BAB IV

ANALISIS HUKUM MENGENAI PENCURIAN DANA NASABAH BANK MELALUI INTERNET DIHUBUNGKAN DENGAN PASAL 362 KITAB UNDANG-UNDANG HUKUM PIDANA (KUHP)

A. Efektivitas Mengenai Pencurian Dana Nasabah Bank Melalui Internet Dihubungkan Dengan Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP)

Kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dengan internet dalam segala bidang seperti *e-banking, e-commerce, e-goverment,* dan lain-lain telah menjadi sesuatu yang lumrah, bahkan apabila masyarakat terutama yang hidup di kota besar tidak bersentuhan dengan teknologi informasi dapat dipandang terbelakang. Internet telah menciptakan dunia baru yang dinamakan *cyberspace* yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realita baru berbentuk virtual (tidak langsung dan tidak nyata).

Kecanggihan teknologi komputer telah memberikan kemudahan-kemudahan, terutama dalam membantu pekerjaan manusia. Perkembangan teknologi komputer selain itu juga menyebabkan munculnya jenis kejahatan-kejahatan baru, yaitu dengan memanfaatkan komputer sebagai modus operandi. Perkembangan teknologi internet, menyebabkan munculnya kejahatan baru yang disebut dengan *cybercrime*. Contoh Kejahatan *cybercrime* di Indonesia antara lain seperti pencurian kartu kredit, menyadap transmisi data orang lain, dan lain-lain. Pelaku dalam melakukan kejahatan biasanya

menggunakan *e-mail*, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program komputer, sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materiil. Delik formil yaitu perbuatan seseorang yang memasuki komputer orang lain tanpa izin, sedangkan delik materiil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain[45].

Mengacu pada kasus-kasus *cyber crime* di antaranya dalam bidang perbankan salah satunya yaitu modus pencurian dana nasabah bank melalui internet (*carding database*) dalam prakteknya akan sangat mempengaruhi stabilitas dan rasa aman bagi nasabah bank.

Ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP) banyak yang sudah tidak sesuai lagi dengan perkembangan tindak pidana yang ada saat ini, hal ini dikarenakan masyarakat bersifat dinamis, oleh karena itu *ius constitutum* (hukum positif atau hukum yang berlaku sekarang) tidak sama dengan *ius constituendum* (Hukum yang berlaku di masa akan datang).

Kitab Undang-Undang Hukum Pidana (KUHP) tidak mengatur tentang *cybercrime,* hal ini dapat dipahami karena pada saat Kitab Undang-Undang Hukum Pidana (KUHP) dibuat belum dikenal tindak pidana di bidang *cyber*. kasus pencurian dana nasabah bank melalui internet semakin banyak terjadi antara lain disebabkan karena banyaknya nasabah yang memanfaatkan fasilitas *internet banking.*

---

[45] Petrus Rainhard Golose, *Makalah Pengamanan Aplikasi Komputer Dalam Sistem Perbankan dan Aspek Penyelidikan dan Tindak Pidana*, http://buletin.melsa.net , Diakses Pada Tanggal 18 Juni 2010, Pukul 15.00 WIB

Indonesia adalah negara hukum, di mana salah satu asas yang penting dalam negara hukum adalah asas legalitas yang menyatakan bahwa setiap tindakan atau kebijakan pemerintah harus berdasarkan peraturan perundang-undangan. Salah satu asas terpenting dalam negara hukum adalah asas legalitas antara lain didasarkan pada ketentuan dalam Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP) yang berbunyi :

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

Mengenai ketiadaan undang-undang yang secara khusus mengatur *cybercrime* berdasarkan asas legalitas dalam ketentuan Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP) maka pelaku *cybercrime* khususnya *carding database* di Indonesia tidak dapat dijerat oleh hukum, akan tetapi *cybercrime* tetaplah sebuah kejahatan, oleh karena itu, harus dikenakan sebuah ketentuan hukum yang pasti dan tegas untuk melindungi kepentingan dan ketertiban umum. Apabila ditinjau dari substansi tindak pidana *cybercrime*, maka pelaku *carding database* dapat dijerat dengan rumusan Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP).

Saat ini kejahatan-kejahatan yang dilakukan di dunia maya sudah diatur dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Namun demikian, ada beberapa kejahatan yang tidak diatur secara khusus seperti pencurian dana nasabah bank melalui internet (*carding database*). Pada Pasal 32 ayat 2 Undang-Undang Nomor 11 Tahun

2008 Tentang Informasi dan Transaksi Elektronik yang berbunyi diatur mengenai perbuatan-perbuatan yang dilarang, antara lain sebagai berikut :

> “ Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak. ”

Pasal 32 ayat 2 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengandung unsur-unsur, baik unsur subjektif maupun unsur objektif, yaitu :

Unsur subjektif : 1. dengan sengaja

2. secara melawan hukum atau tanpa hak

Unsur Objektif : 1. setiap orang

2.memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak.

Pasal 32 ayat 2 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tidak dapat diterapkan untuk kasus *carding database*. Hal tersebut dikarenakan unsur-unsur dalam pasal tersebut tidak terpenuhi secara khusus sebagaimana sebuah tindak pidana pencurian dana nasabah bank melalui internet (*carding database*).

Sekalipun pada saat ini belum ada ketentuan yang mengatur tindak pidana pencurian dana nasabah bank melalui internet (*carding database*)secara khusus, bukan berarti tindak pidana termaksud dapat lolos dari hukum, karena masih ada ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) yaitu Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) dapat diterapkan terhadap kejahatan tersebut.

Pencurian dana nasabah bank melalui internet terjadi pada bulan Desember 2008 di Purwokerto. Seorang nasabah bank Mandiri pengguna fasilitas *internet banking*, kehilangan uang sebesar Rp. 38 Juta yang dicuri oleh seseorang yang menggunakan teknologi internet. Korban yang bernama Johannes mengatakan telah kehilangan uang Rp 38 Juta yang diambil hampir tiap hari oleh pencuri tersebut. Johannes sebelumnya menerima sebuah *e-mail* dari situs internet banking mandiri yang isinya diharuskan mengaktifkan kembali *user ID* dan PIN yang sebelumnya telah dinonaktifkan.

Carder mengaku sebagai pihak bank, sehingga *carder* dapat meyakinkan korbannya sampai 5% dari penerima *e-mail* untuk mengikuti perintahnya. Pada isi *e-mail*, *carder* memberitahukan tentang perlunya verifikasi *user ID dan PIN* dengan cara mengklik *link* URL pada *e-mail* dan mengirimkannya dengan alasan agar *account*-nya dapat dipergunakan kembali dan ter-*update*, setelah *carder* berhasil mendapatkan *user ID dan PIN*, lalu *carder* dapat menggunakannya untuk berbelanja atau meminjam identitas kita.

Tindak pidana pencurian diatur dalam Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) yang berbunyi:

> ”Barangsiapa mengambil barang sesuatu yang seluruhnya atau sebagian kepunyaan orang lain dengan maksud untuk dimiliki secara melawan hukum diancam karena pencurian dengan pidana penjara paling lama lima tahun atau denda paling banyak enam puluh rupiah.”

Unsur-unsur dalam Pasal 362 Kitab Undang-Undang Hukum Pidana tersebut terdiri dari:

1. Mengambil barang, artinya perbuatan mengambil barang, kata mengambil dalam arti sempit terbatas pada menggerakan tangan dan jari-jari, memegang barangnya, dan mengalihkanya ke tempat orang lain.

   Barang yang diambil, artinya merugikan kekayaan korban, maka barang yang harus diambil harus berharga, harga ini tidak harus bersifat ekonomis.
2. Tujuan memiliki barangnya dengan melanggar hukum, artinya tindak pidana pencurian dalam bentuknya yang pokok berupa perbuatan mengambil suatu benda yang sebagian atau seluruhnya adalah kepunyaan orang lain.

Pelaku pencurian dana nasabah bank melalui internet khususnya *carding database* di Indonesia tidak dapat dijerat oleh pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) dikarenakan Kitab Undang-Undang

Hukum Pidana (KUHP) tidak mengatur tentang kejahatan tersebut, akan tetapi kejahatan mengenai pencurian dana nasabah bank melalui internet tetaplah sebuah kejahatan, oleh karena itu, harus dikenakan sebuah ketentuan hukum yang pasti dan tegas untuk melindungi kepentingan dan ketertiban umum.

Ketentuan tidak adanya yang mengatur suatu tindak pidana tidak boleh menyebabkan hakim menolak perkara tersebut, hal ini didasarkan pada Pasal 10 Ayat (1) Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman yang berbunyi :

> ” Pengadilan dilarang menolak untuk memeriksa, mengadili, dan memutus suatu perkara yang diajukan dengan dalih bahwa hukum tidak ada atau kurang jelas, melainkan wajib untuk memeriksa dan mengadilinya. ”

Berdasarkan ketentuan dalam Pasal 10 Ayat (1) Undang-Undang Nomor 48 Tahun 2009 Tentang Pokok-Pokok Kekuasaan Kehakiman maka pengadilan tidak boleh menolak suatu perkara hanya karena belum ada aturan mengenai perkara yang diajukan ke pengadilan, termasuk pencurian dana nasabah bank melalui internet.

Pelaku kejahatan tidak terlepas dari jeratan hukum walaupun belum disertai dengan adanya ketentuan perundang undangan *cybercrime*, karena *law is a tool of social engginering* yang menyatakan bahwa hukum adalah alat untuk merekayasa masyarakat. Pemerintah dalam hal ini aparat penegak hukum dituntut agar dapat membentuk hukum sesuai dengan perkembangan masyarakat, hal ini sesuai dengan ketentuan Pasal 2 ayat (1) dan (2) Undang-

Undang Nomor 48 Tahun 2009 Tentang Pokok-Pokok Kekuasaan Kehakiman, yaitu :

> ”Peradilan dilakukan "DEMI KEADILAN BERDASARKAN KETUHANAN YANG MAHA ESA".
>
> “Peradilan negara menerapkan dan menegakkan hukum dan keadilanberdasarkan Pancasila.”

Ketentuan Pasal 2 ayat (1) dan (2) Undang-Undang Nomor 48 Tahun 2009 Tentang Pokok-Pokok Kekuasaan Kehakiman Dalam hal ini, apabila belum ada aturan secara khusus mengenai pencurian dana nasabah bank melalui internet, hakim sebagai penegak hukum dan keadilan wajib menggali, mengikuti, dan memahami nilai-nilai yang hidup dalam masyarakat berdasarkan ketuhanan dan Pancasila[46].

Oleh karena itu, apabila belum ada aturan secara khusus mengenai pencurian dana nasabah bank melalui internet, hakim sebagai penegak hukum dan keadilan wajib menggali, mengikuti, dan memahami nilai-nilai yang hidup dalam masyarakat[47]. Dalam menghadapi kasus-kasus *carding database* , hakim dapat menggunakan penafsiran hukum.

Dalam menyelesaikan kasus pencurian dana nasabah bank melalui internet, hakim menggunakan penafsiran ekstensif yaitu penafsiran yang memperluas dengan cara melampaui batas-batas yang ditentukan dalam

---

[46] Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sapta Arta Jaya, Jakarta, 1996, Hlm. 112

[47] Andi Hamzah, *Op Cit*., hlm 112

penafsiran gramatikal. dalam penafsiran ekstensif arti kata pencurian dalam Pasal 362 KUHP di perluas, tidak hanya mencangkup pencurian secara konvensional tetapi mencangkup juga pencurian dengan menggunakan media, dalam hal ini internet. kasus pencurian dana nasabah bank melalui internet, benda yang dicuri yaitu benda tidak berwujud tetapi benda tersebut memiliki nilai ekonomis.

Berdasarkan rumusan unsur-unsur diatas maka perbuatan yang dilakukan oleh *carder* memenuhi unsur obyektif dan unsur subjektif sebagaimana yang terdapat dalam Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) mengenai tindak pidana pencurian. Dengan demikian, Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) mengenai tindak pidana pencurian dapat diterapkan terhadap tindak pidana pencurian dana nasabah bank melalui internet (*carding database*).

B. Tindakan Hukum yang dapat Dilakukan Terhadap Pelaku Tindak Pidana pencurian dana nasabah bank melalui internet

Teknologi komputer berkembang terus-menerus, disamping hasilnya dapat dimanfaatkan untuk meningkatkan efisiensi dan kehematan (ekonomis) bagi kehidupan, juga sering menimbulkan ide-ide negatif.

Masalah yang muncul saat ini, yang dihadapi oleh aparat penegak hukum adalah bagaimana menjaring pelaku *cybercrime* dikaitkan dengan ketentuan hukum pidana yang berlaku. Aparat penegak hukum dihadapkan

pada kesulitan untuk menentukan kualifikasi kejahatan mengingat sulitnya menemukan alat bukti.

Masalah yang dihadapi oleh penyidik dalam melakukan penyelidikan dan pengumpulan barang bukti terhadap kasus kejahatan *cyber*[48] :

1. kesulitan dalam mendeteksi kejahatan komputer. Hal ini disebabkan karena :
    a. Sistem keamanan dari komputer itu sendiri belum memadai
    b. Adanya keengganan dari pemilik komputer untuk melaporkan setiap timbulnya peristiwa penyalahgunaan komputer
    c. Masyarakat belum begitu berperan di dalam upaya mendeteksi kejahatan komputer
2. Barang bukti mudah dihilangkan/dimusnahkan/dirusak/dihapus
3. Penyidikan dapat terputus/tertunda oleh sistem yang macet
4. Rekaman pada sistem dapat dimodifikasikan sehingga barang bukti dapat dirubah
5. Komputer dapat melaksanakan perintah siapa saja, sehingga sulit dilacak siapa pelaku yang sebenarnya.

Sistem pembuktian di era teknologi informasi saat ini menghadapi tantangan besar yang memerlukan penanganan serius, khususnya dalam kaitannya dengan upaya pemberantasan *cybercrime*. Hal ini muncul karena

[48] Al Wisnubroto, *Kebijakan hukum pidana dalam penanggulangan penyalahgunaan komputer*, Yogyakarta : Universitas Widyatama, 1999, hlm 256-257

bagi sebagian pihak jenis-jenis alat bukti yang selama ini dipakai untuk menjerat pelaku tindak pidana tidak mampu lagi dipergunakan untuk menjerat pelaku kejahatan di dunia maya.

Masalah pembuktian dalam tindak pidana pencurian dana nasabah bank melalui internet berkaitan erat dengan kondisi Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang belum direvisi. Sistem peradilan pidana memandang keempat aparatur penegak hukum yaitu kepolisian, kejaksaan, pengadilan dan lembaga pemasyarakatan sebagai institusi pelaksana peraturan perundang-undangan yang berlaku sehingga keempat aparatur tersebut merupakan bagian yang tidak dapat terpisahkan dari sistem penegak hukum.[49]

Salah satu tugas dari hukum acara pidana adalah mencari dan mendapatkan kebenaran materil yaitu kebenaran yang sesungguh-sungguhnya. Tugas itu tidaklah mudah bagi penyidik, penuntut umum dan hakim sehingga antara aparatur penegak hukum ini harus bekerja sama satu sama lainnya. Hukum acara pidana hanya dapat menunjukkan jalan untuk mencari sebanyak mungkin persesuaian antara keyakinan hakim dengan kehadiran alat bukti dan barang bukti.

Pembuktian merupakan masalah yang memegang peranan dalam proses pemeriksaan sidang pengadilan. Melalui pembuktian ditentukan nasib terdakwa.[50] Oleh karena itu, hakim harus berhati-hati, cermat, teliti dalam

---

[49] Andi Hamzah, *Op Cit*., hlm 267

[50] M Yahya harahap, *Pembahasan Permasalahan dan penerapan KUHAP*, Jakarta:Sinar Grafika, 2000, hlm 252

menilai dan mempertimbangkan nilai pembuktian. Hakim harus meneliti sampai sejauh mana batas minimal kekuatan pembuktian dari setiap alat bukti yang disebut dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Mengenai alat bukti di pengadilan diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yaitu terdiri dari[51] :

1. Keterangan saksi, dalam Pasal 185 ayat 1 KUHAP disebutkan bahwa keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan dalam persidangan. Berdasarkan penjelasan KUHAP dinyatakan bahwa dalam keterangan saksi tidak termasuk keterangan yang diperoleh dari orang lain. Pasal 1 angka 27 KUHAP menyatakan bahwa keterangan saksi adalah salah satu alat bukti dalam perkara pidana berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia lihat sendiri dan dialami sendiri dengan menyebut alasan dari pengetahuannya itu.
2. Keterangan ahli, Pasal 186 KUHAP menyatakan bahwa keterangan seorang ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Selanjutnya penjelasan Pasal 186 KUHAP menyatakan bahwa keterangan ahli ini dapat juga telah diberikan pada waktu pemeriksaan oleh penyidik atau penuntut umum yang dituangkan dalam suatu bentuk laporan dan dibuat dengan mengingat sumpah pada waktu ia menerima jabatan atau pekerjaan. Menurut teori

[51] Dikdik M. Arief Mansur dan Alisataris Gultom, *Op Cit*., hlm. 101

hukum pidana yang dimaksud dengan keterangan ahli adalah keterangan yang diberikan seseorang berdasarkan ilmu dan pengetahuan yang dikuasainya.

3. Surat, sebagai alat bukti diatur dalam Pasal 187 KUHAP. Menurut komentar KUHAP yang disusun oleh M. Karjadi dan R. Soesilo, Pasal 187 membedakan atas empat macam surat, yaitu :
   a. Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, didengar, dilihat atau dialaminya sendiri, disertai dengan alasan tentang keterangan itu;
   b. Surat yang dibuat menurut peraturan undang-undang atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukan bagi pembuktian sesuatu hal atau keadaan;
   c. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai suatu hal atau keadaan yang diminta secara resmi dari padanya; dan
   d. Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.
4. Petunjuk, Pasal 188 ayat 1 KUHAP memberi definisi petunjuk sebagai perbuatan, kejadian atau keadaan, yang karena penyesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya. Selanjutnya Pasal 188

ayat 3 KUHAP dinyatakan bahwa penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan arif dan bijaksana, setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan keseksamaan berdasarkan hati nuraninya.

5. Keterangan terdakwa, menurut Pasal 189 ayat 1 KUHAP adalah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri dan alami sendiri. Keterangan terdakwa tidak perlu sama dengan pengakuan, karena pengakuan sebagai alat bukti mempunyai syarat, yaitu :
   a. Mengaku ia yang melakukan delik yang didakwakan; dan
   b. Mengaku ia bersalah

Kesulitan yang dihadapi oleh aparat penegak hukum dapat diatasi dengan menambahkan data elektronik dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) sebagai alat bukti yang sah. Perbaikan pada Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) merupakan salah satu cara untuk menghadapi *cybercrime*. Sebagaimana yang dikemukakan oleh pakar teknologi Onno W Purbo yaitu [52] :

> “Sudah saatnya pemerintah memperbaiki Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dengan menempatkan data elektronik sebagai alat bukti yang sah di pengadilan. Kitab Undang-Undang Hukum Acara

[52] www.hukumonline.com, diakses pada tanggal 21 Juli 2010, pukul 21.00 WIB

Pidana (KUHAP) harus mengakui data elektronik sebagai alat bukti yang sah untuk mengungkap kasus kejahatan *cyber*."

Dalam pasal 44 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik telah diatur mengenai alat bukti dalam penyidikan, penuntutan dan pemeriksaan di sidang pengadilan yang berbunyi :

> "Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang - undang ini adalah sebagai berikut:
>
> a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang - undangan; dan
> b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)."

Dengan diaturnya alat bukti dalam Pasal 44 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik maka pembuktian bukan lagi menjadi suatu kendala dalam menangani kajahatan-kejahatan dalam dunia maya. Pada Pasal 5 ayat (1) Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik dijelaskan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Pasal 5 ayat (2) Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik dijelaskan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana

dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Menurut Ahmad M Ramli terdapat 3 pendekatan untuk mempertahankan keamanan di *cyberspace* yaitu [53] :

1. Pendekatan Teknologi
2. Pendekatan Sosial,Budaya-Etika
3. Pendekatan Hukum

Berbicara mengenai kejahatan (*crime*), tidak dapat dilepaskan dari 5 faktor yang saling bekaitan erat yaitu pelaku kejahatan, modus kejahatan, korban kejahatan, reaksi sosial atas kejahatan dan hukum. Hukum menjadi instrumen penting dalam pencegahan dan penanggulangan kejahatan.

Kejahatan yang kompleks seperti saat ini terlambat diantisipasi oleh Polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya. Untuk itu, pencegahan kejahatan tidak selalu harus menggunakan hukum pidana, agar penanggulangan *cybercrime* khususnya *carding database* ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Dalam konteks *cybercrime* khususnya *carding database* ini erat hubungannya dengan teknologi, khususnya teknologi komputer dan telekomunikasi sehingga pencegahan *carding database* dapat digunakan

[53] Ahmad M Ramli, *Op Cit.,* Hlm 3

melalui saluran teknologi atau disebut juga *techno-prevention*. Pendekatan teknologi ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau kultural ini perlu dilakukan untuk mebangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cybercrime* khususnya *carding database* dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan. Pentingnya pendekatan budaya ini, khususnya upaya mengembangkan kode etik dan perilaku.[54]

Ketidaksiapan hukum dan polri dalam menanggulangi *carding database* ini menyebabkan pencegahan dengan menggunakan teknologi dan budaya menjadi alat yang ampuh. Kejahatan *carding database* ini dapat dicegah oleh penerima *e-mail* dengan cara sebagai berikut[55] :

1. Tidak merespon terhadap permintaan informasi pribadi lewat *e-mail* atau *pop-up window*. Situs-situs resmi tidak akan bertanya tentang *password*, nomor kartu kredit, atau informasi pribadi lainnya dalam bentuk *e-mail*.
2. Kunjungi situs pada *link* yang ada dengan menulis URL pada *address bar browser*, jangan percaya dengan cara meng*klik* langsung pada *link* tersebut. Apabila menganggap bahwa *e-mail* dari perusahaan kartu kredit, bank atau *online payment service*, atau situs web tersebut bukan asli, jangan mengikuti *link* yang

[54] Agus Raharjo, *Op Cit*., Hlm 246
[55] http://buletin.melsa.net, idjan1001carding6/html, diekses pada tanggal 13 Juni 2010, pukul 15.00 WIB

menunjukkan ke situsnya dari *e-mail* tersebut. *Link* tersebut dapat berupa *link* palsu, dimana tertulis resmi, tetapi mengarah ke situs web yang palsu.

3. Cek *security* untuk memastikan situs web tersebut memakai enkripsi. Sebelum memasukan informasi, cek terlebih dahulu apakah situs tersebut memakai enkripsi atau tidak. Nasabah atau *netter* dapat memastikan situs tersebut memakai enkripsi bila situs tersebut alamatnya berawalan https:// dan bukan http://. Pada *browser*, akan terlihat tanda aman pada bagian bawah *browser*, di status bar , yaitu adanya sebuah tanda gembok yang terkunci. Tanda gembok tersebut menandakan bahwa situs itu memakai enkripsi untuk melindungi informasi berharga seperti nomor kartu kredit dan sebagainya.
4. Secara rutin mengecek kartu kredit dan pernyataan bank.
5. Laporkan tindakan kriminal dari tersangka ke instansi yang berwenang.

Pada upaya penanggulangan *carding database*, tidak hanya pendekatan penal dan non penal yang diperlukan, mengingat sifat *cybercrime* yang dapat dilakukan oleh orang dengan melalui batas negara maka perlu dilakukan kerjasama dengan negara lain. Bentuk kerja sama ini dapat berupa kerja sama ekstradisi maupun harmonisasi hukum pidana substantif. Salah satu lagi agar penanggulangan *cybercrime* khususnya *carding database* ini dapat dilakukan dengan baik, maka perlu dilakukan kerja sama dengan *Internet Service Provider* (ISP) atau penyedia jasa internet. Meskipun *Internet*

Service Provider (ISP) hanya berkaitan dengan layanan sambungan atau akses internet, tetapi *Internet Service Provider* (ISP) memiliki catatan mengenai keluar atau masuknya seorang pengakses, sehingga dapat diidentifikasikan siapa yang melakukan kejahatan dengan melihat *log file* yang ada.

Perbuatan yang dilakukan oleh pelaku tindak pidana pencurian dana nasabah bank melalui internet telah memenuhi unsur obyektif dan unsur subjektif dari Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) mengenai tindak pidana pencurian serta didukung oleh alat bukti yang sah sebagaimana yang diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Pasal 44 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Berdasarkan kasus-kasus *carding database* yang telah dilakukan oleh para *carder* dan merugikan korban secara materil dan imateril maka pelaku pencurian melalui internet atau *carder* dapat dilakukan dengan cara pendekatan secara represif (penindakan).

Korban dapat melaporkan tindak pidana pencurian dana nasabah bank melalui internet (*carding database*) melalui pengiriman *e-mail* yang terjadi kepada pihak kepolisian untuk diproses sesuai dengan prosedur yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Selanjutnya dilakukan proses penyerahan berkas perkara disertai penyerahan tersangka dan barang bukti kepada Jaksa Penuntut Umum untuk membuat dakwaan agar selanjutnya perkara tersebut dapat diproses di pengadilan dengan menerapkan Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP).