para pelaku mengaku, perbuatan itu awalnya hanya iseng belaka.

Wakil Direktur Reserse Kriminal Polda Jabar AKBP Dede Suryana didampingi Kepala Dinas Penerangan Komisaris Besar Muryan Faisal mengatakan, polisi tidak menemui hambatan berarti saat menangkap para tersangka. Aparat membutuhkan waktu sebulan untuk mengendus jejak kejahatan mereka. Informasi awal mereka terima dari Interpol di Jakarta, lalu dikembangkan di lapangan. kenyataannya, para pelaku tersebut telah melakukan puluhan kali transaksi. Hal ini diakui bukan iseng. Motifnya adalah pencurian, penipuan, ataupun penggelapan barang orang..

¹³ Komputekonline.com *pembobol kartu kredit sulit disidang*. [serial online]. [12 april 2004]. <http://www.komputekonline.com/harian/0509/14/nas20.htm> , diakses 24 agustus 2006.

Di antara pelaku terdapat seorang pelajar dan tiga mahasiswa. Mereka adalah Jackson Ronald Simanjuntak (21), Omar Syarif (28), Novtan Ladali (22), Hari Parlindungan (24) Hardi Yunus (19), Eri Vontinus Depari (23), dan Supriyanto (30).¹⁴

Kenyataan yang ada di lapangan bahwa para pelaku diatas mendapatkan banyak kemudahan sehingga mereka dapat dengan mudah lolos dari jeratan hukum tanpa penyidikan yang lebih lanjut mereka yang semula menjadi tersangka dapat dengan mudah bebas atau di bebaskan dari segala tuntutan dengan alasan karena masih belum ada undang-undang yang mengatur lebih lanjut tentang kasus serupa

Cybercrime memang sulit untuk dinyatakan atau dikategorikan sebagai tindak pidana karena terbentur oleh asas legalitas, asas ini cenderung sangat membatasi penegak hukum di Indonesia untuk melakukan penyelidikan dan atau penyidikan guna mengungkap perbuatan, tersebut karena suatu aturan undang-undang yang mengatur *cybercrime* belum tersedia, apalagi asas legalitas ini tidak memperbolehkan adanya suatu analogi untuk menentukan perbuatan pidana. Meskipun penerapan asas legalitas ini tidak boleh disimpangi, tetapi pada prakteknya asas ini tidak diterapkan secara tegas atau tidak diperkenankan untuk terdapat pengecualian¹⁵. Dalam era demokratisasi, perumusan peraturan hukum harus mempertimbangkan secara komprehensif beragam dimensi persoalan.

¹⁴ Polda jabar, *kejahatan teknologi tumbuh subur di indonesia*. [serial online]. [19 juli 2003]. <http://www.kompas.com/harian/14/nas13.htm> , diakses 24 agustus 2006.

¹⁵ Dikdik M. Aries Mansur Elisatris Gultom. 2005. *CYBER LAW* . "aspek hukum teknologi informasi". Bandung: rafika ADITAMA. hal 93-94

2.2 Dasar Hukum

Dasar hukum yang digunakan penulis dalam skripsi ini yaitu.

1. Undang-Undang Dasar 1945 (Amandemen)

a). Pasal 28I ayat (1)

...dan hak untuk tidak dituntut atas dasar hukum yang berlaku surut adalah hak asasi manusia yang tidak dapat dikurangi dalam keadaan apapun.

b). Pasal 28J ayat (2)

Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang

c) Pasal 28f

Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia

2. Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana (KUHAP)

a). Pasal 2

Undang-undang ini berlaku untuk melaksanakan tatacara peradilan dalam lingkungan peradilan umum pada semua tingkat peradilan.

b). Pasal 3

Peradilan dilakukan menurut tata cara yang diatur dalam undang-undang ini.

c). Pasal 41

Dalam hal tertangkap tangan penyidik berwenang menyita paket atau surat atau benda yang pengangkutannya atau pengiriman yang dilakukan oleh kantor pos atau telekomunikasi, jawatan atau perusahaan komunikasi atau pengangkutan, sepanjang paket, surat atau benda tersebut diperuntukkan bagi tersangka atau yang berasal daripadanya dan untuk itu kepada tersangka atau kepada pejabat kantor pos dan telekomunikasi, jawatan atau perusahaan komunikasi atau pengangkutan yang bersangkutan, harus diberikan surat tanda penerimaan.

3. Kitab Undang-Undang Hukum Pidana (KUHP)

a) Pasal 1 ayat (1)

Suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan ketentuan perundang-undangan pidana yang telah ada

b) Pasal 264 ayat (1)

Barangsiapa bersalah karena memalsukan surat dipidana dengan pidana penjara selama-lamanya delapan tahun, kalau perbuatan itu dilakukan terhadap surat kredit atau surat dagang yang disediakan untuk diedarkan

b) Pasal 362

Barangsiapa mengambil barang yang sama sekali atau sebagian kepunyaan orang lain dengan maksud untuk memiliki barang itu dengan melawan hukum, dipidana karena mencuri dengan pidana penjara selama lamanya lima tahun atau denda sebanyak-banyaknya sembilan ribu rupiah

c) Pasal 303 ke 1

Diancam dengan pidana penjara paling lama empat tahun atau pidana denda paling banyak sepuluh juta rupiah:

1. barang siapa menggunakan kesempatan main judi, yang diadakan dengan melanggar ketentuan Pasal 303;
2. barang siapa ikut serta main judi di jalan umum atau di pinggir jalan umum atau di tempat yang dapat dikunjungi umum, kecuali kalau ada izin dari penguasa yang berwenang yang telah memberi izin untuk mengadakan perjudian itu.

d) Pasal 378

Barang siapa dengan maksud untuk menguntungkan 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 kepadanya, atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun.

e) Pasal 480

Dipidana dengan pidana penjara selama-lamanya empat tahun denda sebanyak-banyaknya sembilan ratus rupiah :

Barang siapa mengambil untung dari hasil sesuatu barang, yang diketahuinya atau patut dapat disangkanya bahwa barang-barang tersebut diperoleh karena kejahatan

f) Pasal 282

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.

g) Pasal 112

Barang siapa dengan sengaja mengumumkan surat-surat, berita-berita atau keterangan- keterangan yang diketahuinya bahwa harus dirahasiakan untuk kepentingan negara, atau dengan sengaja memberitahukan atau memberikannya kepada negara asing, diancam dengan pidana penjara paling lama tujuh tahun.

h) Pasal 262

Dalam hal ppidanaan berdasarkan salah.satu kejahatan yang diterangkan dalam pasal 253 - 260 bis, maka hak-hak sebagaimana dimaksud dalam pasal 35 No. 1 – 4 dapat dicabut. Bab XII - Pemalsuan Surat

i) Pasal 406

Barangsiapa dengan sengaja dan dengan melawan hukum , menghancurkan, merusakkan, mebuat sehingga tidak dapat dipakai lagi atau menghilangkan barang yang sama sekali atau sebagian kepunyaan orang lain, dipidana dengan pidana penjara selama-lamanya dua tahun delapan bulan atau denda sebanyak-banyaknya empat ribu lima ratus rupiah

Pasal 372

Barang siapa dengan sengaja dan melawan hukum memiliki barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan 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.

j) Pasal 264 ke 5

Pemalsuan surat diancam dengan pidana penjara paling lama delapan tahun, jika dilakukan terhadap surat kredit atau surat dagang yang diperuntukkan untuk diedarkan.

4. Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi

a) Pasal 40

Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.

b) Pasal 22

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.

c) Pasal 38

Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi.

d) Pasal 40

Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun. dipidana penjara paling lama 15 (lima belas) tahun.

g) Pasal 57

Penyelenggara jasa telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 42 ayat (1), dipidana dengan pidana penjara paling lama 2 (dua) tahun dan atau denda paling banyak Rp 200.000.000,00 (dua ratus juta rupiah).



2.3 Tinjauan Pustaka

2.3.1 Pengertian dan jenis *Cybercrime*

Internet selain memberi manfaat juga menimbulkan eksek negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Hal itu terjadi pula untuk data dan informasi yang dikerjakan secara elektronik. Dalam jaringan komputer seperti *internet*, masalah kriminalitas menjadi semakin kompleks karena ruang lingkungannya yang luas.

Kriminalitas di *internet* atau *cybercrime* pada dasarnya adalah suatu tindak pidana yang berkaitan dengan *cyberspace*, baik yang menyerang fasilitas umum di dalam *cyberspace* ataupun kepemilikan pribadi. Jenis-jenis kejahatan di *internet* terbagi dalam berbagai versi. Salah satu versi menyebutkan bahwa kejahatan ini terbagi dalam dua jenis, yaitu kejahatan dengan motif intelektual. Biasanya jenis yang pertama ini tidak menimbulkan kerugian dan dilakukan untuk kepuasan pribadi. Jenis kedua adalah kejahatan dengan motif politik, ekonomi atau kriminal yang berpotensi menimbulkan kerugian bahkan perang informasi.

Secara garis besar, ada beberapa tipe *cybercrime*¹⁶, yaitu:

- a. *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi komputer.
- b. *Hacking*, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal
- c. *The Trojan Horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi pribadi atau orang lain.
- d. *Data Leakage*, yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa berupa

¹⁶ Philip Renata. "suplemen BisTek". Warta Ekonomi No. 24 edisi Juli 2000. h.52. Lihat juga www.permasalahancybercrime.com., "pendekatan hukum untuk keamanan dunia cyber serta urgensi cyber law bagi indonesia." [Serial Online]. [14 September 2005]. <http://www.duniacyber.com/harian/1/nas33.htm> , diakses 1 september 2006.

rahasia negara, perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu.

- e. *Data Diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah *input* data atau *output* data.
- f. *To frustate data communication* atau penyalahgunaan data komputer.
- g. *Software piracy* yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi Hak Kekayaan Intelektual (HKI).

Dilihat dari beberapa tipe *cybercrime* diatas nampak bahwa inti *cybercrime* adalah penyerangan di *content*, *computer system* dan *communication system* milik orang lain atau umum di dalam *cyberspace*¹⁷

Pola umum yang digunakan untuk menyerang jaringan komputer adalah memperoleh akses terhadap *account user* dan kemudian menggunakan sistem milik korban sebagai *platform* untuk menyerang situs lain.¹⁸

Kasus-kasus *cybercrime* yang banyak terjadi di Indonesia setidaknya ada tiga jenis berdasarkan modusnya, yaitu:¹⁹

1. Pencurian Nomor Kartu Kredit.

Penyalahgunaan kartu kredit milik orang lain di *internet* merupakan kasus *cybercrime* terbesar yang berkaitan dengan dunia bisnis *internet* di Indonesia.

Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau *on-line*. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi pembelian barang di *internet*.

¹⁷ Ibid. (Edmon Makarim, 2001: 12).

¹⁸ Ibid (Purbo, dan Wijahirto, 2000: 9).

¹⁹ Menurut RM. Roy Suryo dalam Warta Ekonomi No. 9, 5 Maret 2001 h.12. Lihat juga www.hukumonline.com, "roy suryo sebagai saksi ahli dalam sidang pembobolan kartu kredit." [Serial Online], [02 januari 2004]. <http://www.hukumonline.com/>, diakses 1 september 2006

2. Memasuki, memodifikasi atau merusak *homepage* (hacking)

Tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia baru sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank

3. Penyerangan situs atau *e-mail* melalui virus atau *spamming*.

Modus yang paling sering terjadi adalah mengirim virus melalui *e-mail*, di luar negeri kejahatan seperti ini sudah diberi hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya.

kasus-kasus *cybercrime* yang paling sering terjadi di Indonesia menjadi sorotan pada beberapa tahun belakang dapat di kategorikan menjadi lima, yaitu:²⁰

- a. Pencurian nomor kartu kredit.
- b. Pengambilalihan situs *web* milik orang lain.
- c. Pencurian akses *internet* yang sering dialami oleh ISP.
- d. Kejahatan nama *domain*.
- e. Persaingan bisnis dengan menimbulkan gangguan bagi situs saingannya

2.3.2 Yurisdiksi hukum pidana di dalam *Cybercrime*

Yurisdiksi adalah kekuasaan atau kompetensi hukum negara terhadap orang benda atau peristiwa (hukum). Yurisdiksi ini merupakan refleksi dari prinsip dan kedaulatan Negara, kesamaan derajat Negara dan prinsip tidak campur tangan,. Yurisdiksi juga merupakan sebagai suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum.²¹

²⁰ Teguh wahyono. 2006. *Etika Komputer dan tanggung jawab profesional dibidang teknologi informasi*. Yogyakarta : Andi, h. 30

²¹ Dikdik M. Aries Mansur dan Elisatris Gultom. Opcit h. 30 lihat juga shaw, *international la*, London : Butterworths, 1986, hlm.342. sebagaimana dikutip oleh Huala Adolf, aspek-aspek Negara dalam hukum internasional, rajawali pers, Jakarta,1996, hlm. 1430

Yurisdiksi suatu Negara yang diakui hukum Internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sementara komunikasi multimedia bersifat internasional, multiyurisdiksi, dan tanpa batas, sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu Negara dapat di berlakukan terhadap komunikasi multimedia sebagai salah satu pemanfaatan teknologi informasi.²²

Berkaitan dengan hal diatas maka di perlukan suatu azas –azas hukum sebagai hukum yang bersifat khusus hukum pidana mempunyai asas-asas hukum yang yang bersifat khusus pula. Dalam hal dilarang dan diancam suatu perbuatan (dengan pidana), yaitu mengenai perbuatan pidananya sendiri, dengan *criminal act*, ada dasar yang pokok yaitu asas legalitas, asas yang menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana dengan jika tidak ditentukan terlebih dahulu dalam undang-undang²³

Kitab Undang-undang Hukum Pidana mengenal subjek hukum yaitu orang (Pribadi Kodrati). Timbul pemahaman baru mengenai subjek hukum pidana ini yang diawali dengan pemikiran terhadap suatu perkumpulan orang yang melakukan kegiatan hukum. Subjek hukum ini dikenal sebagai Badan Hukum (Pribadi Hukum), sehingga dengan demikian muncul permasalahan apakah bisa suatu badan hukum diajukan sebagai pelaku tindak pidana ? Pandangan hukum pidana yang tidak menghendaki bahwa badan hukum dapat menjadi subjek hukum pidana tidak lagi digunakan.

Penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu : pertama, *subjective territoriality*, yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain. Kedua, *objective territoriality*, yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi

²² Dikdik M. Aries Mansur dan Elisatris Gultom, *loc cit*

²³ Wahid,abdul dan labib, Muhammad. 2006. *Kejahatan mayantara.*, Bandung: Rafika Aditama. hlm

dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan. Ketiga, *nationality* yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku. Keempat, *passive nationality* yang menekankan yurisdiksi berdasarkan kewarganegaraan korban. Kelima, *protective principle* yang menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah, dan keenam, asas *Universality*²⁴.

Asas *Universality* selanjutnya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus *Cyber*. Asas ini disebut juga sebagai "*universal interest jurisdiction*". Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (*crimes against humanity*), misalnya penyiksaan, genosida, pembajakan udara, dan lain-lain. Meskipun di masa mendatang asas yurisdiksi universal ini mungkin dikembangkan untuk *internet piracy*, seperti *computer, cracking, carding, hacking and viruses*, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional.²⁵

2.3.3 Pembobolan kartu kredit sebagai salah satu bentuk dari *cybercrime*

Carding, sebuah ungkapan mengenai aktivitas berbelanja secara maya (lewat komputer), dengan menggunakan berbagai macam alat pembayaran yang tidak sah. Dalam kasus *carding* tercatat mendominasi kejahatan sejak 1999 hingga akhir Agustus 2004 dimana selama periode Januari–Agustus tahun ini, kerugian akibat *carding* dilaporkan telah mencapai US\$4.543.176²⁶

²⁴ Philip Renata. *Loc cit*

²⁵ Ramli, ahmad. prinsip-prinsip cyber law dan kendala hukum positif dalam menanggulangi cyber crime.padjajaran 2004

²⁶ Mk7 des. "suatu penelitian tentang kejahatan *carding* di bandung". [serial online] [15 januari 2006], <http://www.komputekonline.com/>, diakses 1 september 2006

Modus operandi ini merupakan cara bagaimana proses *carding* dilakukan oleh para *carder* adalah sebagai berikut²⁷ :

1. Mencari kartu kredit yang masih valid, hal ini dilakukan dengan mencuri atau kerjasama dengan orang-orang yang bekerja pada hotel atau toko-toko gede (biasanya kartu kredit orang asing yang disikat). atau masuk ke program MIRC (chatting) pada server dal net, kemudian ke channel #CC, #Carding, #indocarder, #Yogyacarding,dll. nah didalamnya kita dapat melakukan trade istilah tukar antar kartu kredit (bila kita memiliki kartu kredit juga, tapi jika tidak punya kartu kredit, maka dapat melakukan aktivitas *rippe*" dengan menipu salah seorang yang memiliki kartu kredit yang masih valid).
2. Setelah berhasil mendapatkan kartu kredit, maka *carder* dapat mencari situs-situs yang menjual produk-produk tertentu (biasanya di cari pada *search engine*). tentunya dengan mencoba terlebih dahulu kartu kredit tersebut di situs-situs porno (hal ini disebabkan karena kartu kredit tersebut tidak hanya dipakai oleh *carder* tersebut). jika di terima, maka kartu kredit tersebut dapat di belanjakan ke toko-toko tersebut.
3. Cara memasukan informasi kartu kredit pada merchant pembayaran toko adalah dengan memasukan nama panggilan (*nick name*), atau nama palsu dari si *carder*, dan alamat aslinya. atau dengan mengisi alamat asli dan nama asli si empunya kartu kredit pada form billing dan alamat si *carder* pada *shipping address*.

Indonesia menduduki peringkat tertinggi sebagai pelaku *cyber crime* atau kejahatan internet. Sebesar 90 persennya adalah kejahatan *carding* atau pemalsuan kartu kredit. Kecenderungan ini diduga akan terus meningkat.

Hal itu disampaikan anggota Badan Reserse Kriminal Kepolisian RI Direktorat II Ekonomi dan Khusus Unit V Infotek-Cyber Crime Komisarisi Polisi

²⁷ FN Jovan. *Pembobolan Kartu Kredit. "Menyingkap tehnik & cara kerja para carder internet.* Tangerang. Mediakita h.5

Idam Wasiadi pada Seminar Nasional Sehari Information Technology Security di Hotel Horison Bandung, Selasa (13/9). Menurut Idam, tahun 2004 kejahatan *carding* mencapai 177 dari 192 kasus kejahatan internet. Tahun sebelumnya, kejahatan *carding* 145 dari 153 kasus kejahatan internet. "Angka itu dipastikan akan meningkat pada tahun ini. Tahun 2004 Indonesia di posisi kedua di bawah Ukraina, dan tahun lalu Indonesia di peringkat satu," ujar Idam.

Kenyataan ini dibenarkan oleh ahli telematika Roy Suryo Notodiprodo. Roy menegaskan, kejahatan *carding* tahun 2002 sudah tinggi, yaitu 152 dari 155 kejahatan internet. Hampir seluruhnya bermotifkan ekonomi, bahkan pelakunya sebagian besar adalah mahasiswa. "Pasalnya, 48 persen pengguna internet adalah usia 22-25 tahun, kebanyakan mereka mahasiswa. Terbanyak kedua usia 18-21 tahun, sekitar 28 persen," katanya.²⁸

Daerah Yogyakarta menduduki peringkat tertinggi untuk kasus kejahatan *carding*, disusul dengan Semarang, Bandung, Jakarta, Medan, Surabaya, dan Riau. Amerika Serikat adalah negara korban yang paling sering menjadi sasaran kejahatan *carding* dari Indonesia, sekitar 84 persen. Sumber daya manusia di kepolisian belum menguasai teknologi dengan maksimal. Sampai saat ini Markas Besar Kepolisian RI masih berperan sebagai penyelidik untuk kasus di daerah.

Meningkatnya kejahatan ini disebabkan belum adanya undang-undang tentang kejahatan internet di Indonesia, ditambah lagi kemajuan teknologi yang pesat. ". Ketiadaan UU Informasi Elektronik dan Transaksi Elektronik (IETE) sebenarnya dihambat oleh sikap masyarakat yang apatis terhadap masalah ini. RUU IETE yang sudah tiga tahun diajukan belum juga disetujui DPR.²⁹

²⁸ www.hukumonline.com., "roy suryo sebagai saksi ahli dalam sidang pembobolan kartu kredit." [Serial Online], [02 januari 2004]. <http://www.hukumonline.com/>, diakses 1 september 2006

²⁹ Mk7 des. Loc cit

BAB III PEMBAHASAN



3.1 Upaya Penanggulangan Kejahatan *Cybercrime* dengan hukum pidana Sebelum Ada Aturan yang Mengatur Secara Khusus

Proses penegakkan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban didalam kehidupan bermasyarakat. Melalui sistem peradilan pidana dan sistem pemidanaan. Pada dasarnya hak-hak warga negara yang terganggu akibat perbuatan melawan hukum seseorang akan diseimbangkan kembali, dengan semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi muncul berbagai jenis kejahatan berdimensi baru, yang termasuk di dalamnya *cybercrime*. Sejalan dengan itu diperlukan penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum upaya ini di realisasikan dengan hukum pidana. Hukum pidana diharapkan mampu untuk memenuhi cita ketertiban masyarakat.

Ahli telematika Roy suryo berpendapat bahwa, masalah *cybercrime* ini belum diatur secara tegas dalam KUHP. Untuk itu, dalam setiap perkara yang disidangkan, perkara ini akan dapat menjadi sebuah yurisprudensi bagi persidangan dengan kasus yang serupa¹⁰. Berdasarkan pernyataan roy suryo diatas hal ini mengacu pada asas legalitas dalam sistem hukum pidana di indonesia, ditentukan bahwa suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan ketentuan perundang-undangan pidana yang telah ada sebelumnya. Sehingga jika mengacu pada ketentuan pasal 1 ayat (1) KUHP tersebut, maka pelaku *cybercrime* di indonesia belum dapat dijerat dengan hukum, ketiadaan undang-undang yang menjadi penyebab tidak dapat dihukumnya para pelaku kejahatan ini. Tetapi apabila kejahatan ini dibiarkan maka akan semakin merajalela. Sebenarnya hakim dapat melakukan penafsiran hukum

¹⁰ rakyat.com., "mahasiswa pembobol kartu kredit diadili", [Serial Online], [3 Agustus 2002]. Diakses tanggal 16 september 2006

terhadap setiap permasalahan yang dihadapkan kepadanya apabila perkara tersebut merupakan perkara baru bahkan kalau putusan hukum yang dikeluarkan oleh hakim dapat diterima oleh masyarakat hukum, maka putusan tersebut dapat menjadi yurisprudensi

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana. Pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal dengan menggunakan sarana hukum pidana, dan oleh karena itu termasuk bagian dari kebijakan hukum pidana³¹.(Barda Nawawi Arief, 2001:2-3)

Di samping usaha penanggulangan kejahatan, lewat pembuatan undang-undang pidana pada hakekatnya merupakan bagian integral dari usaha kesejahteraan masyarakat (*social welfare*). Oleh karena itu wajar pula apabila dikatakan, bahwa politik hukum pidana juga merupakan bagian integral dari kebijakan sosial (*social policy*). *Social policy* dapat diartikan sebagai segala usaha yang rasional untuk mencapai kesejahteraan masyarakat sekaligus mencakup perlindungan masyarakat. Jadi di dalam pengertian *social policy*, sekaligus didalamnya tercakup *social welfare policy* dan *social defence policy*.

Dilihat dari sudut yang luas tersebut, maka dapat ditegaskan bahwa masalah kebijakan hukum pidana pada hakikatnya bukanlah semata-mata pekerjaan teknik perundang-undangan yang dapat dilakukan secara yuridis normatif dan sistematis-dogmatik. Di samping pendekatan yuridis normatif, kebijakan hukum pidana juga memerlukan pendekatan yuridis faktual yang dapat berupa pendekatan sosiologis, psikologis, historis dan komparatif, bahkan memerlukan pula pendekatan integral dengan kebijakan sosial dengan pembangunan nasional pada umumnya.

Pada dasarnya pencegahan dan penanggulangan kejahatan harus dilakukan dengan integral yaitu adanya keseimbangan antara sarana penal dan non penal, dilihat

³¹ Barda nawawi Arif.2001. "Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tindak Pidana Mayantara", Makalah Seminar Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi, Semarang, 26 Juli 2001. hal 2-3

dari sudut kriminal dalam permasalahan ini paling strategis menggunakan sarana non penal karena lebih bersifat preventif.

Garis kebijakan penanggulangan *Cybercrime*, dikatakan lebih lanjut oleh Barda Nawawi arif, diharapkan tidak hanya penanggulangan kejahatan melalui kebijakan *penal* (baik hukum pidana formil maupun materiil) yang dalam hal ini dilakukan dengan beberapa tahap yaitu

1. Formulasi (kebijakan legislatif)
2. Aplikasi (kebijakan yudikatif)
3. Eksekusi (kebijakan eksekutif)

Suatu pengaturan secara khusus diperlukan apabila tindak pidana mayantara dianggap sebagai kejahatan kategori baru (*new category of crime*) yang membutuhkan suatu kerangka hukum yang baru dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan biasa, dan karena itu perlu diatur secara tersendiri di luar KUHP. Sedangkan apabila menganggap tindak pidana mayantara sebagai kejahatan biasa (*orninary crime*) yang dilakukan dengan komputer teknologi tinggi (*high-tech*) dan KUHP dapat dipergunakan untuk menanggulangnya baik melalui amandemen KUHP maupun perubahan KUHP secara menyeluruh.

Untuk menentukan pilihan tersebut maka secara konseptual harus mempertimbangkan sistem hukum (pidana) di Indonesia. Rene David pernah mengatakan bahwa sistem hukum di Indonesia adalah *mixed system of law*.³² Namun dibidang hukum publik khususnya hukum pidana tradisi hukum kontinental nampak lebih menonjol dalam praktek dan pengembangan ilmu hukum. Oleh sebab itu pengembangan pengaturan mengenai masalah tindak pidana mayantara lebih tepat apabila menggunakan pendekatan integratif dengan pengaturan dalam KUHP baik melalui amandeman maupun perubahan menyeluruh KUHP.

³² *Ibid*

Selain dengan kebijakan penal perlu juga digunakan kebijakan *non penal* yang diharapkan dapat untuk mempertahankan keamanan di *cyberspace*³³, kebijakan tersebut antara lain :

1. Pendekatan teknologi (*technoprevention*),
2. Pendekatan sosial budaya-etika, dan

Kebijakan *non penal* terkait dengan pendekatan *technoprevention* yaitu upaya pencegahan/penanggulangan kejahatan dengan menggunakan teknologi. Terkait pernyataan tersebut maka untuk mengatasi gangguan keamanan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, dintersepsi, atau diakses secara ilegal dan tanpa hak. jadi dalam hal ini suatu pendekatan teknologi dipergunakan untuk mengetahui segala hal yang berkaitan dengan *Cybercrime* utamanya dalam hal penentuan hukumnya, oleh karenanya diperlukan suatu kepercayaan tersendiri terhadap suatu teknologi untuk pemecahan masalahnya

Oleh karenanya dengan adanya tahap formulasi maka upaya penanggulangan dan pencegahan kejahatan bukan hanya tugas aparat semata, bahkan pada tahap formulasi ini merupakan tahap yang paling strategis dari upaya penanggulangan dan pencegahan kejahatan oleh karenanya kesalahan kebijakan legislatif merupakan kesalahan strategis yang dapat menjadi penghambat dalam tahap-tahap berikutnya

Antony mulder mengemukakan bahwa kebijakan hukum pidana ini adalah garis kebijakan untuk menentukan seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu dirubah atau diperbaharui, apa yang dapat di perbuat untuk mencegah tindak pidana dan bagaimana cara penyelesaiannya.

Penafsiran Antony mulder diatas merunut pada suatu fungsi dari kebijakan hukum pidana yaitu untuk menyelesaikan suatu bentuk tindak pidana, dua pendekatan non penal diatas semata dilakukan untuk mendapatkan suatu arah dari perkembangan

³³ danan mursito. 2005. *pendekatan hukum untuk keamanan dunia cyber serta urgensi cyber law bagi Indonesia*. Dalam sebuah tesis sarjana ilmu komputer, perpustakaan universitas indonesia. h.11

teknologi. Sangat disadari tampaknya oleh kongres PBB bahwa *cybercrime*, yang terkait erat dengan kemajuan teknologi, tidak dapat semata-mata ditanggulangi dengan pendekatan yuridis tetapi juga harus ditanggulangi dengan pendekatan teknologi itu sendiri.³⁴ Dengan demikian dapat disimpulkan bahwa hukum dalam menghadapi *Cybercrime* masih sangat jauh dan memadai, apalagi sebagaimana diketahui bahwa KUHP adalah produk masa silam, yang pada waktu dibuatnya tidak mengenal komputer apalagi internet. Oleh karena itu sangat penting untuk melakukan pendekatan ini sebelum di buatnya peraturan yang mengatur secara spesifik.

Kebijakan penanggulangan *cybercrime* melalui pendekatan sosial budaya dan etika, yaitu membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cybercrime* dan menyebarluaskan serta mengajarkan etika penggunaan computer melalui media pendidikan, pentingnya pendekatan budaya di khususnya sebagai upaya pengembangan kode etik dan perilaku³⁵. Hal ini terungkap didalam pernyataan International Information Industri Congress IIC sebagai berikut :

IIC members are also committed to participate in the development of codes of behaviour and ethics around computer and internet use, and in campaigns for the need for ethical and responsible online behaviour. Given the international reach of internet user around the world must be made aware of the need for high standards of conduct in cyberspace³⁶

Istilah *cybercrime* sendiri dijelaskan lebih lanjutkan dalam kongres PBB dapat dikategorikan menjadi 2 yaitu dalam arti sempit ("*in a narrow sense*") dan dalam arti luas ("*in a broader sense*").³⁷

a. *cybercrime in a narrow sense (computer crime) :*

any illegal behaviour directed by means of electronics operations target the security of computer systems and the data processed by them

Barda nawawi Arif. 2001. *Masalah Penegakkan Hukum dan Kebijakan Penanggulangan Kejahatan*. Bandung.Citra Aditya Bakti. H. 246

³⁵ ibid

³⁶ Barda Nawawi Arif, 2006. *tindak pidana mayantara*. Jakarta: Raja Grafindo Perkasa. H.6

³⁷ Ibid

b. *cybercrime in a broader sense (" computer-related crime")*

any illegal behaviour committed by means of or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.

Ditegaskan oleh barda nawawi arif bahwa dalam dokumen itu *Cybercrime* meliputi kejahatan yang dilakukan :

- 1) Dengan menggunakan sarana-sarana dari sistem/jaringan komputer ("*by eans of a computer system or network*")
- 2) Di dalam sistem/jaringan komputer ("*in a computer system or network*")
- 3) Terhadap sistem atau jaringan komputer ("*against a computer system or network*")

Cybercrime dalam hal ini berkaitan langsung dengan suatu sistem

Kendala yang dihadapi dalam penanggulangan *CyberCrime* dengan sarana penal antara lain :

1. Perbuatan jahat yang dilakukan berada dilingkungan elektronik. Oleh karena itu penanggulangannya memerlukan keahlian khusus, prosedur investigasi, dan kekuatan/dasar hukum yang mungkin tidak tersedia pada aparat penegak hukum di negara kita
2. *Cybercrime* melampaui batas-batas negara, sedangkan upaya penyidikan dan penegakkan hukum selama ini di batasi dalam wilayah teritorial Negeranya sendiri
3. Struktur terbuka dari jaringan computer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum yang belum mengkriminalisasi *cybercrime*. terjadinya "*data havens*" (Negara tempat berlindung/singgahnya data yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha Negara lain untuk memberantas kejahatan itu

Terjadinya kendala tersebut menyebabkan perbedaan kebijakan “penal” di setiap negara yang dapat menjadikan penghambat, dengan demikian masalah tersebut perlu adanya harmonisasi kebijakan “penal” di berbagai negara, Sebagai contoh adalah apabila ada seorang warga negara indonesia yang melakukan tindak pidana di negara orang lain maka pemerintah indonesia dapat mengambil tindakan tegas, pelaku tersebut dapat di hukum di indonesia sesuai dengan ketentuan pasal 5 KUHP

Dalam pasal ini diletakkan prinsip nasional aktif atau personalitas, bagi Warga Negara Indonesia yang melakukan kejahatan yang disebutkan dalam pasal 5, meskipun pada waktu melakukan kejahatan itu di luar wilayah Indonesia tetapi dapat dikenakan Undang-Undang Republik Indonesia apabila ia melakukan peristiwa pidana lainnya yang dipandang sebagai kejahatan, maka sebaliknya dia ke indonesia dapat diadili di pengadilan negeri jakarta pusat hal ini sesuai dengan Pasal 84 KUHP

Saat ini Dewan Eropa berusaha melakukan harmonisasi kebijakan penal melalui suatu konversi dan kemudian akan di sosialisasikan ke masing-masing negara anggota. Maka dapat disimpulkan bahwa jika melihat unturnya maka ada sebagian dari *cybercrime* yang dapat dijerat dengan hukum pidana Indonesia, dan sebagian lagi tidak dapat dikarenakan merupakan hal yang bersifat baru. Namun demikian apabila melihat ketentuan yang mengatur tentang berlakunya hukum pidana maka sulit sekali. Hal ini dikarenakan *cybercrime* tidak jelas yurisdiksinya atau merupakan *globalcrime*

Undang-undang yang diharapkan (*ius Constituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan *internet* dengan berbagai motivasi yang dapat menimbulkan korban seperti kerugian materi dan non materi.³⁸

Indonesia sebetulnya sudah memiliki payung *Cyberlaw*. Paling tidak, hal ini tertuang dalam Undang Undang Dasar (UUD) 45 yang saat ini sudah diubah dan

³⁸ Petrus Reinhard Golose. Sebuah makalah tentang. *Perkembangan cybercrime dan upaya penanganannya di Indonesia oleh Polri*, H. 10

sangat canggih serta akomodatif. Pasal 28 F sebagai bagian dari Bab XA mengenai Hak Asasi Manusia, berbunyi sebagai berikut

Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia

Pasal 28 F tersebut terdapat kata-kata yang menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia, maka terlihat bahwa perubahan UUD ini sangat jeli untuk tidak terjebak dalam perkembangan teknologi. Artinya tidak mau menyebut jenis salurannya, karena yang membuat UU mungkin sadar bahwa perkembangan teknologi ini sangat cepat dan UU harus berlaku universal. Teknologi netral ini, sangat tepat. Sebab, dicantumkan pula segala jenis saluran informasi dan komunikasi. Artinya, bisa saja diinterpretasikan bahwa media meliputi, media tradisional (media cetak, majalah, koran), media elektronik (media tv, radio, bahkan telepon dan *faximile*) dan media modern seperti *internet (email, radio internet, radio satelit, wireless* dan lain sebagainya). Segala UU yang ada hubungannya dengan komunikasi dan informasi, nantinya dapat bertumpu atau menjadi turunan dari Pasal 28 F. Contohnya, RUU IETE.

RUU IETE ini, juga menimbang pada UUD 45 secara umum. Jadi, dengan adanya perubahan pada UUD 45 yang sudah disahkan tersebut, maka dimasa mendatang RUU IETE dapat menimbang, khususnya pada Pasal 28 F. Dengan demikian, Pasal seperti pasal 3 dari RUU IETE yang berbunyi, setiap orang tidak boleh menolak keberadaan dari suatu informasi hanya karena berbentuk elektronik dan Pasal 5 yang berbunyi, setiap orang yang menyatakan hak, memperkuat hak yang telah ada atau menolak hak orang lain berdasarkan keberadaan suatu informasi elektronik, sebetulnya dapat menjadi penjelasan dari Pasal 28 F yang sudah ada di UUD 45 yang baru. Oleh karena itu perlu dilakukan upaya lebih lanjut dari pihak aparat penegak hukum di dalam penanggulangan masalah *cybercrime* sebelum adanya aturan yang mengatur secara khusus.

Menurut Widyopramono, SH. undang-undang tradisional masih dapat digunakan. Hal ini juga diungkapkan oleh Kabag Reserse Ekonomi (Resek) Ditserse Polda DIY Kopol Didik S Yasmin mengatakan bahwa Kejahatan seperti *Cybercrime* memang belum diatur KUHP, namun yang kita bidik adalah perbuatannya itu," tutur Didik³⁹.

Cybercrime adalah suatu kejahatan konvensional yang membutuhkan suatu pengaturan tersendiri, oleh karena itu hukum bersifat dinamis, maka dalam hal ini hakim sebagai penegak hukum hanya memandang kodifikasi sebagai pedoman agar ada kepastian hukum, sedangkan didalam memberi putusan hakim harus juga mempertimbangkan dan mengingat perasaan keadilan, di dalam permasalahan *cybercrime* ini hakim dapat memberikan penafsiran secara ekstensif yang memberikan dengan memperluas arti kata-kata dalam itu sehingga sesuatu peristiwa dapat diansukkannya dan untuk itu dalam hal ini penulis berpendapat bahwa pasal di dalam KUHP masih dapat dipergunakan dan menyimpulkan bahwa ada beberapa hukum positif yang berlaku umum yang dapat di jadikan sebagai acuan dalam menjerat tindakan para pelaku *cybercrime* tersebut, antara lain:

1. Kitab Undang-Undang Hukum Pidana (KUHP)

- a. Pasal 362 KUHP

Pasal ini dapat di kenakan untuk kasus Pencurian Data. Meski istilah ini dikategorikan sebagai kejahatan yang populer namun kasus ini di interpretasikan dengan tindak kejahatan konvensional pada umumnya yaitu pencurian

- b. Pasal 378 KUHP

Pasal ini dapat dikenakan untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan disalah satu

³⁹ www.pikiranrakyat.com, "mahasiswa pembobol kartu kredit diadili", [SerialOnline], [3 Agustus 2002]. Diakses tanggal 16 september 2006

website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan, tetapi pada kenyataannya barang itu tidak ada

c. pasal 303 KUHP

Pasal ini dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di *internet*

d. Pasal 282 KUHP

Pasal ini dapat dikenakan untuk kasus penyebaran pornografi baik untuk tujuan kesenangan belaka ataupun untuk bisnis

e. Pasal 112 KUHP

Pasal ini dikenakan bagi paa *hacker* karena tindakan yang dia lakukan bisa membahayakan negara dengan jalan membocorkan rahasia

f. Pasal 262 KUHP

Pasal ini dikenakan pada kasus pembobolan kartu kredit karena pelaku melakukan penipuan seolah-olah ingin membeli sesuatu barang dan membayarnya dengan kartu kredit yang nomornya merupakan curian

g. Pasal 406 KUHP

Pasal ini dikenakan kepada *hacker* yang karena aktivitasnya menimbulkan kerusakan atau kerugian yang luar biasa kepada usaha seseorang, institusi atau negara

h. Pasal 372 KUHP

Pasal ini digunakan untuk menjaring pelaku penggelapan data. Dalam hal ini pelakunya orang dri suatu perusahaan yang bergerak di bidang Teknologi Informasi (TI) atau operator sistem suatu perusahaan *server*

i. Pasal 264 KUHP

Pasal ini dikenakan pada kasus pemalsuan surat kredit yang nantinya di jadikan sebagai dasar di dalam belanja *online*

Dan beberapa Undang-Undang Khusus yang mengatur secara tidak langsung hal-hal yang berkaitan dengan *cybercrime*:

1. Undang-Undang No.19 tahun 2002 tentang Hak Cipta
Undang-undang ini digunakan untuk melindungi pembajakan karena maraknya aksi pembajakan di Indonesia di nilai sudah sangat merugikan pemilik hak cipta
2. Undang-Undang No.36 tahun 1999 tentang Telekomunikasi
Bahwa dalam undang-undang ini diatur lebih lanjut tentang internet sebagai bentuk alat komunikasi,. Dan penyalahgunaan dari internet dapat dikenakan sanksi tersendiri dalam undang-undang ini
3. Undang-Undang No. 8 tahun 1997 tentang Dokumen Perusahaan
Dalam hal ini diatur tentang permasalahan pembuktian yaitu pengakuan atas *microfilm* dan media lainnya sebagai alat penyimpan informasi yang bukan kertas dan mempunyai tingkat keamanan yang dapat menjamin keaslian dokumen yang dialihkan
4. Undang-Undang No.25 tahun 2003 tentang Pencucian Uang
Dalam undang-undang ini merupakan salah satu sarana pembuktian elektronik atau *digital evidence* sesuai dengan pasal 38 (b) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

Cybercrime di negara kita adalah hal awam bahkan para aparaturnya Negara kita masih belum mampu untuk menjangkau serta memberikan solusi yang tepat di dalam penyelesaiannya hal ini disebabkan beberapa faktor :

1. faktor kesadaran hukum masyarakat
2. faktor keamanan
3. faktor penegak hukum
4. faktor ketiadaan undang-undang

Upaya dalam penanganan kejahatan *Cyber* pada dasarnya sudah dilakukan sejak beberapa waktu yang lalu sejalan dengan hal itu peran serta masyarakat selalu

dituhkan di dalamnya, sikap kooperatif dengan aparat akan sangat membantu penyelesaiannya penanganan kasus *Cybercrime*,

Sebagai bagian dari kebijakan formulasi dari penanggulangan permasalahan outdemikian juga dari aparat penegak hukum hendaknya lebih meningkatkan upaya tindakan seperti yang dikatakan oleh Petrus Reinhard Golose⁴⁰ :

1. **Personil**

Terbatasnya Sumber Daya manusia merupakan salah satu masalah yang penting, kemauan dan usaha untuk menjadikan Negara Indonesia lebih maju hendaknya di tanamkan pada diri setiap aparat penegak hukum sehingga mereka tidak segan untuk meluangkan waktu untuk belajar dari Negara luar

2. **Sarana Prasarana**

Perkembangan tekhnologi yang cepat tidak dapat dihindari sehingga aparat berusaha semaksimal mungkin untuk *mengupdate* dan *mengupgrade* sarana dan prasarana yang dimiliki

3. **Kerjasama dan Koordinasi**

Malakukan kerjasama antar penegak hukum dalam masalah *Cybercrime* hendaknya lebih sering di lakukan mengingat dalam kasus ini tidak mengenal batas wilayah

4. **Sosialisasi dan Pelatihan**

Memberikan sosialisasi mengenai kejahatan *Cyber* dan cara penanganan serta pelatihan dan ceramah mengenai *Cybercrime* agar memiliki kesamaan persepsi dan pengertian yang sama dalam melakukan penanganan.

Keempat hal diatas pada dasarnya saling terkait antara yang satu dengan yang Di sadari atau tidak bangsa kita memang lambat dalam upaya penanganan lah *Cybercrime* ini, berbagai alasan menyertai sebab kenapa kita tidak cepat ap di dalam penyelesaian masalah. Pada umumnya apabila kita ingin melakukan masi hukum hendaknya satu hal yang paling mendasar adalah menuju perbaikan al, dalam penegakkan hukum perlu juga disertai dengan reformasi kualitas uan para aparat yang berwenang.

Sangatlah bijaksana apabila aparat menyatakan bahwa langkah-langkah aksanaannya akan didasarkan pada penekatan kilmuan. Diharapkan hal ini dapat ngkatkan kualitas produk legeslatif dan produk penegakkan hukum. Tidaklah

us Reinhard Golose, *op.cit.*, h.22

ada artinya undang-undang dan lembaga penegakkan hukumnya diperbaharui, apabila ilmu pembuat undang-undang dan aparat penegak hukumnya tidak juga di perbaharui dan ditingkatkan. Terlalu banyak fenomenaproduk legeslatif dan produk yudikatif atau produk penegakkan hukum lainnya yang bersumber pada latar belakang keilmuannya yang lemah

3.2 Alternatif Penyelesaian Perkara Pembobolan Kartu Kredit Sebelum Diundangkannya Undang-Undang yang Mengatur

Pembobolan kartu kredit yang marak saat ini adalah salah satu bentuk dari *cybercrime*. Di beberapa negara berkembang yang sudah memiliki undang-undang tentang *cybercrime* mungkin hal ini bukanlah menjadi sebuah masalah yang pelik mengingat setiap negara berkembang telah menjadikan masalah *cyber* suatu masalah yang wajib untuk segera di tangani, ada beberapa pihak yang terkait dalam perkara pembobolan kartu kredit ini yaitu:

1. Pemilik kartu kredit
2. Pihak bank sebagai pemantau arus keluar masuknya transaksi pada kartu kredit
3. *Merchant* atau pembeli

Pembobolan kartu kredit ini di Indonesia umumnya sudah bukan kejahatan baru lagi Pelaku dijerat menggunakan pasal-pasal KUHP yaitu Pasal 362 tentang pencurian, Pasal 378 tentang penipuan, Pasal 268 tentang pemalsuan identitas, karena belum ada Undang Undang khusus *Cyber Crime*, baru ada RUU. Hal ini semata dilakukan agar tidak terjadi kekosongan hukum

Langkah-langkah pencegahan yang selama ini polisi lakukan adalah :

- Mencabut / melarang penggunaan channel-channel chatting
- Penggalangan kerjasama dengan warnet, dengan cara himbauan

Kasus pembobolan kartu kredit jika diteliti lebih lanjut ada beberapa alternatif penyelesaian yang dapat dijadikan landasan bagi para penegak hukum untuk

dapat memutuskan suatu perkara pembobolan kartu kredit sebelum di undangkannya undang-undang Teknologi informasi, yaitu dengan menggunakan KUHP dan UU no. 36 Tahun 1999 tentang Telekomunikasi pertama apabila menggunakan KUHP maka mengacu pada pasal :

1. Pasal 264 ayat (1) ke 5

Yang bersalah karena memalsukan surat dipidana dengan pidana penjara selamamanya delapan tahun, kalau perbuatan itu dilakukan terhadap surat kredit atau surat dagang yang disediakan untuk diedarkan

Diancam hukuman dalam pasal ini adalah orang yang membikin surat palsu atau memalsukan surat kredit atau surat dagang yang disediakan untuk diedarkan dengan maksud untuk memakai atau menyuruh orang lain memakai surat itu, seolah-olah surat itu asli dan tidak dipalsukan, jikalau pemakaian surat itu dapat mendatangkan kerugian.⁴¹

Pada pasal ini yang dapat dijadikan unsur pemberat pidana adalah

4. mempergunakan salah satu jenis surat palsu atau dipalsukan
5. seakan-akan asli dan tidak palsu
6. penggunaannya menimbulkan kerugian
7. dengan sengaja

Disini penafsiran lain dari surat adalah sebuah kartu kredit yang dapat di pergunakan sebagai alat pembayaran secara elektronik yang sah, dalam hal ini sebuah kartu kredit dapat dipalsukan datanya atau dapat digandakan guna kepentingan pribadi ataupun golongan. Pada dasarnya sebuah kartu kredit memegang peran penting dalam transaksi elektronik, bagi para *carder* salah satu tujuan yang hendak dicapai adalah untuk mencuri nomor dari kartu tersebut yang selanjutnya untuk di pakai berbelanja *online*.

⁴¹ R.Sugandi. 1980. *KUHP DAN PENJELASANNYA*. Surabaya: Usaha Nasional. H.281

maka secara otomatis hal ini akan mendatangkan kerugian bagi pemiliknya dan dalam hal ini pemalsuan jenis surat ini dianggap memiliki sifat yang merugikan bagi orang lain

2. Pasal 362

Barangsiapa mengambil barang yang sama sekali atau sebagian kepunyaan orang lain dengan maksud untuk memiliki barang itu dengan melawan hukum, dipidana karena mencuri dengan pidana penjara selama lamanya lima tahun atau denda sebanyak-banyaknya sembilan ribu rupiah

Tindak pidana ini masuk dalam golongan pencurian biasa yang unsur-unsurnya sebagai berikut⁴² :

1. Tindakan yang dilakukan adalah mengambil
2. Yang diambil adalah barang
3. Status barang itu sebagian atau seluruhnya menjadi milik orang lain
4. Tujuan perbuatan itu ialah dengan maksud untuk memiliki barang itu dengan melawan hukum

Dalam hal ini analisis penulis untuk kasus *carding* dimana pelaku mencuri atau mengambil nomor kartu kredit milik orang lain walaupun tidak secara fisik tidak berbentuk barang karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card generator* di internet untuk melakukan transaksi. Karena jelas dalam pasal ini pengambilan nomor kartu kredit itu untuk dimiliki dan dipergunakan secara melawan hukum.

Pembobolan kartu kredit ini utamanya mempunyai tujuan untuk melakukan transaksi dengan modus tanpa modal dapat mendapatkan barang, dalam pasal pencurian ini berbagai macam modus operandi yang dipergunakan oleh para pemburu kartu kredit yaitu dengan cara berpura-pura menjadi penjual gadungan, untuk menarik minat para korbannya biasanya mereka menawarkan berbagai barang yang menarik di berbagai situs lelang. Dan umumnya mereka akan mendapatkan nomor tersebut dengan menjebak seseorang yang akan menjadi pembeli di dalam toko palsu tersebut,

⁴² *Ibid.*, .h. 376

setelahnya para pembeli akan terjebak dengan melakukan pembayaran dengan menggunakan kartu kredit yang mereka punya.

Pasal 378

Barang siapa dengan maksud untuk menguntungkan 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 kepadanya, atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun.

Pasal 378 ini menyebutkan yang diancam hukuman dalam pasal ini ialah orang yang membujuk orang lain supaya memberikan sesuatu barang atau supaya menyerahkan sesuatu barang atau supaya membuat utang atau menghapuskan piutang secara melawan hukum dengan cara tipu muslihat, rangkaian kebohongan, nama palsu dan peri keadaan palsu dengan maksud menguntungkan dirinya sendiri atau orang lain.⁴³

Unsur-unsur terkait pasal ini adalah :

1. Membujuk ialah menanamkan pengaruh sedemikian rupa terhadap orang, sehingga orang yang dipengaruhinya mau berbuat sesuatu sesuai dengan kehendaknya, padahal apabila orang itu mengetahui duduk soal yang sebenarnya, tidak akan mau melakukan hal itu.
2. Mengenai barang
3. Mengenai membuat utang atau menghapuskan piutang
4. Mengenai cara memberikan barang, tidak mutlak harus diserahkan kepada terdakwa sendiri, sedang orang yang menyerahkan tidak mutlak pula harus orang yang dibujuk itu sendiri, hal itu boleh dilakukan oleh orang lain
5. Menguntungkan diri sendiri dengan melawan hukum berarti menguntungkan diri sendiri dengan tiada hak
6. Tipu muslihat ialah suatu usaha yang sedemikian rapi sehingga orang yang berfikiran normal pun dapat mempercayainya

7. Rangkaian kebohongan ialah susunan kalimat-kalimat bohong yang tersusun sedemikian rupa, sehingga kebohongan yang satu di tutup dengan kebohongan yang lain sehingga semuanya seakan-akan benar
8. nama palsu ialah nama yang bukan sebenarnya
9. peri keadilan palsu misalnya seseorang yang tidak mempunyai sesuatu jabatan mengaku dan bertindak sebagai subyek yang lain

Kaitannya dengan *pembobolan kartu kredit*, biasanya para *carder* mereka menggunakan identitas orang lain untuk memenuhi kepentingannya sendiri, identitas orang lain digunakan dengan maksud jahat yakni merugikan orang lain yang identitasnya dipakai atau di curi. hal ini dapat disebut sebagai *Fraud* atau penipuan dengan kepentingan ekonomis. Dalam pasal ini barang yang dimaksud juga dapat diartikan sebagai identitas tau nomor kartu kredit dari para pembeli di *internet*. Oleh karenanya pasal ini lebih banyak digunakan oleh para aparat penegak hukum dalam mengatasi permasalahan *Cybercrime* adapun unsur-unsur yang ada pada pasal pada dasarnya sudah mencakup semua hal yang berhubungan dengan *Cybercrime*

4. Pasal 480

Dipidana dengan pidana penjara selama-lamanya empat tahun tahun denda sebanyak-banyaknya sembilan ratus rupiah :

Ke-1 karena bersalah menadah, barangsiapa membeli, menyewa, menukari, menerima gadai, menerima sebagian hadiah atau karena mau mendapatkan untung, menjual, menyewakan, menukarkan, menggadaikan, membawa, menyimpan, atau menyembunyikan sesuatu barang yang diketahuinya atau patut dapat disangkanya bahwa barang-barang itu diperoleh karena kejahatan.

Ke-2 barang sapa mengambil untung dari hasil sesuatu barang, yang diketahuinya atau patut dapat disangkanya bahwa barang-barang tersebut diperoleh karena kejahatan

5. Pasal 379a

Barangsiapa mejadikan pencarian atau kebiasaan membeli barang, dengan maksud mendapat barang itu untuk dirinya atau orang lain, dengan tidak membayar lunas, dipidana dengan pidana penjara selama-lamanya empat tahun

Kelima pasal dalam KUHP sebenarnya sudah dapat mewakili sebagai suatu dasar hukum didalam proses penuntutan tetapi masih banyak kelemahan apabila masih tidak menggunakan undang-undang lain sebagai pelengkap, jadi pada dasarnya dalam suatu penuntutan dalam kasus pembobolan kartu kredit tidak sesederhana seperti yang dilakukan para aparat penegak hukum, dalam penentuan lamanya hukuman.

Aspek kerugian lain yang jauh lebih berharga dari dilakukannya aktifitas pembobolan kartu kredit ini yaitu :

1. Kerugian dari segi materiil yang diterima oleh objek
2. Kerugian dari segi moril yang di dapatkan oleh negara atas kecaman negara lain.

Kerugian diatas jelas lebih besar efek negatifnya daripada jumlah hukuman yang dijatuhkan oleh para penegak hukum terhadap para pelaku pembobolan kartu kredit ini. Kerugian dari segi materiil dirasakan oleh objek yang di jadikan sasaran oleh para *carder* lebih besar sedangkan kita tidak dapat memberikan jaminan pengembalian kepada korbannya, sedangkan kerugian kedua yaitu dari segi moril, negara akhirnya di tetapkan sebagai *black list* oleh dunia sebagai sarang *Carder*.

Pada dasarnya ada kelebihan dan kekurangan apabila kita menggunakan KUHP secara mutlak, maka tonggak pengembangan sektor teknologi informasi dimulai pada pemerintahan presiden Habibie dengan membentuk Undang-Undang no 36 tahun 1999 (UU No.36 Th 1999)⁴⁴. Didalam peraturan ini disebutkan dengan jelas jenis tindakan pidana dan menjelaskan dengan tegas tentang sanksi pidananya, pada kasusu pembobolan kartu kredit hal ini dapat ditemukan pada pasal :

Pasal 22 jo. 50

Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

- a. akses ke jaringan telekomunikasi; dan atau

⁴⁴ Ramli, ahmad. prinsip-prinsip cyber law dan kendala hukum positif dalam menanggulangi cyber crime.padjajaran 2004

- b. akses ke jasa telekomunikasi; dan atau
- c. akses ke jaringan telekomunikasi khusus.

Dengan ancaman pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)

Pasal 38 jo. 55

Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi. dipidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

Pasal 40 jo. 56

Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun. dipidana penjara paling lama 15 (lima belas) tahun.

Kejelian seorang hakim dalam menentukan suatu hukum yang ada mutlak di perlukan agar tercipta suatu supremasi hukum, hal yang paling utama bahwa selama ini para hakim terlalu memfokuskan diri kepada undang undang saja namun dari analisis penulis masih terdapat beberapa kelebihan dan kekurangan pada masing masing sumber hukum tertulis ini. Beberapa diantaranya kelebihan yang di dapat dalam penerapan KUHP sebagai bentuk upaya penegakkan hukum terkait dengan *Cybercrime* adalah

1. Karena memang tidak adanya peraturan yang mengatur tentang *cybercrime* maka KUHP sebagai hukum positif merupakan langkah yang efektif dirasa untuk saat ini.

Sedangkan kerugian yang didapat adalah

1. KUHP dapat menjadi kerugian apabila kejahatan yang dilakukan membutuhkan suatu pembuktian dan sementara didalam KUHP Pasal 184 sendiri tidak diatur pembuktian elektronik.

2. Menumbuhkan anggapan bahwa KUHP terlalu mudah dan lemah di dalam penentuan hukuman yang akan dijatuhkan terhadap pelaku pembobolan kartu kredit
3. Pengadilan masih belum dapat menerima informasi elektronik sebagai alat bukti
4. Hak dan kewajiban masyarakat tidak diatur dalam hal pemanfaatan internet sebagai sumber informasi

Apabila kita memakai UU Telekomunikasi maka kelebihan yang didapat adalah :

1. Sudah adanya aturan pidana yang mengatur secara pasti
2. Dijelaskan lebih lanjut tentang fungsi alat bukti elektronik dan di sahkan di dalam pengadilan
3. Adanya hak dan kewajiban masyarakat didalam memanfaatkan telekomunikasi

kekurangan yang ada pada UU Telekomunikasi ini adalah

1. Tidak memuat pertanggung jawaban pidana terhadap korporasi

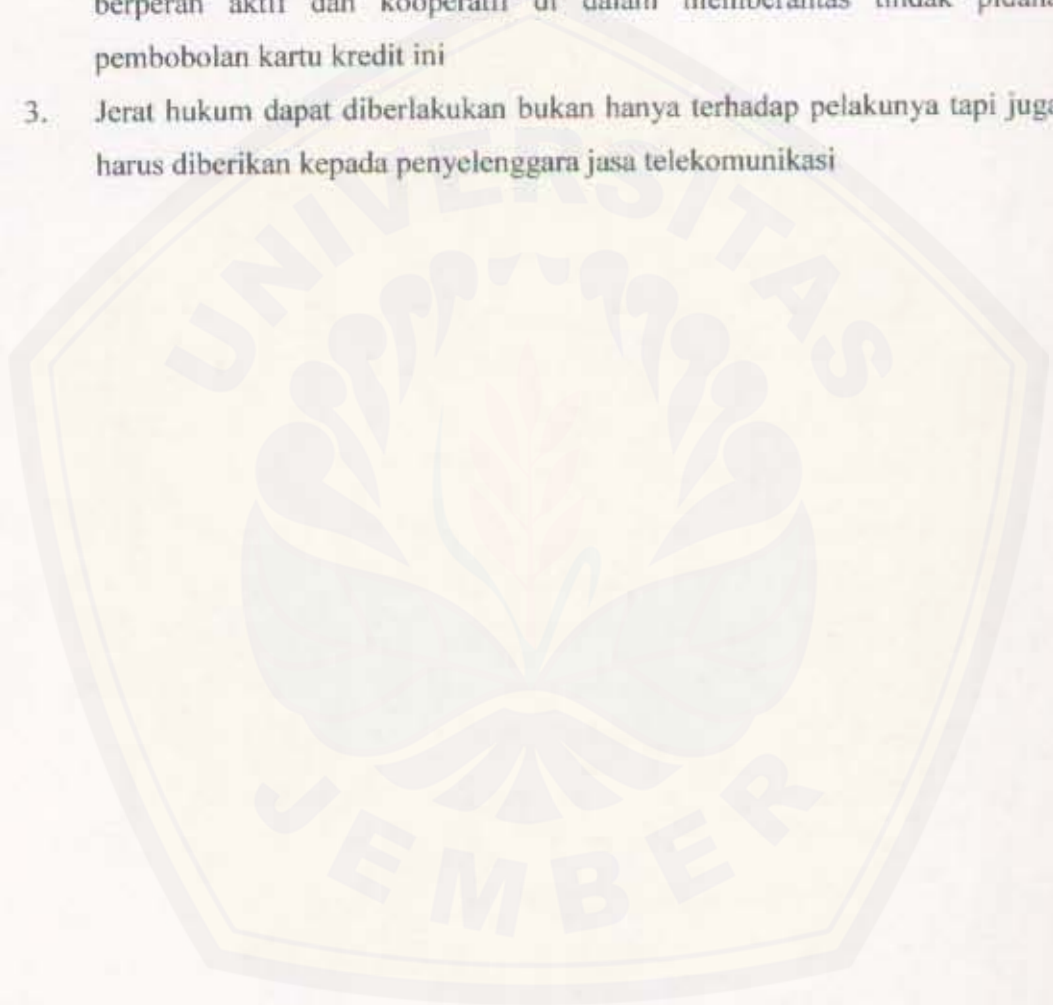
Dengan memperhatikan kondisi peraturan perundang-undangan yang ada, seyogyanya ada keberanian dari inovasi dari aparat penegak hukum untuk mengaktifkan peraturan yang ada dengan melakukan interpretasi atau konstruksi hukum yang bersumber pada teori/ilmu hukum, pendapat para ahli, jurisprudensi atau bersumber dari ide-ide dasar yang secara konseptual dapat dipertanggung jawabkan.

Aparat penegak hukum dalam upaya penanganan kasusnya hendaknya di pergunakan kedua dasar hukum diatas agar lebih efektif di dalam menjerat pelaku Pembobolan kartu kredit. Disini sebuah solusi yang dapat ditawarkan adalah dalam upaya penanggulangan suatu tindak pidana pembobolan kartu kredit adalah :

1. Para aparat penegak hukum hendaknya lebih melakukan studi banding terhadap jenis pidana yang akan di jatuhkan baik itu dengan berdasarkan pada KUHP maupun UU Telekomunikasi sehingga nantinya putusan pidana

yang dijatuhkan dapat dirasakan adil dan tidak ada lagi putusan ringan bahkan bebas

2. Bagi para penyelenggara jasa telekomunikasi khususnya Warnet untuk lebih berperan aktif dan kooperatif di dalam memberantas tindak pidana pembobolan kartu kredit ini
3. Jerat hukum dapat diberlakukan bukan hanya terhadap pelakunya tapi juga harus diberikan kepada penyelenggara jasa telekomunikasi



BAB IV PENUTUP



4.1 Kesimpulan

Berdasarkan permasalahan dan pembahasan yang telah penulis uraikan pada bab-bab sebelumnya, maka dapat disimpulkan bahwa :

1. Upaya penanggulangan kejahatan *Cybercrime* dilakukan dengan kebijakan *penal* dan *non penal* sebagai bagian dari kebijakan kriminalisasi. Dalam kebijakan *penal* karena masih belum adanya undang-undang yang mengatur maka sebagai bagian dari aplikasinya masih menggunakan KUHP sebagai acuan dan hal ini sudah dilakukan terhadap beberapa permasalahan. Sedangkan dalam kebijakan *non penal* terkait dengan pendekatan *Technoprevention*, hal ini mutlak dilakukan karena pendekatan ini dilakukan dengan menggunakan teknologi, hal ini semua bertujuan sebagai suatu bentuk upaya penanggulangan *cybercrime*.
2. Pembobolan kartu kredit yang terus meningkat saat ini sesuai dengan keterangan yang dikeluarkan oleh BARESKRIM Mabes Polri merupakan salah satu bentuk dari *cybercrime*. Pembobolan kartu kredit ini di Indonesia umumnya sudah bukan kejahatan baru lagi Pelaku dapat dijerat menggunakan pasal-pasal KUHP (362 tentang pencurian, 378 tentang penipuan, 264 tentang pemalsuan identitas, 480 tentang penadahan dan pasal 379a), karena belum ada Undang Undang khusus *Cybercrime*. Disamping itu terdapat alternatif penyelesaian dalam kasus pembobolan kartu kredit ini yaitu dengan menyertakan Undang-Undang Telekomunikasi sebab pada Undang-Undang telekomunikasi terdapat unsur pembuktian dan jerat pidana yang lebih tegas,

4.2 Saran

Berdasarkan uraian tersebut di atas, maka saran yang dapat penulis berikan adalah:

1. Segera disahkannya Rancangan Undang - Undang IETE menjadi Undang-Undang yang sah. Mengingat perkembangan *Cybercrime* yang begitu cepat sehingga membutuhkan suatu dasar hukum baru
2. kepolisian dan Kejaksaan sebagai lembaga yang juga mempunyai kewenangan dalam menangani tindak pidana pembobolan kartu kredit, harus meningkatkan kinerjanya dalam mempelajari, memahami dan memperbaiki segala kelemahan-kelemahan yang dimilikinya agar apabila terjadi masalah serupa mereka di harapkan lebih profesional dalam memutuskan dan menjatuhkan pidana dengan seadil-adilnya

DAFTAR PUSTAKA

A. Buku Kepustakaan

- Anwar, D. 2003. *Kamus Lengkap Bahasa Indonesia Terbaru*. Surabaya: AMELIA.
- Wahid, A. 2005. *Kejahatan Mayantara (cyber crime)*. Malang: Rafika aditama.
- Nawawi Arif, Barda. 2001. *Masalah Penegakkan Hukum dan Kebijakan Penanggulangan Kejahatan*. Bandung: Citra Aditya Bakti
- Nawawi Arif, Barda. 2005. *Tindak Pidana Mayantara :Perkembangan Kajian Cybercrime di Indonesia*. Jakarta: Raja Grafindo Persada
- Bawengan, G.W. 1979. *Hukum Pidana di dalam Teori dan Praktek*. Jakarta: Pradnya Paramita.
- Kansil, CST. 1989. *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*. Jakarta: Balai Pustaka
- Agus Riswandi, Budi. 2006. *Hukum Cyberspace*. Cetakan Pertama. Yogyakarta: Gita Nagari
- Hamzah, A. 1985. *Pengantar Hukum Acara Pidana Indonesia: Edisi Revisi*. Jakarta: Ghalia Indonesia.
- , 2001. *Hukum Acara Pidana Indonesia: Edisi Revisi*. Jakarta: Sinar Grafika Offset.
- Jovan, F.N. 2006. *Pembobolan Kartu Kredit : Menyingkap Teknik dan Cara Kerja Para Carder Internet*. Tangerang: Mediakita.
- Kartanegara, S. (Tanpa Tahun). *Hukum Pidana: Buku I. (Tanpa Tempat Terbit)*: Balai Lektor Mahasiswa.
- Lamintang, P.A.F. dan Samosir, C.D. 1983. *Hukum Pidana Indonesia*. Bandung: Sinar Baru.

Lamintang, P.A.F. dan Simons, D. 1992. *Kitab Pelajaran Hukum Pidana (Leerboek Van Het Nederlanches Straftrecht)*. Bandung: Pioner Jaya.

Anwar, Moch., 1989. *Hukum Pidana bagian Khusus: DADING*. Bandung: Citra Aditya Bakti

Wahyono, Teguh. 2006. *Etika Komputer dan Tanggung Jawab Profesional di Bidang Teknologi Informasi*. Yogyakarta: Andi

Prodjodikoro, R.W. 1986. *Hukum Acara Pidana di Indonesia*. Bandung: PT. Bale.

Universitas Jember. 1998. *Pedoman Penulisan Karya Ilmiah: Edisi Pertama*. Jember: Badan Penerbit Universitas Jember.

-----, 2005. *Pedoman Penulisan Karya Tulis Ilmiah: Edisi Revisi*. Jember: Badan Penerbit Universitas Jember.

Marzuki, P.M. *Penelitian Hukum*.

R.Sugandi. 1980. *KUHP DAN PENJELASANNYA*. Surabaya: Usaha Nasional

B. Peraturan Perundang-undangan

Undang-Undang Republik Indonesia Nomor 12 Tahun 1946 Tentang Kitab Undang-undang Hukum Pidana (KUHP).

Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana (KUHAP).

Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi

Undang-Undang Republik Indonesia Nomor 19 Tahun 2002 Tentang Hak Cipta

Undang-Undang Republik Indonesia Nomor. 8 tahun 1997 tentang Dokumen Perusahaan

Undang-Undang Republik Indonesia Nomor No.25 tahun 2003 tentang Pencucian Uang

C. Majalah atau Jurnal

- Rahardjo, Budi. September 2000. "Teknolaw: Beberapa Masalah Teknologi Dan Hukum" Pusat Penelitian Antar Universitas Bidang Mikroelektronika (Ppaume) Institut Teknologi Bandung (Itb)
- Ramli, Ahmad. 2006. Modul I E-Learning :Prinsip-Prinsip Cyber Law Dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime. Fakultas Hukum Universitas Padjadjaran
- Mursito, Danan. 2005. *pendekatan hukum untuk keamanan dunia cyber serta urgensi cyber law bagi Indonesia*. Dalam sebuah tesis sarjana ilmu komputer, perpustakaan universitas indonesia.
- Petrus Reinhard Golose. Sebuah makalah tentang. *Perkembangan cybercrime dan upaya penanganannya di Indonesia oleh polri*

D. Internet dan Lain-lain

- Komputekonline.com *pembobol kartu kredit sulit disidang*. [serial online]. [12 april 2004]. <http://www.komputekonline.com/harian/0509/14/nas20.htm> , diakses 24 agustus 2006
- Polda jabar. *kejahatan teknologi tumbuh subur di indonesia*. [serial online]. [19 juli 2003]. <http://www.kompas.com/harian/14/nas13.htm> , diakses 24 agustus 2006
- Philip Renata. "suplemen BisTek". Warta Ekonomi No. 24 edisi Juli 2000. h.52. Lihat juga www.permasalahancybercrime.com., "pendekatan hukum untuk keamanan dunia cyber serta urgensi cyber law bagi indonesia." [Serial Online], [14 September 2005]. <http://www.duniacyber.com/harian/1/nas33.htm> , diakses 1 september 2006
- RM. Roy Suryo dalam Warta Ekonomi No. 9, 5 Maret 2001 h.12, Lihat juga www.hukumonline.com., "roy suryo sebagai saksi ahli dalam siding pembobolan kartu kredit." [Serial Online], [02 januari 2004]. <http://www.hukumonline.com/>, diakses 1 september 2006

Mk7 des. "suatu penelitian tentang kejahatan carding di bandung". [serial online] [15 januari 2006], <http://www.komputekonline.com/>, diakses 1 september 2006

www.hukumonline.com., "roy suryo sebagai saksi ahli dalam sidang pembobolan kartu kredit." [Serial Online], [02 januari 2004]. <http://www.hukumonline.com/>, diakses 1 september 2006

[www.pikiran rakyat.com](http://www.pikiranrakyat.com)., "mahasiswa pembobol kartu kredit diadili", [SerialOnline], [3 Agustus 2002]. Diakses tanggal 16 september 2006



TELEKOMUNIKASI

(Undang-Undang Republik Indonesia No. 36 Tahun 1999 tanggal 8 September 1999)

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang :

- a. bahwa tujuan pembangunan nasional adalah untuk mewujudkan masyarakat adil dan makmur yang merata materiil dan spiritual berdasarkan Pancasila dan Undang-Undang Dasar 1945;
- b. bahwa penyelenggaraan telekomunikasi mempunyai arti strategis dalam upaya memperkuat persatuan dan kesatuan bangsa, memperlancar kegiatan pemerintahan, mendukung terciptanya tujuan pemerataan pembangunan dan hasilnya, serta meningkatkan hubungan antarbangsa;
- c. bahwa pengaruh globalisasi dan perkembangan teknologi telekomunikasi yang sangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi;
- d. bahwa segala sesuatu yang berkaitan dengan perubahan mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi tsb, perlu dilakukan penataan dan pengaturan kembali penyelenggaraan telekomunikasi nasional;
- e. bahwa sehubungan dengan hal tsb di atas, maka Undang-undang No. 3 Tahun 1989 tentang Telekomunikasi dipandang tidak sesuai lagi, sehingga diganti;

Mengingat:

Pasal 5 ayat (1), Pasal 20 ayat (1) dan Pasal 33 Undang-Undang Dasar 1945;

Dengan persetujuan :

DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA

MEMUTUSKAN :

Menetapkan :

UNDANG-UNDANG TENTANG TELEKOMUNIKASI.

BAB I KETENTUAN UMUM

Pasal 1

Dalam Undang-undang ini yang dimaksud dengan :

1. Telekomunikasi adalah setiap pemancaran, pengiriman, dan atau penerimaan dari setiap informasi dalam bentuk tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya;
2. Alat telekomunikasi adalah setiap alat perlengkapan yang digunakan dalam bertelekomunikasi;
3. Perangkat telekomunikasi adalah sekelompok alat telekomunikasi yang memungkinkan bertelekomunikasi;
4. Sarana dan prasarana telekomunikasi adalah segala sesuatu yang memungkinkan dan mendukung berfungsinya telekomunikasi;

5. Pemancar radio adalah alat telekomunikasi yang menggunakan dan memancarkan gelombang radio;
6. Jaringan telekomunikasi adalah rangkaian perangkat telekomunikasi dan kelengkapannya yang digunakan dalam bertelekomunikasi.
7. Jasa telekomunikasi adalah layanan telekomunikasi untuk memenuhi kebutuhan bertelekomunikasi dengan menggunakan jaringan telekomunikasi;
8. Penyelenggara telekomunikasi adalah perseorangan, koperasi, Badan Usaha Milik Daerah (BUMD), Badan Usaha Milik Negara (BUMN), badan usaha swasta, instansi pemerintah, dan instansi pertahanan keamanan negara;
9. Pelanggan adalah perseorangan, badan hukum, instansi pemerintah yang menggunakan jaringan telekomunikasi dan atau jasa telekomunikasi berdasarkan kontrak;
10. Pemakai adalah perseorangan, badan hukum, instansi pemerintah yang menggunakan jaringan telekomunikasi dan atau jasa telekomunikasi yang tidak berdasarkan kontrak.;
11. Pengguna adalah pelanggan dan pemakai;
12. Penyelenggaraan telekomunikasi adalah kegiatan panyediaan dan pelayanan telekomunikasi sehingga memungkinkan terselenggaranya telekomunikasi;
13. Penyelenggaraan jaringan telekomunikasi adalah kegiatan penyediaan dan atau pelayanan Jaringan telekomunikasi yang memungkinkan terselenggaranya telekomunikasi;
14. Penyelenggaraan jasa telekomunikasi adalah kegiatan penyediaan dan atau pelayanan jasa telekomunikasi yang memungkinkan terselenggaranya telekomunikasi;
15. Penyelenggaraan telekomunikasi khusus adalah penyelenggaraan telekomunikasi yang sifat, peruntukan, dan pengoperasiannya khusus;
16. Interkoneksi adalah keterhubungan antar jaringan telekomunikasi dari penyelenggara jaringan telekomunikasi yang berbeda.
17. Menteri adalah Menteri yang ruang lingkup tugas dan tanggung jawabnya di bidang telekomunikasi.

BAB II ASAS DAN TUJUAN

Pasal 2

Telekomunikasi diselenggarakan berdasarkan asas manfaat, adil dan merata, kepastian hukum, keamanan, kemitraan, etika, dan kepercayaan pada diri sendiri.

Pasal 3

Telekomunikasi diselenggarakan dengan tujuan untuk mendukung persatuan dan kesatuan bangsa, meningkatkan kesejahteraan dan kemakmuran rakyat secara adil dan merata, mendukung kehidupan ekonomi dan kegiatan pemerintahan, serta meningkatkan hubungan antarbangsa.

BAB III PEMBINAAN

Pasal 4

- (1) Telekomunikasi dikuasai oleh Negara dan pembinaannya dilakukan oleh Pemerintah.
- (2) Pembinaan telekomunikasi diarahkan untuk meningkatkan penyelenggaraan telekomunikasi yang meliputi penetapan kebijakan, pengaturan, pengawasan dan pengendalian.

- (3) Dalam penetapan kebijakan, pengaturan, pengawasan dan pengendalian di bidang telekomunikasi, sebagaimana dimaksud pada ayat (2), dilakukan secara menyeluruh dan terpadu dengan memperhatikan pemikiran dan pandangan yang berkembang dalam masyarakat serta perkembangan global.

Pasal 5

- (1) Dalam rangka pelaksanaan pembinaan telekomunikasi sebagaimana dimaksud dalam Pasal 4, Pemerintah melibatkan peran serta masyarakat.
- (2) Peran serta masyarakat sebagaimana dimaksud pada ayat (1), berupa penyampaian pemikiran dan pandangan yang berkembang dalam masyarakat mengenai arah pengembangan pertelekomunikasian dalam rangka penetapan kebijakan, pengaturan, pengendalian dan pengawasan di bidang telekomunikasi.
- (3) Pelaksanaan peran serta masyarakat sebagaimana dimaksud pada ayat (2), diselenggarakan oleh lembaga mandiri yang dibentuk untuk maksud tsb.
- (4) Lembaga sebagaimana dimaksud pada ayat (3) keanggotaannya terdiri dari asosiasi yang bergerak di bidang usaha telekomunikasi, asosiasi profesi telekomunikasi, asosiasi produsen peralatan telekomunikasi, asosiasi pengguna jaringan, dan jasa telekomunikasi serta masyarakat intelektual di bidang telekomunikasi.
- (5) Ketentuan mengenai tata cara peran serta masyarakat dan pembentukan lembaga sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 6

Menteri bertindak sebagai penanggung jawab administrasi telekomunikasi Indonesia.

BAB IV PENYELENGGARAAN

Bagian Pertama Umum

Pasal 7

- (1) Penyelenggaraan telekomunikasi meliputi :
 - a. penyelenggaraan jaringan telekomunikasi;
 - b. penyelenggaraan jasa telekomunikasi;
 - c. penyelenggaraan telekomunikasi khusus.
- (2) Dalam penyelenggaraan telekomunikasi, diperhatikan hal2 sbb.:
 - a. melindungi kepentingan dan keamanan negara;
 - b. mengantisipasi perkembangan teknologi dan tuntutan global;
 - c. dilakukan secara profesional dan dapat dipertanggungjawabkan;
 - d. peran serta masyarakat.

Bagian Kedua Penyelenggara

Pasal 8

- (1) Penyelenggaraan jaringan telekomunikasi dan atau penyelenggaraan jasa telekomunikasi sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf a dan huruf b, dapat dilakukan oleh

badan hukum yang didirikan untuk maksud tsb berdasarkan peraturan perundang-undangan yang berlaku, yaitu

- a. Badan Usaha Milik Negara (BUMN);
 - b. Badan Usaha Milik Daerah (BUMD);
 - c. Badan usaha swasta; atau
 - d. koperasi.
- (2) Penyelenggaraan telekomunikasi khusus sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf c, dapat dilakukan oleh :
- a. perseorangan;
 - b. instansi pemerintah;
 - c. badan hukum selain penyelenggara jaringan telekomunikasi dan atau penyelenggara jasa telekomunikasi.
- (3) Ketentuan mengenai penyelenggaraan telekomunikasi sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 9

- (1) Penyelenggara jaringan telekomunikasi sebagaimana dimaksud dalam Pasal 8 ayat (1) dapat menyelenggarakan jasa telekomunikasi.
- (2) Penyelenggara jasa telekomunikasi sebagaimana dimaksud dalam Pasal 8 ayat (1) dalam menyelenggarakan jasa telekomunikasi, menggunakan dan atau menyewa jaringan telekomunikasi milik penyelenggara jaringan telekomunikasi.
- (3) Penyelenggara telekomunikasi khusus sebagaimana dimaksud dalam Pasal 8 ayat (2), dapat menyelenggarakan telekomunikasi untuk :
 - a. keperluan sendiri;
 - b. keperluan pertahanan keamanan negara;
 - c. keperluan penyiaran.
- (4) Penyelenggaraan telekomunikasi khusus sebagaimana dimaksud pada ayat (3) huruf a, terdiri dari penyelenggaraan telekomunikasi untuk keperluan :
 - a. perseorangan;
 - b. instansi pemerintah;
 - c. dinas khusus;
 - d. badan hukum.
- (5) Ketentuan mengenai persyaratan penyelenggaraan telekomunikasi sebagaimana dimaksud pada ayat (1), ayat (2), ayat (3), dan ayat (4) diatur dengan Peraturan Pemerintah.

Bagian Ketiga Larangan Praktek Monopoli

Pasal 10

- (1) Dalam penyelenggaraan telekomunikasi dilarang melakukan kegiatan yang dapat mengakibatkan terjadinya praktek monopoli dan persaingan usaha tidak sehat di antara penyelenggara telekomunikasi.
- (2) Larangan sebagaimana dimaksud pada ayat (1) sesuai dengan peraturan perundang-undangan yang berlaku.

Bagian Keempat Perizinan

Pasal 11

- (1) Penyelenggaraan telekomunikasi sebagaimana dimaksud dalam Pasal 7 dapat diselenggarakan setelah mendapat izin dari Menteri.
- (2) Izin sebagaimana dimaksud pada ayat (1) diberikan dengan memperhatikan :
 - a. tata cara yang sederhana;
 - b. proses yang transparan, adil dan tidak diskriminatif; serta
 - c. penyelesaian dalam waktu yang singkat.
- (3) Ketentuan mengenai perizinan penyelenggaraan telekomunikasi sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dengan Peraturan pemerintah.

Bagian Kelima Hak dan Kewajiban Penyelenggara dan Masyarakat

Pasal 12

- (1) Dalam rangka pembangunan, pengoperasian, dan atau pemeliharaan jaringan telekomunikasi, penyelenggara telekomunikasi dapat memanfaatkan atau melintasi tanah negara dan atau bangunan yang dimiliki atau dikuasai Pemerintah.
- (2) Pemanfaatan atau pelintasan tanah negara dan atau bangunan sebagaimana dimaksud pada ayat (1), berlaku pula terhadap sungai, danau, atau laut, baik permukaan maupun dasar.
- (3) Pembangunan, pengoperasian dan atau pemeliharaan jaringan telekomunikasi sebagaimana dimaksud pada ayat (1), dilaksanakan setelah mendapatkan persetujuan dari instansi pemerintah yang bertanggung jawab dengan memperhatikan peraturan perundang-undangan yang berlaku.

Pasal 13

Penyelenggara telekomunikasi dapat memanfaatkan atau melintasi tanah dan atau bangunan milik perseorangan untuk tujuan pembangunan, pengoperasian, atau pemeliharaan jaringan telekomunikasi setelah terdapat persetujuan di antara para pihak.

Pasal 14

Setiap pengguna telekomunikasi mempunyai hak yang sama untuk menggunakan jaringan telekomunikasi dan jasa telekomunikasi dengan memperhatikan peraturan perundang-undangan yang berlaku.

Pasal 15

- (1) Atas kesalahan dan atau kelalaian penyelenggara telekomunikasi yang menimbulkan kerugian, maka pihak2 yang dirugikan berhak mengajukan tuntutan ganti rugi kepada penyelenggara telekomunikasi.
- (2) Penyelenggara telekomunikasi wajib memberikan ganti rugi sebagaimana dimaksud pada ayat (1), kecuali penyelenggara telekomunikasi dapat membuktikan bahwa kerugian tsb bukan diakibatkan oleh kesalahan dan atau kelalaiannya.
- (3) Ketentuan mengenai tata cara pengajuan dan penyelesaian ganti rugi sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 16

- (1) Setiap penyelenggara jaringan telekomunikasi dan atau penyelenggara jasa telekomunikasi wajib memberikan kontribusi dalam pelayanan universal.
- (2) Kontribusi pelayanan universal sebagaimana dimaksud pada ayat (1) berbentuk penyediaan sarana dan prasarana telekomunikasi dan atau kompensasi lain.
- (3) Ketentuan kontribusi pelayanan universal sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 17

Penyelenggara jaringan telekomunikasi dan atau penyelenggara jasa telekomunikasi wajib menyediakan pelayanan telekomunikasi berdasarkan prinsip:

- a. perlakuan yang sama dan pelayanan yang sebaik-baiknya bagi semua pengguna;
- b. peningkatan efisiensi dalam penyelenggaraan telekomunikasi; dan
- c. pemenuhan standar pelayanan serta standar penyediaan sarana dan prasarana.

Pasal 18

- (1) Penyelenggara jasa telekomunikasi wajib mencatat/merekam secara rinci pemakaian jasa telekomunikasi yang digunakan oleh pengguna telekomunikasi.
- (2) Apabila pengguna memerlukan catatan/rekaman pemakaian jasa telekomunikasi sebagaimana dimaksud pada ayat (1), penyelenggara telekomunikasi wajib memberikannya.
- (3) Ketentuan mengenai pencatatan/perekaman pemakaian jasa telekomunikasi sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 19

Penyelenggara jaringan telekomunikasi wajib menjamin kebebasan penggunanya memilih jaringan telekomunikasi lain untuk pemenuhan kebutuhan telekomunikasi.

Pasal 20

Setiap penyelenggara telekomunikasi wajib memberikan prioritas untuk pengiriman, penyaluran, dan penyampaian informasi penting yang menyangkut :

- a. keamanan negara;
- b. keselamatan jiwa manusia dan harta benda;
- c. bencana alam;
- d. marabahaya, dan atau
- e. wabah penyakit.

Pasal 21

Penyelenggara telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, keamanan, atau ketertiban umum.

Pasal 22

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.

Bagian Keenam Penomoran

Pasal 23

- (1) Dalam penyelenggaraan jaringan telekomunikasi dan jasa telekomunikasi ditetapkan dan digunakan sistem penomoran.
- (2) Sistem penomoran sebagaimana dimaksud pada ayat (1) ditetapkan oleh Menteri.

Pasal 24

Permintaan penomoran oleh penyelenggara jaringan telekomunikasi dan atau penyelenggara jasa telekomunikasi diberikan berdasarkan sistem penomoran sebagaimana dimaksud dalam Pasal 23.

Bagian Ketujuh Interkoneksi dan Biaya Hak Penyelenggaraan

Pasal 25

- (1) Setiap penyelenggara jaringan telekomunikasi berhak untuk mendapatkan interkoneksi dari penyelenggara jaringan telekomunikasi lainnya.
- (2) Setiap penyelenggara jaringan telekomunikasi wajib menyediakan interkoneksi apabila diminta oleh penyelenggara jaringan telekomunikasi lainnya.
- (3) Pelaksanaan hak dan kewajiban sebagaimana dimaksud pada ayat (1) dan ayat (2) dilakukan berdasarkan prinsip :
 - a. pemanfaatan sumber daya secara efisien;
 - b. keserasian sistem dan perangkat telekomunikasi;
 - c. peningkatan mutu pelayanan; dan
 - d. persaingan sehat yang tidak saling merugikan.
- (4) Ketentuan mengenai interkoneksi jaringan telekomunikasi, hak dan kewajiban sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 26

- (1) Setiap penyelenggara jaringan telekomunikasi dan atau penyelenggara jasa telekomunikasi wajib membayar biaya hak penyelenggaraan telekomunikasi yang diambil dari prosentase pendapatan.
- (2) Ketentuan mengenai biaya hak penyelenggaraan telekomunikasi sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.



**Bagian Kedelapan
T a r i f**

Pasal 27

Susunan tarif penyelenggaraan jaringan telekomunikasi dan atau tarif penyelenggaraan jasa telekomunikasi diatur dengan Peraturan Pemerintah.

Pasal 28

Besaran tarif penyelenggaraan jaringan telekomunikasi dan atau jasa telekomunikasi ditetapkan oleh penyelenggara jaringan telekomunikasi dan atau jasa telekomunikasi dengan berdasarkan formula yang ditetapkan oleh Pemerintah.

**Bagian Kesembilan
Telekomunikasi Khusus**

Pasal 29

- (1) Penyelenggaraan telekomunikasi khusus sebagaimana dimaksud dalam Pasal 9 ayat (3) huruf a dan huruf b, dilarang disambungkan ke jaringan penyelenggara telekomunikasi lainnya.
- (2) Penyelenggaraan telekomunikasi khusus sebagaimana dimaksud dalam Pasal 9 ayat (3) huruf c, dapat disambungkan ke jaringan penyelenggara telekomunikasi lainnya sepanjang digunakan untuk keperluan penyiaran.

Pasal 30

- (1) Dalam hal penyelenggara jaringan telekomunikasi dan atau penyelenggara jasa telekomunikasi belum dapat menyediakan akses di daerah tertentu, maka penyelenggara telekomunikasi khusus sebagaimana dimaksud dalam Pasal 9 ayat (3) huruf a, dapat menyelenggarakan jaringan telekomunikasi dan atau jasa telekomunikasi sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf a dan huruf b setelah mendapat izin Menteri.
- (2) Dalam hal penyelenggara jaringan telekomunikasi dan atau penyelenggara jasa telekomunikasi sudah dapat menyediakan akses di daerah sebagaimana dimaksud pada ayat (1), maka penyelenggara telekomunikasi khusus dimaksud tetap dapat melakukan penyelenggaraan jaringan telekomunikasi dan atau jasa telekomunikasi.
- (3) Syarat-syarat untuk mendapatkan izin sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 31

- (1) Dalam keadaan penyelenggara telekomunikasi khusus untuk keperluan pertahanan keamanan negara sebagaimana dimaksud dalam Pasal 9 ayat (3) huruf b belum atau tidak mampu mendukung kegiatannya, penyelenggara telekomunikasi khusus dimaksud dapat menggunakan atau memanfaatkan jaringan telekomunikasi yang dimiliki dan atau digunakan oleh penyelenggara telekomunikasi lainnya.
- (2) Ketentuan lebih lanjut sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

**Bagian Kesepuluh
Perangkat Telekomunikasi**

Spektrum Frekuensi Radio, dan Orbit Satelit

Pasal 32

- (1) Perangkat telekomunikasi yang diperdagangkan, dibuat, dirakit, dimasukkan dan atau digunakan di wilayah Negara Republik Indonesia wajib memperhatikan persyaratan teknis dan berdasarkan izin sesuai dengan peraturan perundang-undangan yang berlaku.
- (2) Ketentuan mengenai persyaratan teknis perangkat telekomunikasi sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 33

- (1) Penggunaan spektrum frekuensi radio dan orbit satelit wajib mendapatkan izin Pemerintah.
- (2) Penggunaan spektrum frekuensi radio dan orbit satelit harus sesuai dengan peruntukannya dan tidak saling mengganggu.
- (3) Pemerintah melakukan pengawasan dan pengendalian penggunaan spektrum frekuensi radio dan orbit satelit.
- (4) Ketentuan penggunaan spektrum frekuensi radio dan orbit satelit yang digunakan dalam penyelenggaraan telekomunikasi diatur dengan Peraturan Pemerintah.

Pasal 34

- (1) Pengguna spektrum frekuensi radio wajib membayar biaya penggunaan frekuensi, yang besarnya didasarkan atas penggunaan jenis dan lebar pita frekuensi.
- (2) Pengguna orbit satelit wajib membayar biaya hak penggunaan orbit satelit.
- (3) Ketentuan mengenai biaya sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 35

- (1) Perangkat telekomunikasi yang digunakan oleh kapal berbendera asing dari dan ke wilayah perairan Indonesia dan atau yang dioperasikan di wilayah perairan Indonesia, tidak diwajibkan memenuhi persyaratan teknis sebagaimana dimaksud dalam Pasal 32.
- (2) Spektrum frekuensi radio dilarang digunakan oleh kapal berbendera asing yang berada di wilayah perairan Indonesia di luar peruntukannya, kecuali :
 - a. untuk kepentingan keamanan negara, keselamatan jiwa manusia dan harta benda, bencana alam, keadaan marabahaya, wabah, navigasi, dan keamanan lalu lintas pelayaran; atau
 - b. disambungkan ke jaringan telekomunikasi yang dioperasikan oleh penyelenggara telekomunikasi; atau
 - c. merupakan bagian dari sistem komunikasi satelit yang penggunaannya sesuai dengan ketentuan yang berlaku dalam penyelenggaraan telekomunikasi dinas bergerak pelayaran.
- (3) Ketentuan mengenai penggunaan spektrum frekuensi radio sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 36

- (1) Perangkat telekomunikasi yang digunakan oleh pesawat udara sipil asing dari dan ke wilayah udara Indonesia tidak diwajibkan memenuhi persyaratan teknis sebagaimana dimaksud dalam Pasal 32.
- (2) Spektrum frekuensi radio dilarang digunakan oleh pesawat udara sipil asing dari dan ke wilayah udara Indonesia di luar peruntukannya, kecuali :

- a. untuk kepentingan keamanan negara, keselamatan jiwa manusia dan harta benda, bencana alam, keadaan marabahaya, wabah, navigasi, dan keselamatan lalu lintas penerbangan, atau
 - b. disambungkan ke jaringan telekomunikasi yang dioperasikan oleh penyelenggara telekomunikasi, atau
 - c. merupakan bagian dari sistem komunikasi satelit yang penggunaannya sesuai dengan ketentuan yang berlaku dalam penyelenggaraan telekomunikasi dinas bergerak penerbangan.
- (3) Ketentuan mengenai penggunaan spektrum frekuensi radio sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 37

Pemberian izin penggunaan perangkat telekomunikasi yang menggunakan spektrum frekuensi radio untuk perwakilan diplomatik di Indonesia dilakukan dengan memperhatikan asas timbal balik.

Bagian Kesebelas Pengamanan Telekomunikasi

Pasal 38

Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi.

Pasal 39

- (1) Penyelenggara telekomunikasi wajib melakukan pengamanan dan perlindungan terhadap instalasi dalam jaringan telekomunikasi yang digunakan untuk penyelenggaraan telekomunikasi.
- (2) Ketentuan pengamanan dan perlindungan sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 40

Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.

Pasal 41

Dalam rangka pembuktian kebenaran pemakaian fasilitas telekomunikasi atas permintaan pengguna jasa telekomunikasi, penyelenggara jasa telekomunikasi wajib melakukan perekaman pemakaian fasilitas telekomunikasi yang digunakan oleh pengguna jasa telekomunikasi dan dapat melakukan perekaman informasi sesuai dengan peraturan perundang-undangan yang berlaku.

Pasal 42

- (1) Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya.

- (2) Untuk keperluan proses peradilan pidana, penyelenggara jasa telekomunikasi dapat merekam informasi yang dikirim dan atau diterima oleh penyelenggara jasa telekomunikasi serta dapat memberikan informasi yang diperlukan atas :
 - a. permintaan tertulis Jaksa Agung dan atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu.
 - b. permintaan penyidik untuk tindak pidana tertentu sesuai dengan Undang-undang yang berlaku.
- (3) Ketentuan mengenai tata cara permintaan dan pemberian rekaman informasi sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 43

Pemberian rekaman informasi oleh penyelenggara jasa telekomunikasi kepada pengguna jasa telekomunikasi sebagaimana dimaksud dalam Pasal 41 dan untuk kepentingan proses peradilan pidana sebagaimana dimaksud dalam Pasal 42 ayat (2), tidak merupakan pelanggaran Pasal 40.

BAB V PENYIDIKAN

Pasal 44

- (1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, juga Pejabat Pegawai Negeri Sipil tertentu di lingkungan Departemen yang lingkup tugas dan tanggung jawabnya di bidang telekomunikasi, diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang telekomunikasi.
- (2) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang :
 - a. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana di bidang telekomunikasi.
 - b. melakukan pemeriksaan terhadap orang dan atau badan hukum yang diduga melakukan tindak pidana di bidang telekomunikasi.
 - c. menghentikan penggunaan alat dan atau perangkat telekomunikasi yang menyimpang dari ketentuan yang berlaku.
 - d. memanggil orang untuk didengar dan diperiksa sebagai saksi atau tersangka
 - e. melakukan pemeriksaan alat dan atau perangkat telekomunikasi yang diduga digunakan atau diduga berkaitan dengan tindak pidana di bidang telekomunikasi.
 - f. menggebedah tempat yang diduga digunakan untuk melakukan tindak pidana di bidang telekomunikasi.
 - g. menyegel dan atau menyita alat dan atau perangkat telekomunikasi yang digunakan atau yang diduga berkaitan dengan tindak pidana di bidang telekomunikasi.
 - h. meminta bantuan ahli dalam rangka pelaksanaan tugas penyidikan tindak pidana di bidang telekomunikasi, dan
 - i. mengadakan penghentian penyidikan.
- (3) Kewenangan penyidikan sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan Undang-undang Hukum Acara Pidana.

**BAB VI
SANKSI ADMINISTRASI**

Pasal 45

Barang siapa melanggar ketentuan Pasal 16 ayat (1), Pasal 18 ayat (2), Pasal 19, Pasal 21, Pasal 25 ayat (2), Pasal 26 ayat (1), Pasal 29 ayat (1), Pasal 29 ayat (2), Pasal 33 ayat (1), Pasal 33 ayat (2), Pasal 34 ayat (1), atau Pasal 34 ayat (2) dikenai sanksi administrasi.

Pasal 46

- (1) Sanksi administrasi sebagaimana dimaksud dalam Pasal 45 berupa pencabutan izin.
- (2) Pencabutan izin sebagaimana dimaksud pada ayat (1) dilakukan setelah diberi peringatan tertulis.

**BAB VII
KETENTUAN PIDANA**

Pasal 47

Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1), dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

Pasal 48

Penyelenggara jaringan telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 19 dipidana dengan pidana penjara paling lama 1 (satu) tahun dan atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).

Pasal 49

Penyelenggara telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 20, dipidana dengan pidana penjara paling lama 2 (dua) tahun dan atau denda paling banyak Rp 200.000.000,00 (dua ratus juta rupiah).

Pasal 50

Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

Pasal 51

Penyelenggara telekomunikasi khusus yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 29 ayat (1) atau Pasal 29 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan atau denda paling banyak Rp 400.000.000,00 (empat ratus juta rupiah).

Pasal 52

Barang siapa memperdagangkan, membuat, merakit, memasukkan atau menggunakan perangkat telekomunikasi di wilayah Negara Republik Indonesia yang tidak sesuai dengan persyaratan teknis sebagaimana dimaksud dalam Pasal 32 ayat (1) Dipidana dengan pidana penjara paling lama 1 (satu) tahun dan atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).

Pasal 53

- (1) Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 33 ayat (1) atau Pasal 33 ayat (2), dipidana dengan pidana penjara paling lama 4 (empat) tahun dan atau denda paling banyak Rp 400.000.000,00 (empat ratus juta rupiah).
- (2) Apabila tindak pidana sebagaimana dimaksud pada ayat (1) mengakibatkan matinya seseorang, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun.

Pasal 54

Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 35 ayat (2) atau Pasal 36 ayat (2), dipidana dengan pidana penjara paling lama 2 (dua) tahun dan atau denda paling banyak Rp. 200.000.000,00 (dua ratus juta rupiah).

Pasal 55

Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 38, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

Pasal 56

Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun.

Pasal 57

Penyelenggara jasa telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 42 ayat (1), dipidana dengan pidana penjara paling lama 2 (dua) tahun dan atau denda paling banyak Rp 200.000.000,00 (dua ratus juta rupiah).

Pasal 58

Alat dan perangkat telekomunikasi yang digunakan dalam tindak pidana sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 52 atau Pasal 56 dirampas untuk negara dan atau dimusnahkan sesuai dengan peraturan perundang-undangan yang berlaku.

Pasal 59

Perbuatan sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51, Pasal 52, Pasal 53, Pasal 54, Pasal 55, Pasal 56, dan Pasal 57 adalah kejahatan.

**BAB VIII
KETENTUAN PERALIHAN**



Pasal 60

Pada saat berlakunya Undang-undang ini, penyelenggara telekomunikasi sebagaimana dimaksud dalam Undang-undang Nomor 3 Tahun 1989 tentang Telekomunikasi, tetap dapat menjalankan kegiatannya dengan ketentuan dalam waktu selambat-lambatnya 1 (satu) tahun sejak Undang-undang ini dinyatakan berlaku wajib menyesuaikan dengan Undang-undang ini.

Pasal 61

- (1) Dengan berlakunya Undang-undang ini, Hak-hak tertentu yang telah diberikan oleh Pemerintah kepada Badan Penyelenggara untuk jangka waktu tertentu berdasarkan Undang-undang Nomor 3 Tahun 1989 masih berlaku.
- (2) Jangka waktu hak tertentu sebagaimana dimaksud pada ayat (1), dapat dipersingkat sesuai dengan kesepakatan antara Pemerintah dan Badan Penyelenggara.

Pasal 62

Pada saat Undang-undang ini berlaku semua peraturan pelaksanaan Undang-undang Nomor 3 Tahun 1989 tentang Telekomunikasi (Lembaran Negara Tahun 1989 Nomor 11, Tambahan Lembaran Negara Nomor 3391) masih tetap berlaku sepanjang tidak bertentangan dan atau belum diganti dengan peraturan baru berdasarkan Undang-undang ini.

**BAB IX
KETENTUAN PENUTUP**

Pasal 63

Dengan berlakunya Undang-undang ini, Undang-undang Nomor 3 Tahun 1989 tentang Telekomunikasi dinyatakan tidak berlaku.

Pasal 64

Undang-undang ini mulai berlaku 1 (satu) tahun terhitung sejak tanggal diundangkan.
Agar setiap orang mengetahuinya, memerintahkan pengundangan Undang-undang ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Disahkan di Jakarta
pada tanggal 8 September 1999
PRESIDEN REPUBLIK INDONESIA
ttd.
BACHARUDDIN JUSUF HABIBIE

Diundangkan di Jakarta
pada tanggal 8 September 1999
MENTERI NEGARA SEKRETARIS NEGARA
REPUBLIK INDONESIA
ttd.
M U L A D I