Card-Fraud dalam *Electronics Banking* di Indonesia*

Oleh :
Malkian Elvani, SH, M.Hum
Vegitya Ramadhani-Putri, SH, S.Ant
(Dosen Fakultas Hukum Unsri)

Abstrak

Card-fraud merupakan gangguan dan ancaman kejahatan elektronik yang signifikan terhadap Bank Sentral, dan lembaga perbankan/keuangan, penerbit kartu kredit/kartu pembayaran dan lembaga keuangan lainnya, *merchant*, terutama juga nasabah bank. Penelitian ini menggunakan metode penelitian hukum empiris dengan alat dan teknik pengumpulan data melalui observasi, studi pustaka dan wawancara. Berdasarkan regulasi-regulasi di bidang perbankan terhadap *card-fraud* sejauh ini hanya berkisar pada pengaturan pidana bagi berbagai praktek manipulasi dokumen bank. Dalam hal ini, kartu (*card*) adalah termasuk dokumen bank. *Card-fraud* dapat dianalogikan sebagai bagian dari manipulasi dokumen bank sehingga bisa dikategorikan kejahatan perbankan, baik bank sebagai pelaku, bank sebagai korban, maupun bank sebagai media *card-fraud*. Dalam bidang telematika, *card-fraud* dapat dikategorikan sebagai kejahatan *carding* dan kejahatan *hacking*, yaitu kejahatan dengan modus penyadapan tanpa hak (*illegal interception*), manipulasi yang menyebabkan disfungsi (*manipulation to disfunctioning*), penyalinan tanpa hak (*copying without rights*), dan akses tanpa hak (*illegal acces*), dan semua jenis tersebut dapat dikenai sanksi pidana.

Kata Kunci : *card-fraud, e-commerce*, perbankan.

A. Pendahuluan

Kejahatan berbasis kartu atau biasa disebut *carding* ditujukan pada suatu proses untuk melakukan verifikasi validitas suatu data kartu yang telah dicuri. Pembayaran dalam transaksi *real-time* di internet tidak membutuhkan pembayaran fisik, maka perlu dilakukan uji coba apakah kartu tersebut masih valid atau tidak. Pelaku kejahatan mentargetkan pada transaksi internet yang real-time untuk memastikan bahwa data pada kartu tersebut masih dalam kondisi bagus. Jika kartu tersebut dapat diproses dengan baik, maka uji coba tersebut dianggap berhasil dan bisa digunakan terus-menerus. Biasanya kartu tersebut digunakan untuk pembelanjaan dalam jumlah kecil karena setiap kartu memiliki

* Artikel ini adalah hasil penelitian Insentif Riset yang dibiayai DIPA Unsri tahun anggaran 2008

batas maksimum kredit. Selain itu, transaksi dalam jumlah kecil tidak akan memperoleh perhatian yang lebih dari bank sehingga tidak mencurigakan.

Para pelaku *carding* biasanya menggunakan suatu program komputer yang biasa disebut 'generator' untuk memproduksi suatu rangkaian nomor kartu kredit, lalu mencoba apakah beberapa nomor masih valid atau tidak. Namun cara ini dianggap tidak efisien. Sekarang *carding* lebih difokuskan pada verifikasi data langsung dari kartu korban, baik melalui metode skimming dan phishing.

B. Definisi dan Modus *Card-Fraud*

Kejahatan berbasis kartu (*card fraud*) identik dengan kejahatan kartu kredit. Definisi umum dari kejahatan kartu kredit yaitu:

> *Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft.*

Berikut ini adalah beberapa *card-fraud* yang umum terjadi pada transaksi perbankan :

- Rekayasa Rekening melalui Pencurian Data (*Compromised Accounts by ID Thieft)*
  Informasi rekening kartu terdiri atas suatu nomor (data) terformat. Data rekening tersebut umumnya dicetak dalam kartu yang tersebut secara tersamar begitu juga tercetak secara tersamar pada pita magnetik di belakang kartu dengan suatu format yang hanya bisa dibaca oleh mesin pengidentifikasi. Data tersebut terdiri atas nama pemegang kartu (name of card holder), Nomor rekening (*account number*), waktu kadaluarsa (*expiration date*), dan kode verifikasi (*verification/CVV code* – khusus kode verifisasi ini tidak tercantum pada kartu).

- Kejahatan Melalui Internet / Email (*Internet/Mail Fraud*)
  Email dan internet adalah rute yang paling sering digunakan dalam melakukan kejahatan berbasi kartu. Pembayaran melalui internet pada pedagang (merchants) yang menggunakan jasa pembayaran online merupakan sasaran empuk bagi jenis kejahatan ini. Merchants akan kesulitan mengidentifikasi apakah kartu yang sedang digunakan memiliki validasi yang sah atau tidak.

- Pengambil-alihan Rekening (*account takeover*)
  Terdapat dua jenis modus pencurian identitas, yaitu kejahatan aplikasi (application fraud) dan pengambil-alihan rekening (*account takeover*). Kejahatan aplikasi terjadi ketika pelaku memcuri data atau memalsukan dokumen untuk membuka suatu rekening atas nama orang lain. Pelaku kejahata biasanya mencoba mencuri dokumen seperti berkas tagihan ataupun pernyataan dari bank untuk mengetahui informasi personal. Bisa juga pelaku kejahatan tersebut memalsukan dokumen yang dibutuhkan untuk aksinya.
  Pengambil-alihan rekening (*account takeover*) meliputi upaya kriminal untuk mengambil alih rekening orang lain dengan cara mengumpulkan semua data korban, kemudian menghubungi bank yang bersangkutan atau penerbit kartu kredit (bertindak seolah-oleh pemilik kartu yang asli) untuk mengubah alamat asal menjadi alamat baru. Pelaku melaporkan bahwa kartu telah tercuri dan meminta kartu pengganti dikirim ke alamat yang baru. Kartu pengganti tersebut digunakan untuk tindak kejahatan.

- Skimming
  Modus skimming ini adalah menggunakan 'transaksi yang sah' dengan melibatkan 'orang dalam' yang berkerja pada merchant ataupun bank. Caranya yaitu dengan mennggunakan metode dasar seperti memfotokopi struk kartu ataupun menggunakan alat skimmer. Melalui metode adan alat tersebut akan dieketahui banyak sekali data para perlanggan / konsumen / nasabah. Alat skimmer ini biasanya ditemukan pada mesin Automatic Teller Machines (ATM) maupun pada mesin Electronic Digital Cassier (EDC). Dengan sistem penyadapan ini akan diketahui data pemegang kartu (*card-holder*) sekaligus Personal Identification Number (PIN).

Menurut perusahaan *Security Clear Commerce* di Texas USA, saat ini Indonesia menduduki peringkat ke 2 setelah Ukraina dalam hal kejahatan *Carding* dengan memanfaatkan teknologi informasi (Internet) yaitu menggunakan nomor kartu kredit orang lain untuk melakukan pemesanan barang secara *online*. Komunikasi awalnya dibangun melalui *e-mail* untuk menanyakan kondisi barang

dan melakukan transaksi. Setelah terjadi kesepakatan, pelaku memberikan nomor kartu kreditnya dan penjual mengirimkan barangnya, cara ini relatif aman bagi pelaku karena penjual biasanya membutuhkan 3 – 5 hari untuk melakukan kliring atau pencairan dana sehingga pada saat penjual mengetahui bahwa nomor kartu kredit tersebut bukan milik pelaku barang sudah terlanjur terkirim[1].

Sesungguhnya siapapun, tidak harus nasabah bank yang bersangkutan, dapat masuk ke dalam suatu sistem jaringan perbankan untuk mencuri informasi nasabah yang terdapat di dalam server mengenai *data base* rekening bank tersebut, karena dengan adanya *e-banking* jaringan tersebut dapat dikatakan terbuka serta dapat diakses oleh siapa saja. Kalaupun pencurian data yang dilakukan sering tidak dapat dibuktikan secara kasat mata karena tidak ada data yang hilang tetapi dapat diketahui telah diakses secara *illegal* dari sistem yang dijalankan[2].

Dunia perbankan melalui Internet (*e-banking*) Indonesia, dikejutkan oleh ulah seseorang bernama Steven Haryanto, seorang *hacker* dan jurnalis pada majalah Master Web. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan *Internet banking* Bank Central Asia, (BCA). Steven membeli domain-domain dengan nama mirip www.klikbca.com (situs asli Internet banking BCA), yaitu domain *wwwklik-bca.com, kilkbca.com, clikbca.com, klickca.com.* dan *klikbac.com*. Isi situs-situs plesetan inipun nyaris sama, kecuali tidak adanya security untuk bertransaksi dan adanya formulir akses (*login form*) palsu. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (*user id*) dan nomor identitas personal (PIN) dapat di ketahuinya. Diperkirakan, 130 nasabah BCA tercuri datanya. Menurut pengakuan Steven pada situs bagi para *webmaster* di Indonesia, www.webmaster.or.id, tujuan membuat situs plesetan adalah agar publik menjadi lebih berhati – hati dan tidak ceroboh saat melakukan pengetikan alamat situs (*typo site*), bukan untuk mengeruk keuntungan[3].

Dalam kaitannya dengan transaksi keuangan perbankan, sebagai Undang-Undang yang akan menjadi semacam 'undang-undang payung' bagi kegiatan-kegiatan bank yang terkait dengan media elektronik termasuk mengenai kegiatan transfer dana secara elektronik, maka keberadaan UU ITE dalam menunjang kelancaran sistem pembayaran menjadi sangat penting dan sangat besar kontribusinya[4]. Dalam kaitannya dengan upaya pencegahan tindak pidana, ataupun penanganan tindak pidana, UU ITE akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme.

Beberapa aspek penting yang terkait dengan aspek pidana yang perlu diatur secara jelas antara lain:

- *Pertama,* terkait tanggung jawab penyelenggara sistem elektronik, perlu dilakukan pembatasan atau limitasi atas tanggungjawab sehingga tanggungjawab penyelenggara tidak melampaui kewajaran.
- *Kedua,* seluruh informasi elektronik dan tanda tangan elektronik yang dihasilkan oleh suatu sistem informasi, termasuk *print out*-nya harus dapat menjadi alat bukti di pengadilan.
- *Ketiga,* perlunya aspek perlindungan hukum terhadap Bank Sentral, dan lembaga perbankan/keuangan, penerbit kartu kredit/kartu pembayaran dan lembaga keuangan lainnya dari kemungkinan adanya gangguan dan ancaman kejahatan elektronik. Dalam UU ITE ini, perlindungan tersebut dapat dilakukan dengan mengkriminalisasi setiap penggunaan dan akses yang dilakukan secara *illegal* terhadap komputer institusi/lembaga tersebut, mengingat peranan yang sangat vital dari lembaga-lembaga keuangan dalam perekonomian dan dalam rangka menjaga tingkat kepercayaan masyarakat terhadap lembaga keuangan.
- *Keempat,* perlunya ancaman pidana yang bersifat *deterren* terhadap tindak kejahatan elektronik (*Cybercrime*), sehingga dapat memberikan perlindungan terhadap integritas sistem dan nilai investasi yang telah dibangun dengan alokasi sumber daya yang cukup besar.

---

[1] Gatra , 13 September 2003

[2] Logic, David, 2004, **Cybercrime**, California

[3] **Waspada** , edisi 21 Februari 2005 dengan judul "Penipuan melalui Internet", juga terdapat dalam **Gatra**, edisi 13 September 2003, dan juga terdapat pada ***CyberTECH*** , 6 November 2002 dengan judul "Steven Haryanto".

[4] Data Bank Indonesia:

Sebagai gambaran umum, jika dilihat dari pergerakan dana melalui *e-banking,* data Bank Indonesia menunjukkan bahwa pada tahun 2005 volume transaksi pembayaran yang diproses melalui sistem kliring setiap harinya mencapai 317 ribu transaksi dengan nilai nominal mencapai Rp. 5.5 triliun. Sedangkan yang dilakukan melalui sistem *Real Time Gross Settlement* (Sistem BIRTGS) pada tahun 2005 mencatat volume transaksi sebesar 25 ribu dengan nilai nominal mencapai Rp. 79.6 triliun per hari. Pada kuartal 1 tahun 2006 nilai transaksi pembayaran elektronik melalui Sistem BI-RTGS menunjukkan peningkatan yang lebih signifikan, yaitu mencapai rata-rata sebesar Rp. 103.6 triliun per hari. Dengan demikian secara umum, nilai transaksi transfer dana melalui sistem kliring dan Sistem BI-RTGS di Bank Indonesia dari tahun ke tahun menunjukkan kecenderungan pertumbuhan yang sangat pesat

Dalam pengertian masyarakat umum, transfer dana *(funds transfers)* dapat diartikan sebagai perpindahan dana antara pengirim dan penerima yang dilakukan secara elektronik maupun non elektronik baik melalui bank maupun lembaga bukan bank, seperti kantor pos dan jasa titipan kilat. Kegiatan tersebut telah dipraktikkan oleh masyarakat dalam kurun waktu yang lama, sebagai bagian dari sistem pembayaran yang mendukung kegiatan perekonomian masyarakat, bahkan telah bersifat lintas negara *(cross border)* dan melibatkan berbagai mata uang dalam jumlah nominal dan volume yang besar serta bersifat kompleks.

Berdasarkan data Bank Indonesia, angka nominal dan transaksi secara agregat dari proses kliring dan Sistem BI-RTGS tersebut dari tahun ke tahun selalu meningkat. Apalagi angka tersebut belum mencakup data perputaran dana antar nasabah yang terjadi di dalam bank sendiri *(intra bank)* dan transfer dana di lembaga selain bank yang diperkirakan mencapai volume dan nilai transaksi yang cukup besar, karena melibatkan jutaan pemilik rekening yang dapat melakukan ribuan transaksi pemindah-bukuan (intra bank) per hari[5].

Contoh *cybercrime* dalam transaksi perbankan yang menggunakan sarana Internet sebagai basis transaksi adalah sistem layanan kartu kredit dan layanan perbankan *online* (*online banking*). Dalam sistem layanan yang pertama, yang perlu diwaspadai adalah tindak kejahatan yang dikenal dengan istilah *carding*. Prosesnya adalah sebagai berikut, pelaku *carding* memperoleh data kartu kredit korban secara tidak sah (*illegal interception*) dan kemudian menggunakan kartu kredit tersebut untuk berbelanja di toko *online* (*forgery*). Modus ini dapat terjadi akibat lemahnya sistem autentifikasi yang digunakan dalam memastikan identitas pemesan barang di toko *online*. Kegiatan yang kedua yaitu perbankan *online* (*online banking*).

Beberapa contoh dari *illegal interception* yaitu antara lain:

a) penggunaan kartu asli yang tidak diterima oleh pemegang kartu sesungguhnya (*Non received card*),
b) kartu asli hasil curian/temuan *(lost/stolen card)*,
c) kartu asli yang diubah datanya (*altered card)*,
d) kartu kredit palsu (*totally counterfeit*),
e) menggunakan kartu kredit polos yang menggunakan data asli (*white plastic card*),

[5] Tingginya frekuensi transfer dana secara nasional dapat dilihat dari volume dan nominal perpindahan dana dalam rata-rata harian perputaran kliring tahun 2005 yang mencapai Rp. 5,61 triliun dengan warkat harian rata-rata mencapai 325.287 lembar dan proses Bank Indonesia *Real Time Gross Settlement* (Sistem BI-RTGS) yang mencapai rata-rata Rp79,36 triliun dengan volume transaksi sebesar 25.409.

f) penggandaan sales draft oleh oknum pedagang kemudian diserahkan kepada oknum merchant lainnya untuk diisi dengan transaksi fiktif (*record of charge pumping atau multiple imprint*), dan lain sebagainya.

Dalam kaitan itu *United Nations Commission on International Trade Law (UNCITRAL)*, telah mengeluarkan *Legal Guide* tentang *Electronic Funds Transfer* dan *Model Law* tentang *International Credit Transfer*. Meskipun tidak bersifat *mandatory*, *model law* tersebut telah banyak dijadikan referensi oleh negara-negara dalam penyusunan Undang-Undang Transfer Dana.

Dalam *The Model Law on Electronic Commerce* yang dikeluarkan oleh *the United Nations Commissions on International Trade Law (UNCITRAL Model Law on Electronic Commerce)* diatur beberapa prinsip berkaitan dengan transaksi elektronik, antara lain:

a. *Information shall not be denied its legal effect, validity or enforceability solely on the grounds that it is in the form of a data message* (*Article 5*).
b. *Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference (Article 6).*

Di dalam UU ITE disebutkan bahwa transaksi elektronik adalah hubungan hukum[6] yang dilakukan melalui komputer, jaringan komputer atau media elektronik lainnya. Lebih lanjut yang dimaksud dengan komputer adalah alat pemroses data elektronik, magnetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan. Berdasarkan pengertian tersebut, maka transaksi elektronik memiliki cakupan yang sangat luas, baik mengenai subyeknya yaitu setiap orang pribadi atau badan yang memanfaatkan komputer, jaringan komputer atau media elektronik lainnya, maupun mengenai obyeknya yang meliputi berbagai barang dan jasa.

Sebagai perbandingan, dalam regulasi di bidang transaksi eletronik di Singapura yaitu *Electronic Transaction Act* (ETA), ditentukan beberapa prinsip yang berkaitan dengan transaksi elektronik, antara lain:

[6] Yang dimaksud dengan hubungan hukum adalah hubungan yang menimbulkan akibat hukum yaitu hak dan kewajiban (Mertokusumo, Sudikno, 1988, *Mengenal Hukum*, Liberty, Jogjakarta, hlm. 97).

a. Tidak ada perbedaan antara data elektronik dengan dokumen kertas;
b. Suatu data elektronik dapat menggantikan suatu dokumen tertulis;
c. Para pihak dapat melakukan kontrak secara elektronik;
d. Suatu data elektronik merupakan alat bukti yang sah di pengadilan;
e. Jika suatu data elektronik telah diterima oleh para pihak, maka mereka harus bertindak sebagaimana kesepakatan yang terdapat pada data tersebut.

Kejahatan di cyberspace ini tidak mengenal batas wilayah (*borderless*) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. Semua aksi itu dapat dilakukan hanya dari depan komputer yang memiliki akses Internet tanpa takut diketahui oleh orang lain / saksi mata, sehingga kejahatan ini termasuk dalam *Transnational Crime* / kejahatan antar negara yang pengungkapannya sering melibatkan penegak hukum lebih dari satu negara.

Mencermati hal tersebut dapatlah disepakati bahwa kejahatan IT / *Cybercrime* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar KUHP. Dampak negatif tersebut menimbulkan suatu kejahatan yang dikenal dengan nama "*cybercrime*" yang tentunya harus diantisipasi dan ditanggulangi. Dalam hal ini Polri sebagai aparat penegak hukum telah menyiapkan unit khusus untuk menangani kejahatan *cyber* ini yaitu Unit V IT / Cybercrime Direktorat II Ekonomi Khusus Bareskrim Polri[7].

C.Penemuan Hukum dalam Menghadapi Card-Fraud

C. a. *Copying* Tanpa Hak sebagai Pencurian

Delik tentang pencurian dalam dunia maya termasuk salah satu delik yang paling sering diberitakan di media masa. Pencurian disini tidak diartikan secara konvensional karena barang yang dicuri adalah berupa data digital, baik yang berisikan data transaksi keuangan milik orang lain maupun data yang menyangkut *software* (program) ataupun data yang menyangkut hal-hal yang bersifat rahasia. Delik pencurian di atur dalam Pasal 362 KUHP dan variasinya diatur dalam Pasal 363 KUHP, yakni tentang pencurian dengan pemberatan; Pasal 364 KUHP tentang pencurian ringan, Pasal 365, tentang pencurian yang disertai dengan kekerasan; Pasal 367 KUHP, tentang pencurian di lingkungan keluarga. Pasal 362 KUHP berbunyi:

[7] Golose, Petrus Reinhard, 2006, **Perkembangan Cybercrime dan Upaya Penangananya di Indonesia oleh Polri**, pada Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006

"Barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak Sembilan ratus rupiah"

Menurut hukum pidana, pengertian benda diambil dari penjelasan Pasal 362 KUHP yaitu segala sesuatu yang berwujud atau tidak berwujud seperti listrik, dan mempunyai nilai di dalam kehidupan ekonomi dari seseorang. Data atau program yang tersimpan di dalam media penyimpanan disket atau sejenisnya yang tidak dapat diketahui wujudnya dapat berwujud dengan cara menampilkan pada layar penampil komputer (*screen*) atau dengan cara mencetak pada alat pencetak (printer). Dengan demikian data atau program komputer yang tersimpan dapat dikategorikan sebagai benda seperti pada penjelasan Pasal 362 KUHP.

Kendatipun demikian dalam sistem pembuktian terutama yang menyangkut elemen penting dari alat bukti (Pasal 184 KUHAP ayat (1) huruf c) masih belum mengakui data komputer sebagai bagiannya karena sifatnya yang digital. Padahal dalam kasus *cybercrime* data elektronik seringkali menjadi barang bukti yang ada. Karenanya sangat realistis jika data elektronik dijadikan sebagai bagian dari alat bukti yang sah.

Menurut pengertian *computer related crime*, pengertian mengambil adalah dalam arti meng-copy atau mereka data atau program yang tersimpan di dalam suatu disket dan sejenisnya ke disket lain dengan cara memberikan instruksi-instruksi tertentu pada komputer sehingga data atau program yang asli masih utuh dan tidak berubah dalam posisi semula. Menurut penjelasan pasal 362 KUHP, barang yang sudah diambil dari kekuasaan pemiliknya itu, juga harus berindah dari tempat asalnya, padahal dengan mengambil adalah melepaskan kekuasaan atas benda itu dari pemiliknya untuk kemudian dikuasai dan perbuatan itu dilakukan dengan sengaja dengan maksud untuk dimiliki sendiri, sehingga perbuatan meng-copy yang dilakukan dengan sengaja tanpa ijin dari pemiliknya dapat dikategorikan sebagai perbuatan "mengambil" sebagaimana yan dimaksud dengan penjelasan Pasal 362 KUHP.

Penggunaan fasilitas *Internet Service Provider* (ISP) untuk melakukan kegiatan *hacking* erat kaitannya dengan delik pencurian yang diatur dalam Pasal 362 KUHP. Pencuri biasanya lebih mengutamakan memasuki sistem jaringan perusahaan financial, misalnya: penyimpanan data kartu kredit, situs-situs belanja *on-line* yang ditawarkan di media internet dan data yang didapatkan secara melawan hukum itu diharapkan meberi keuntungan badi si pelaku.

Dalam UU No.10 tahun 2008 tentan Informasi dan Transaksi Elektronik, terdapat beberapa jenis perbuatan yang dilarang yang bias disamakan dengan copying, yaitu :

Pasal 32

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) 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.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Dalam sistem jaringan (*network*), peng-copy-an data dapat dilakukan secara mudah tanpa harus melalui izin dari pemilik data. Hanya sebagian kecil saja dari data internet yang tidak dapat "diambil" oleh para pengguna internet. Pencurian bukan lagi hanya berupa pengambilan barang/benda berwujud saja, tetapi juga termasuk pengambilan data secara tidak sah, termasuk menyadap.

Pemidanaan dalam hal penyadapan, UU ITE Pasal 31 mengatur beberapa kategori yaitu :

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Penjelasan Ayat (1), yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

C. b. *Hacking* sebagai Perusakan

Ketentuan ini erat dengan kejahatan *hacking*. Dalam kejahatan mayantara (*cybercrime*) perbuatan perusakan dan penghancuran barang ini tidak hanya ditujukan untuk merusak/menghancurkan media disket atau media penyimpan sejenis lainnya, namun juga merusak dan menghancurkan suatu data, *web site* ataupun *homepage*. Delik ini juga termasuk di dalamnya perbuatan merusak barang-barang milik publik (*crime against public property*).

Ketentuan mengenai perbuatan perusakan, penghancuran barang diatur dalam Pasal 406-412 KUHP. Pasal 406 KUHP berbunyi:

(4) Barangsiapa dengan sengaja melawan hukum menghancurkan, merusakkn, membikin tidak dapat dipakai lagi atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana dipenjara paling lama dua tahun delapan bulan atau denda paling banyak empat ribu lima ratus rupiah;

(5) Dijatuhkan pidana yang sama terhadap orang, yang dengan sengaja dan melawan hukum membunuh, merusakkan, membikin tidak dapat digunakan atau menghilangkan hewan yang seluruhnya atau sebagian adalah kepunyaan orang lain.

Pengertian-pengertian dalam Pasal 406 KUHP dapat dijelaskan sebagai berikut:

- Menghancurkan atau membinasakan dimaksudkan sebagai merusak sama sekali sehingga suatu barang tidak dapat berfungsi sebagaimana mestinya.

- Merusakkan dimaksudkan sebagai memperlakukan suatu barang sedemikian rupa namun kurang dan membinasakan (*beschacdingen*). Misalnya: perbuatan merusak data atau program komputer yang terdapat di internet dengan cara menghapus data atau program, membuat cacat data atau program, menambahkan data baru ke dalam suatu situs (*web*) atau sejenisnya secara acak. Dengan kata lan, perbuatan tersebut mengacaukan isi media penyimpannnya.
- Tindakan itu harus sedemikian rupa, sehingga barang itu tidak dapat diperbaiki lagi. Kaitannya dengan *cybercrime* adalah perbuatan yang dilakukan tersebut menyebabkan data atau program yang tersimpan dalam media penyimpan (*data base*) atau sejenisnya menjadi tidak dapat dimanfaatkan (tidak berguna lagi). Hal ini disebabkan oleh data atau program telah dirubah sebagian atau seluruhnya, atau dirusak pada suatu bagian atau seluruhnya, atau dihapus pada sebagian atau seluruhnya.
- Pengertian "menghilangkan" adalah membuat barang itu tidak ada lagi. Kaitannya dengan *cybercrime* yakni perbuatan mengilangkan atau menghapus data yang tersimpan pada data base –bisa juga tersimpan dalam suatu web- atau sejenisnya sehingga mengakibatkan semua atau sebagian dari data atau program menjadi hapus sama sekali.

Menurut UU ITE, perbuatan "menghancurkan, merusak, membuat tidak dapat dipakai lagi dan menghilangkan" diatur sebagai berikut :

Pasal 33

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
   a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
   b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

(2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 36

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Berdasarkan pengertian-pengertian mengenai perbuatan "menghancurkan, merusak, membuat tidak dapat dipakai lagi dan menghilangkan", maka dapat disimpulkan bahwa makna dalam perbuatan-perbuatan tersebut tedapat kesesuaian yang pada intinya perbuatan tersebut menyebabkan fugsi dari data atau program dalam suatu jaringan menjadi berubah/berkurang. Perbuatan penghancuran atau perusakan barang yang dilakukan *cracker* dengan kemampuan *hacking*-nya bukanlah perbuatan yang bisa dilakukan oleh semua orang awam. Kemampuan tersebut dimiliki secara khusus oleh orang-orang yang mempunyai keahlian dan kreatifitas dalam memanfaatkan sistem, program, maupn jaringan. Motif untuk kejahatan ini sangat beragam yakni misalnya motif ekonomi, politik, pribadi atau motif kesenangan semata.

C. c. Akses Tanpa Hak sebagai Masuk ke Wilayah Pribadi Orang Lain

Penggunaan sarana jaringan melalui media internet di negara-negara dunia dewasa ini semakin berkembang pesat. Kehadiran internet tidak dapat dielakkan lagi dapat menunjang kerja dari komputer sehingga dapat mengolah data yang bersifat umum melalui suatu *terminal system*. Apabila ada orang asing yang masuk ke dalam jaringan komputer tersebut tanpa ijin dari pemilik terminal ataupun penanggung jawab sistem jaringan komputer, maka perbuatan

ini dikategorikan sebagai *hacking*. Kejahatan komputer jenis hacking –apabila ia melakukan perusakan atau gangguan- sangat berbahaya karena apabila seseorang berhasil masuk ke dalam sistem jaringan orang lain, maka implikasi hukumnya ia mungkin saja membaca dan menyalin informasi yang mungkin sangat rahasia, atau mungkin pula menhapus atau mengubah informasi atau program-program yang tersimpan pada sistem komputer. Ada kemungkinan ia mencuri dengan memerintahkan komputer untuk mengirimkan barang kepadanya.

Perbuatan mengakses ke suatu sistem jaringan tanpa ijin tersebut dapat dikategorikan sebagai perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan tanpa haknya berjalan di atas tanah milik orang lain, sehingga pelaku dapat diancamp idana berdasarkan Pasal 167 KUHP dan Pasal KUHP. Pasal 167 KUHP berbunyi :

(1) Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum atau berada di situ dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama Sembilan bulan atau denda paling banyak empat ribu lima ratus rupiah;

(2) Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu atau barang siapa tidak setahu yang berhak lebih dulu bukan karen kekhilafan masuk dan kedapatan di situ pada waktu malam, dianggap memaksa masuk;

(3) Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, diancam dengan pidana penjara paling lama satu tahun empat bulan;

(4) Pidana tersebut dalam ayat (1) dan (3) ditambah sepertiga jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu.

Dari Pasal 167 KUHP, menurut Andi Hamzah ada beberapa hal yang menyulitkan aparat penegak hukum dalam upaya penanganan kejahatan komputer, antara lain: (a) Apakah komputer dapat disamakan dengan rumah, ruangan atau pekarangan tertutup; (b) Berkaitan dengan cara masuk ke rumah atau ruangan tetutup, apakah test *key* atau *password* yang digunakan oleh seseorang untuk berusaha masuk ke dalam suatu sistem jaringan dapat dikategorikan sebagai kunci palsu, perintah palsu atau pakaian palsu.

Pasal yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain adalah Pasal 551 KUHP. Pasal 551 KUHP berbunyi:

"Barang siapa tanpa wewenang berjalan atau berkendaraan di atas tanah yang oleh pemiliknya dengan cara jelas di larang memasukinya, diancam dengan pidana denda paling banyak dua ratus dua puluh lima rupiah".

Berkaitan dengan pasal di atas, ada beberapa hal yang tidak sesuai lagi untuk diterapkan dalam upaya penanggulangan kejahatan *hacking*, yaitu pidana denda yang sangat ringan – dapat mengganti pidana kurungan - padahal hacking dapat merugikan finansial yang tidak sedikit bahkan mampu melumpuhkan kegiatan dari pemilik suatu jaringan yang berhasil dimasuki oleh pelaku dan perbuatan *hacking* ini merupakan awal dari maraknya kejahatan-kejahatan tradisional dengan sarana komputer dilakukan. Misalnya: pencurian, penipuan, penggelapan, pemalsuan dan lain-lain. Sebagai contoh: Seseorang yang dapat masuk ke suatu jaringan komputer perusahaan akan dengan mudah melakukan transaksi fiktif yang ia kehendaki atau melakukan perbuatan curang lainnya.

Menurut UU ITE, mengakses tanpa hak diatur sebagai berikut :

Pasal 30

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:

a. melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau
b. sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

D. Kesimpulan

Berdasarkan regulasi-regulasi di bidang perbankan terhadap *card-fraud* sejauh ini hanya berkisar pada pengaturan pidana bagi berbagai praktek manipulasi dokumen bank. Dalam hal ini, kartu (*card*) adalah termasuk dokumen bank. *Card-fraud* dapat dianalogikan sebagai bagian dari manipulasi dokumen bank sehingga bisa dikategorikan kejahatan perbankan, baik bank sebagai pelaku, bank sebagai korban, maupun bank sebagai media *card-fraud*. Dalam bidang telematika, *card-fraud* dapat dikategorikan sebagai kejahatan *carding* dan kejahatan *hacking*, yaitu kejahatan dengan modus penyadapan tanpa hak (*illegal interception*), manipulasi yang menyebabkan disfungsi (*manipulation to disfunctioning*), penyalinan tanpa hak (*copying without rights*), dan akses tanpa hak (*illegal acces*), dan semua jenis tersebut dapat dikenai sanksi pidana.

Oleh karena regulasi di ketiga bidang tersebut masih umum, dan tidak secara spesifik mengatur *card-fraud*, maka untuk menemukan titik temu dengan fakta hukum harus dilihat pada proses dan akibat dari *card-fraud* tersebut sehingga bisa dikategorikan sebagai kejahatan atau pelanggaran. Secara keseluruhan, pendekatan ketiga disiplin ilmu hukum tersebut – hukum pidana, hukum perbankan dan hukum telematika – dapat ditarik kesimpulan umum bahwa *card-fraud* merupakan kejahatan dengan modus manipulasi data dan jaringan dengan menggunakan teknologi informasi.

Daftar Pustaka

Buku dan Artikel Ilmiah:

Arief, Barda Nawawi, 2001, **Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan**, Bandung : Citra Aditya Bakti

Arif, Barda Nawawi, 1991, **United Nations** *(Eighth UN Congress On The Prevention Of Crime And The Treatment Of Offenders Report)*

Badrulzaman, Mariam Darus, 2001, "***E-Commerce* : Tinjauan dari Hukum Kontrak Indonesia"**, Jurnal Hukum Bisnis, Vol.12, 2000

Barkatullah, Abdul Halim & Teguh Prasetyo, 2005, **Bisnis *E-Commerce* : Studi Sistem Keamanan dan Hukum di Indonesia**, Yogyakarta : Pustaka Pelajar

Black's Law Dictionary, 7th edition, 1999

Casey, Eoghan, 2001, **Digital Evidence and Computer Crime**, London : A Harcourt Science and Technology Company

Garner, Bryan, 1999, **Black's Law Dictionary Seventh Edition,** St.Paul Minn : West Group.

Golose, Petrus Reinhard, 2006, **Perkembangan Cybercrime dan Upaya Penangananya di Indonesia oleh Polri**, pada Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006

Haris, Freddy, 2000, **Aspek Hukum Transaksi Secara Elektronik di Pasar Modal**, Jakarta.

Irman, Tb, 2006, **Anatomi Kejahatan Perbankan**, Bandung : MQS Publishing

Khairandy, Ridwan, 2002, "**Pengakuan dan Keabsahan *Digital Signature* dalam Perspektif Hukum Pembuktian"**, Jurnal Hukum Bisnis Vo.18, Yayasan Pengembangan Hukum Bisnis, Jakarta.

Laporan Konfererensi PBB X/2000, 19-7-2000

Logic, David, 2004, **Cybercrime**, California

Mertokusumo, Sudikno, 1988, **Mengenal Hukum**, Jogjakarta : Liberty,

Mukti Wibowo, Arrianto, 1998, **Tanda Tangan Digital dan Sertifikat Digital : Apa Itu?**, (artikel belum dipublikasikan), Jakarta

Mukti Wibowo, Arrianto, 2000, "**Kejahatan Kartu Kredit via Internet : Hantu E-Commerce?**", (artikel belum dipublikasikan), Jakarta

Nitibaskara, Tubagus Ronny Rahman, 2001, **Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi**, Jakarta: Peradaban.

Panjaitan, Hinca IP dkk, 2005, **Membangun Cyber Law Indonesia yang Demokratis,** Jakarta : IMLPC

Pengkajian Hukum tentang Masalah Kekuatan Hukum Alat Bukti elektronik, BPHN Departemen Kehakiman RI tahun 1996/1997

Purbo, Onno & AA. Wahyudi, 2001, **Mengenal *E-Commerce***, Jakarta : elex Media Komputindo

Purwadi, Daniel H., 1995, **Belajar Sendiri: Mengenal Internet Jaringan Informasi Dunia**, Jakarta : PT. Elex Media Komputindo

Riswandi, Budi Agus, 2005, **Aspek Hukum Internet Banking**, Jakarta : Radja Grafindo Persada.

Sakti, Nufransa Wira, 2001, **Perpajakan Dalam E-Commerce, Belajar Dari Jepang**, dalam Berita Pajak No. 1443/Tahun XXXIII/15 Mei 2001

Samudera, Teguh, 1992, **Hukum Pembuktian dalam Hukum Acara Perdata**, Bandung : Alumni

Schneir, Bruce, 1996, **Applied Crypthography Second Edition**, New York : John Willey and Sons Inc.

Sitompul, Asril, 2001, **Hukum Internet (Pengenalan Mengenai Masalah Hukum di *Cyberspace*)**, Bandung : Citra Aditya Bakti.

Soekanto, Soerjono, 1986, **Pengantar Penelitian Hukum**, Jakarta : UI Press

Tim Perundang-undangan dan Pengkajian Hukum, Direktorat Hukum Bank Indonesia, Urgensi **Cyberlaw di Indonesia dalam Rangka Penanganan Cybercrime di Sektor Perbankan**, pada Buletin Hukum Perbankan dan Kebanksentralan, Edisi 16 Volume 4 Nomor 2, Agustus 2006

Utadyanto, Riyeke, 2001, **Framework E-Commerce**, Yogyakarta : Penerbit Andy

Wisnusubroto, 1999, **Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer**, Yogyakata: Universitas Atmajaya

Regulasi :
Kitab Undang-Undang Hukum Pidana
Kitab Undang-Undang Hukum Perdata

UNCITRAL Model Law on *Electronic Commerce*
UU No.14 Tahun 1967, jo UU No.7 Tahun 1992, jo UU No. 10 Tahun 1998 tentang Perbankan
UU No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik

Media Cetak :
CyberTECH, 6 November 2002 dengan judul "Steven Haryanto".
Gatra, 13 September 2003
Koran Tempo, edisi *29 Juni 2008*
Waspada, edisi 21 Februari 2005 dengan judul "Penipuan melalui Internet"

E-Data :
Asosiasi Kartu Kredit Indonesia, situs : www.akki.org
Wikipedia, **Bank Fraud**, diakses dari www.wikipedia.com