KEBIJAKAN PENGATURAN *CARDING* DALAM HUKUM PIDANA DI INDONESIA

Sigid Suseno dan Syarif A. Barmawi
Fakultas Hukum Universitas Padjadjaran
Jl. Dipati Ukur No. 35 Bandung

ABSTRAK. Terjadinya berbagai kejahatan yang tergolong *cybercrime* khususnya *carding* telah menimbulkan masalah dalam upaya pencegahan dan penanggulangannya. Salah satu upaya yang saat ini dilakukan adalah dengan menyusun Rancangan Undang-undang tentang Informasi dan Transaksi Elektronik (RUU ITE) yang di dalamnya dirumuskan ketentuan pidana yang mengatur mengenai *cybercrime* termasuk *carding*. Berdasarkan hakekat dan karakteristik *cybercrime*, perumusan kejahatan-kejahatan yang tergolong *cybercrime* tidak tepat apabila dirumuskan sebagai *administrative penal law*, karena pada umumnya *cybercrime* bukan merupakan pelanggaran ketentuan hukum administrasi tetapi merupakan kejahatan murni yang dilakukan dengan menggunakan media komputer atau jaringan komputer (internet). Oleh karena itu lebih tepat apabila *cybercrime* dirumuskan dalam KUHP sebagai tindak pidana umum kecuali kejahatan yang mempunyai karakteristik khusus dapat diatur dalam UU Khusus. Demikian pula pengaturan tindak pidana *carding* sebagaimana dirumuskan dalam Pasal 51 RUU ITE tidak tepat dan tidak cukup representatif untuk mengatur bentuk-bentuk *carding*. Sebaiknya tindak pidana *carding* diatur dalam KUHP sebagai tindak pidana umum atau dalam UU Khusus sebagai tindak pidana khusus.

Kata kunci : *Cybercrime, Carding,* Kejahatan, Undang-undang.

ABSTRACT. Various crimes happened all over the world are anxious for community both individually and publicly, and also these crimes could be operated by traditionally means or high-technically methods such as cybercrime relating to the use of 'carding'. Crime which exercised by computer has induced complicated-trouble of human beings particularly its prevention and suppression. One of efforts to cope the crime is to enact Draft Regulation concerning Information and Electronic Transaction (named in Indonesia RUU Informasi dan Transaksi Elektronik) including of some provision of penal aspect about cybercrime and 'carding'. Based on the original and characteristic of cybercrime, terminology of crime so called cybercrime is not relevant if the crime known as administrative penal law. The reason of the offense is not correct because it does not generally constitute the breach of administrative law, but it is pure-crime performed by computer or computer network named 'internet'. Therefore, cybercrime is more appropriate to be identified in Code Penal (in

Indonesia named KUHP) as general crime, except the wrongdoing has specific typical that it would be governed by another certain act. In conclusion, the arrangement of crime 'carding' as shown by Article 51 of the Draft Act is not right and less representative to order forms of 'carding'. In addition, the crime is better to be regulated in Code Penal as general crime or it is required to be regulated as specific crime.

Key words : Cybercrime, Carding, Crime, Act.

PENDAHULUAN

Perkembangan kejahatan yang termasuk cybercrime, khususnya kejahatan kartu kredit (carding) dan juga pornografi sudah sangat mengkhawatirkan dan meresahkan masyarakat, termasuk masyarakat internasional terutama berkaitan dengan carding yang banyak merugikan warga negara asing (Amerika Serikat dan Eropa). Sehingga Federal Bureau of Investigation (FBI) datang ke Yogyakarta sebagai kota yang paling banyak terjadi carding, untuk melakukan penyelidikan dan membantu Kepolisian RI.

Munculnya berbagai bentuk cybercrime khususnya carding pada era teknologi informasi merupakan sisi negatif dari perkembangan masyarakat dan kenyataannya kejahatan selalu berkembang sejalan dengan perkembangan masyarakatnya.

Masalah penting berkaitan dengan munculnya cybercrime adalah upaya mencegah dan menanggulanginya. Secara teoritis upaya tersebut tidak cukup hanya dengan upaya penal (hukum pidana) tetapi harus dengan upaya non-penal baik melalui hukum perdata, hukum administrasi, peran media massa, pemanfaatan sarana teknologi (techno prevention) serta upaya-upaya sosial lainnya.1

Tanpa bermaksud mengenyampingkan pentingnya upaya non-penal dalam pencegahan dan penanggulangan kejahatan, dalam kesempatan ini penulis akan membatasi masalah pada upaya penal, yaitu mengenai kebijakan pengaturan *cybercrime* khususnya *carding* di Indonesia. Apakah cybercrime (*carding*) harus diatur dalam UU yang bersifat khusus sehingga merupakan tindak pidana khusus atau diatur dalam KUHP sebagai tindak pidana umum ?

Walaupun sudah banyak terjadi *cybercrime* di Indonesia, khususnya *carding*, namun upaya penegakan hukumnya masih sangat memprihatinkan. Data kejahatan *carding* pada tahun 2002 menunjukkan angka yang mencengangkan yaitu terjadi 152 kasus credit card fraud dengan pelaku tersebar di beberapa wilayah di Indonesia antara lain Yogyakarta (62), Jawa Tengah (43), Jawa Barat (36), Jakarta (24), Sumatera (18), Jawa Timur (12), Kalimantan (3), Sulawesi (3) dan daerah lainnya (17). Sebagian besar kejahatan dilakukan di kota-kota besar propinsi tersebut. Korban kejahatan tersebut tersebar di seluruh dunia seperti : USA, Canada, Spanyol, Jerman, Australia, Inggris, Denmark, Perancis, Austria, Jepang, Singapore, dan Korea. Kerugian

yang ditimbulkan mencapai lebih dari US$ 1,296,597 atau Rp. 11.669.373.000.[2] Namun penegakan hukum terhadap kasus-kasus tersebut sangat minim. Hal tersebut terkait dengan berbagai aspek yang mempengaruhi penegakan hukum, diantaranya masalah regulasi di bidang teknologi informasi. Ketentuan-ketentuan dalam Kitab Undang-undang Hukum Pidana (KUHP) dipandang tidak cukup untuk dapat menjangkau *carding* yang sesungguhnya pada hakekatnya adalah sama dengan penipuan (*credit card fraud*). Sesungguhnya dengan menggunakan metoda interpretasi dan konstruksi hukum ketentuan-ketentuan dalam Pasal 263, Pasal 378, dan Pasal 379a KUHP dapat digunakan untuk menjerat pelaku *carding*. Masalah yang mungkin timbul adalah berkaitan dengan pembuktiannya (hukum acara pidana). Aspek lainnya adalah kemampuan aparat penegak hukum, kesadaran hukum masyarakat, dan perlunya sarana-prasarana yang mendukung penegakan hukum terhadap *cybercrime* (carding).

Sampai saat ini Indonesia belum memiliki perangkat hukum yang mengatur aktivitas manusia di bidang teknologi informasi. Bahkan pengaturan mengenai penggunaan sarana computer, yang mengawali perkembangan di dunia internet sekalipun belum punya. Di beberapa Negara pengaturan aktivitas manusia dilakukan sesuai dengan perkembangan yang terjadi di bidang teknologi (informasi). Pengaturan mengenai kejahatan juga didahului dengan pengaturan mengenai *computer crime* terlebih dahulu dan baru kemudian *cybercrime*. Menurut Stein Sehjolberg walaupun *cybercrime is still a computer crime using the worldwide system of connecting computers and networks with the particular set of* communication *standards*, namun beberapa aktivitas di *cyberspace* membutuhkan ketentuan hukum pidana baru atau memperkuat ketentuan hukum pidana yang lama.[3] Beberapa Negara di dunia dalam *Penal Code* sudah mengatur mengenai *computer crime* atau *cybercrime*. Ada pula yang mengatur *cybercrime* secara tersendiri seperti Australia dalam *Cybercrime Act* 2001 No. 161, 2001 atau dalam UU khusus sesuai dengan objek yang dilindungi seperti Amerika Serikat, Malaysia, dan Inggris.

Kebijakan regulasi di bidang teknologi informasi dari Pemerintah sampai saat ini juga belum jelas. Hanya pihak-pihak yang berkepentingan yang punya kepedulian terhadap pentingnya pengaturan *cybercrime*. Sampai saat ini sesungguhnya sudah ada beberapa prakarsa untuk mengatur aktivitas di bidang teknologi informasi antara lain :

1. RUU Pemanfaatan Teknologi Informasi, yang diprakarsai oleh Direktorat Jenderal Pos dan Telekomunikasi Departemen Perhubungan;
2. RUU Informasi Elektronik dan Transaksi Elektronik, yang diprakarsai oleh Departemen Perindustrian dan Perdagangan;
3. RUU Tindak Pidana di Bidang Teknologi Informasi, yang diprakarsai oleh Kepolisian RI.

Di bawah koordinasi Kementrian Komunikasi dan Informasi RUU Pemanfaatan Teknologi Informasi yang sifatnya UU payung (umbrella act)

digabungkan dengan RUU Informasi Elektronik dan Transaksi Elektronik yang sifatnya khusus menjadi RUU Informasi dan Transaksi Elektronik (RUU ITE). Analisis terhadap RUU ITE akan dilakukan terhadap Ketentuan Pidananya berkaitan dengan masalah kebijakan pengaturan *cybercrime* (carding) dalam hukum Indonesia.

METODE

Metode penelitian yang digunakan dalam mengkaji tentang kebijakan pengaturan carding dalam hukum pidana di Indonesia adalah deskriptif analitis. Metode ini digunakan untuk menggambarkan berbagai fakta dan permasalahan berkaitan dengan carding dan kebijakan pengaturannya di Indonesia serta menganalisisnya untuk menemukan alternative solusi terbaik mengenai pengaturan carding di Indonesia.

Di samping itu penulis juga menggunakan metode perbandingan untuk mempertajam analisis atas permasalahan tersebut dengan mengkaji pengaturan carding di Negara Amerika Serikat.

HASIL DAN PEMBAHASAN

Definisi dan Kategorisasi *Cybercrime*

Pengertian *cybercrime* mengalami perkembangan sejalan dengan perkembangan kejahatan di internet. Cybercrime pada awalnya hanya kejahatan berupa perbuatan merusak atau mencuri data dan program komputer. Kemudian berkembang termasuk berbagai kejahatan seperti *forgery, illegal gambling*, dan *cyberstalking*.[4] Dalam Kongres Perserikatan Bangsa-Bangsa X tentang *the Prevention of Crime and the Treatment of Offenders* di Vienna, 10-17 April 2000 pengertian *cybercrime* dibagi dalam 2 kategori, yaitu :

a. *Cybercrime in a narrow sense (computer crime) : any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.*
b. *Cybercrime in a broader sense (computer related crime) : any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.*[5]

Berdasarkan pengertian di atas *computer crime* mencakup perbuatan illegal terhadap *system* dan *data security* dengan menggunakan sarana elektronik. *Computer system* dan *data security* meliputi 3 masalah pokok, yaitu :

a. *the assurance of confidentiality;*
b. *integrity; dan*
c. *availability of data and processing functions.*

Ketiga masalah pokok tersebut meliputi *unauthorized access, damage to computer data or computer programs, computer sabotage, unauthorized interception*, dan *computer espionage*.[6] Sedangkan cybercrime merupakan kejahatan yang dilakukan dengan media elektronik atau dilakukan sebagian atau sepenuhnya dalam lingkungan elektronik.

Pengertian *cybercrime* tersebut tidak tertutup kemungkinan masih mengalami perkembangan di masa yang akan datang sejalan dengan perkembangan kejahatan di bidang teknologi informasi.

Cybercrime dapat dibedakan dalam beberapa kategorisasi kejahatan *berdasarkan* kriteria tertentu. Debra L.Shinder misalnya membuat kategorisasi *cybercrime* berdasarkan cara kejahatan dilakukan : Pertama, kejahatan dilakukan dengan kekerasan atau pelaku secara potensial melakukan kejahatan dengan kekerasan (*crimes committed by violent or potentially violent criminals*) dan Kedua, kejahatan dilakukan tanpa kekerasan (*nonviolent crimes*). Kejahatan-kejahatan yang termasuk kategori pertama (*crimes committed by violent or potentially violent criminals*) antara lain :

a. *Cyberterrorism*
   Terorisme yang direncanakan, dikoordinasikan, dan dilakukan di dunia *cyberspace*, yaitu dengan menggunakan jaringan computer (internet)
b. *Assault by threat*
   Ancaman penyerangan ini dapat dilakukan melalui e-mail sehingga orang dalam keadaan ketakutan dalam hidupnya. Misalnya ancaman bom melalui e-mail yang dikirim ke pusat-pusat bisnis atau pemerintahan.
c. *Cyberstalking*
   Gangguan melalui media elektronik dan seringkali berupa ancaman fisik yang membuat korban ketakutan.
d. *Child pornography*
   Membuat, mendistribusikan dan mengakses materi pornografi yang objeknya anak-anak.

Sedangkan kejahatan-kejahatan yang termasuk kategori kedua (*nonviolent crimes*) antara lain :

a. *Cybertrespass*
   Kejahatan mengakses computer atau jaringan komputer tanpa menyalahgunakan atau merusak data. *Cybertrespass* seringkali disebut sebagai *unauthorized access* atau *breach of network security* atau sejenisnya.
b. *Cybertheft*
   Cybertheft merupakan kejahatan untuk mencuri informasi, uang atau sesuatu yang mempunyai nilai. Keuntungan merupakan motivasi dari pelaku melakukan *cybertheft*. Jenis-jenis *cybertheft* antara lain : embezzlement, *corporate/industrial espionage, plagiarism, piracy, identity theft*, dll.

c. *Cyberfraud*
   Penipuan melalui internet berbeda dengan pencurian. Dalam *cyberfraud* korban mengetahui dan secara sukarela memberikan uangnya kepada pelaku kejahatan.
d. *Destructive cybercrimes*
   Merusak atau menghancurkan data atau jaringan pelayanan. Misalnya *hacking* into *network and deleting data or program files, hacking into a Web server and vadalizing Web pages, worms and other malicious code into a network or computer.*
e. *Other cybercrimes*, termasuk *advertising/soliciting prostitution services over the internet, internet gambling, internet drug sales, cyberlaundering*, dll.[7]

Kategorisasi *cybercrime* dapat dilihat dalam Konvensi Dewan Eropa tentang *Cybercrime*, sebagai berikut :

a. *Offences against the confidentiality, integrity, and availability of computer data and systems :*
b. *Illegal acces*
c. *Illegal interception*
d. *Data interference*
e. *System interference*
f. *Misuse of device*
g. *Computer related offences*
h. *Computer related forgery*
i. *Computer related fraud*
j. *Content related offences*
k. *Offences related to child pornography*
l. *Offences related to infringement of copyright and related right*

Kebijakan Pengaturan Cybercrime dalam RUU Informasi dan Transaksi Elektronik

Berdasarkan uraian mengenai kategorisasi *cybercrime* maka cakupan kejahatan yang termasuk *cybercrime* relatif luas, dapat berupa kejahatan tradisional yang menggunakan media komputer/internet dan kejahatan-kejahatan baru yang menggunakan internet.

Dalam RUU Infromasi dan Transaksi Elektronik terdapat 5 (lima) pasal yang mengatur mengenai *cybercrime*, yaitu Pasal 47 – Pasal 51.

Pasal 47

Setiap orang dengan sengaja dan melawan hukum melanggar ketentuan sebagaimana dimaksud dalam Pasal 30 ayat (1), dipidana dengan pidana penjara paling lama 4 (empat) tahun dan atau denda paling banyak Rp. 1.000.000.000.,- (satu milyar rupiah).

Pasal 30 ayat (1) mengatur mengenai larangan untuk dengan sengaja dan melawan hukum menggunakan dan atau mengakses komputer dan atau

sistem elektronik dengan maksud untuk memperoleh atau mengubah informasi.

Pasal 48

Setiap orang dengan sengaja dan melawan hukum melanggar ketentuan sebagaimana dimaksud dalam Pasal 24, Pasal 29 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) bulan dan atau denda paling banyak Rp.100.000.000.,- (seratus juta rupiah).

Pasal 24 mengatur mengenai kewajiban agen elektronik untuk memberikan kesempatan kepada pihak yang menggunakan bila bermaksud akan melakukan perubahan terhadap informasi yang disampaikan melalui agen elektronik yang masih dalam proses transaksi.

Pasal 29 ayat (1) mengatur mengenai kewajiban adanya persetujuan dari pemilik data dalam penggunaan setiap informasi melalui media elektronik yang menyangkut hak pribadi seseorang.

Pasal 49

(1) Setiap orang dengan sengaja dan melawan hukum melanggar ketentuan sebagaimana dimaksud dalam Pasal 27 ayat (2), dipidana dengan pidana penjara paling lama 6 (enam) bulan dan atau denda paling banyak Rp.100.000.000,- (seratus juta rupiah).
(2) Tindak pidana sebagaimana dimaksud dalam ayat (1) hanya dapat dituntut atas pengaduan dari orang yang terkena tindak pidana.
Pasal 27 ayat (2) mengatur mengenai kewajiban pemilikan dan penggunaan nama domain didasarkan pada itikad baik.

Pasal 50

Setiap orang dengan sengaja dan melawan hukum melanggar ketentuan sebagaimana dimaksud dalam Pasal 30 ayat (2), Pasal 30 ayat (3), Pasal 31, Pasal 32, Pasal 33 ayat (1), Pasal 33 ayat (2), Pasal 33 ayat (3), Pasal 33 ayat (4), Pasal 36 ayat (2), atau Pasal 37, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah).

Pasal 30 ayat (2) mengatur mengenai larangan untuk dengan sengaja dan melawan hukum menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan maksud untuk memperoleh informasi milik pemerintah yang dirahasiakan atau dilindungi.

Pasal 30 ayat (3) mengatur mengenai larangan untuk dengan sengaja dan melawan hukum menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan maksud untuk memperoleh informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara.

Pasal 31 mengatur mengenai larangan melakukan perbuatan yang dapat mengakibatkan transmisi dari program, informasi, kode atau perintah, komputer dan atau sistem elektronik yang dilindungi negara menjadi rusak.

Pasal 32 dan 33 mengatur mengenai larangan menggunakan dan atau mengakses komputer dan atau sistem elektronik milik pemerintah atau dilindungi negara atau dilindungi masyarakat.
Pasal 36 ayat (2) mengatur mengenai larangan menyebarluaskan, memperdagangkan, dan atau memanfaatkan kode akses (password) atau informasi yang dapat digunakan untuk menerobos komputer dan atau sistem elektronik dengan tujuan untuk menyalahgunakan komputer dan atau sistem elektronik yang digunakan atau dilindungi pemerintah.
Pasal 37 mengatur mengenai larangan untuk merusak komputer atau sistem elektronik yang dilindungi negara.

Pasal 51
Setiap orang dengan sengaja dan melawan hukum melanggar ketentuan sebagaimana dimaksud dalam Pasal 34 ayat (1), Pasal 34 ayat (2), Pasal 35, atau Pasal 36 ayat (1), dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah).
Pasal 34 ayat (1) mengatur mengenai larangan untuk menggunakan dan atau mengakses komputer dan atau sistem elektronik secara tanpa hak atau melampaui wewenangnya dengan maksud memperoleh keuntungan atau informasi keuangan dari lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabah
Pasal 34 ayat (2) mengatur mengenai larangan menggunakan dan atau mengakses kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan.
Pasal 35 mengatur mengenai larangan menggunakan dan atau mengakses komputer dan atau sistem elektronik lembaga keuangan dan atau perbankan yang dilindungi.
Pasal 36 ayat (1) mengatur mengenai larangan menyebarkan, memperdagangkan dan atau memanfaatkan kode akses (*password*) atau informasi yang dapat digunakan menerobos komputer dan atau sistem elektronik dengan tujuan menyalahgunakan yang dapat mempengaruhi sistem elektronik keuangan dan atau perbankan.

Apabila dilihat dari perumusannya maka ketentuan pidana dalam RUU Informasi dan Transaksi Elektronik merupakan *administrative penal law* dalam arti hukum pidana digunakan untuk mendukung atau memperkuat efektivitas ketentuan administratif sebagaimana dinyatakan dalam rumusan pasal-pasal Ketentuan Pidana. Perumusan *cybercrime* sebagai ketentuan yang bersifat *administrative penal law* tidak tepat kecuali seperti pelanggaran mengenai domain name dapat dirumuskan secara *administrative penal law*. Tidak semua *cybercrime* merupakan pelanggaran terhadap ketentuan administratif dan bahkan sebagian besar pada hakekatnya murni kejahatan. Perbuatan mencuri,

merusak, menipu, dan sejenisnya bukan merupakan pelanggaran ketentuan administratif tetapi merupakan kejahatan yang menggunakan sarana atau media baru berupa komputer atau jaringan komputer (internet).

Pengaturan kejahatan-kejahatan yang termasuk *cybercrime* akan lebih tepat apabila dirumuskan dalam KUHP, karena pada dasarnya merupakan tindak pidana umum, kecuali kejahatan-kejahatan yang mempunyai karakteristik khusus di bidang teknologi informasi dapat diatur dalam UU khusus. Sehingga tidak terjadi penempatan suatu tindak pidana dalam UU khusus, padahal tindak pidana tersebut tidak mempunyai karakteristik sebagai tindak pidana khusus. Oleh karena itu perlu adanya pengkajian yang lebih mendalam mengenai hal ini agar tidak timbul kerancuan di kemudian hari.

Kebijakan pengaturan *cybercrime* dalam KUHP dapat dilakukan dengan merumuskan tindak pidana baru apabila memang perumusan yang sudah ada tidak cukup memadai untuk mengatur *cybercrime* atau dapat juga dengan merumuskan kembali (memodifikasi) perumusan tindak pidana yang sudah ada sehingga dapat mencakup berbagai perkembangan baru di bidang teknologi informasi.

Dilihat dari kategorisasi *cybercrime* di atas, pengaturan *cybercrime* dalam RUU Informasi dan Transaksi Elektronik juga relatif kecil. Beberapa kejahatan yang diatur dalam RUU Informasi dan Transaksi Elektronik adalah kejahatan yang termasuk *nonviolent crimes*, antara lain : *cybertrespass, cybertheft, cyberfraud, dan destructive cybercrime*. Namun demikian bentuk-bentuk kejahatan dari *cybertrespass, cybertheft,* cyberfraud*, dan destructive cybercrime* juga tidak semua dapat terjangkau dalam RUU Informasi dan Transaksi Elektronik karena dirumuskan secara terbatas. Sedangkan kejahatan yang termasuk *violent crime or potentially violent criminals* sama sekali tidak diatur dalam RUU Informasi dan Transaksi Elektronik. Hal tersebut juga dipengaruhi oleh keterbatasan luas lingkup pengaturan dari RUU Informasi dan Transaksi Elektronik. Oleh karena itu walaupun nantinya RUU Informasi dan Transaksi Elektronik diundangkan akan masih banyak lubang menganga yang membuat *cyber criminals* leluasa melakukan kejahatan di Indonesia.

Kebijakan Pengaturan Carding dalam RUU Informasi dan Transaksi Elektronik

Kejahatan kartu kredit (carding) dapat dilakukan dengan berbagai macam modus operandi. Dari yang paling sederhana seperti membuat identitas palsu untuk aplikasi kartu kredit sampai membuat *credit card* palsu dengan menggunakan teknologi yang super canggih sebagaimana digunakan oleh penerbit *credit card*.

Kebijakan pengaturan carding juga kelihatannya belum jelas dan masih ragu-ragu. Dalam RUU Informasi dan Transaksi Elektronik hanya adanya satu pasal yang mengatur mengenai carding, yaitu berkaitan dengan perbuatan menggunakan dan atau mengakses kartu kredit orang lain secara tanpa hak.

Berdasarkan alur proses transaksi melalui *credit card*, ada beberapa tahapan yang dapat menjadi objek pelanggaran dalam kejahatan kartu kredit, antara lain :

a. *Source of applications*.
   Kejahatan yang dilakukan adalah dengan melakukan *fraud application.*
b. *Application processing*.
   Kejahatan yang dilakukan adalah dengan melakukan *fraud application*.
c. *Card embossing and delivery (courier/recipient or customer)*;
   Kejahatan dilakukan dengan menggunakan kartu kredit yang asli yang tidak diterima (*Non Received Intercept*/NRI)
d. *Usage*.
   Kejahatan dilakukan dengan melakukan pemalsuan.
e. *Payment to merchant*.[8]

Beberapa modus operandi yang dapat dilakukan sesuai dengan alur proses kartu kredit tersebut antara lain :

a. *Fraud application*;
   Menggunakan kartu kredit asli yang diperoleh dengan aplikasi palsu. Pelaku memalsu data pendukung dalam proses aplikasi seperti : KTP, Pasport, rekening koran, Surat Keterangan Pengahsilan dll.
b. *Non received card*;
   Menggunakan kartu kredit asli yang tidak diterima oleh oleh pemegang kartu kredit yang sah (berhak) kemudian pelaku membubuhkan tanda tangan di kolom tanda tangan. Kartu kredit diperoleh melalui kurir atau membobol kantos pos bila dikirim melalui Pos.
c. *Lost/stolen card*;
   Menggunakan kartu kredit asli hasil curian atau hilang. Pada waktu melakukan transaksi pelaku menandatangani sales draft dan meniru tanda tangan pada kartu kredit atau tanda tangan pemegang kartu yang sah. Transaksi dilakukan di bawah *floor limit* agar tidak perlu dilakukan otorisasi.
d. *Altered card*;
   Menggunakan kartu kredit asli yang sudah diubah datanya. Pelaku menggunakan kartu hasil curian (*lost/stolen, non received, expired card*) dan kartu reliefnya dipanasi dan diratakan kemudian direembossed dengan data baru. Sedangkan *magnetic stripe* diisi data baru dengan *reencoded* yang diperoleh dari *point of compromise* (POC).
e. *Totally counterfeited*;
   Menggunakan kartu kredit yang seluruhnya palsu. Pelaku mencetak kartu tiruan dengan menggunakan data nomor dan pemegang kartu yang masih berlaku dengan melakukan *reembossed* dan *reencoded*.
f. *White plastic card*;
   Menggunakan kartu plastik polos yang berisi data asli. Pelaku mencetak data dari pemegang kartu kredit yang sah pada plastik polos, tanpa meniru

hologram dan logo penerbit. Magnetic stripe diisi dengan data pemegang kartu dengan cara *encoding*.

g. *Record of charge (Roc) pumping*;
   Penggandaan *sales draft* oleh *merchant* (pedagang). *Sales draft* yang satu tidak ditandatangi oleh pemegang kartu yang sah dan diserahkan kepada *merchant* lain untuk diisi dengan data transaksi fiktif.
h. *Altered amount*;
   Mengubah nilai transaksi pada *sales draft* oleh *merchant* (pedagang).
i. *Telephone/mail ordered*;
   Memesan barang melalui telepon atau surat dengan menggunakan kartu kredit orang lain yang sudah diketahui nama dan nomornya.
j. *Mengubah* program *Electronic Data/Draft Capture* (EDC);
   Mengubah dan merusak program pada alat otorisasi (*electronic data/draft capture*/EDC) milik pengelola oleh *merchant* (pedagang).
k. *Fictius merchant*.
   Pelaku berpura-pura menjadi pedagang dengan mengajukan aplikasi disertai dengan data-data palsu.

Pelaksanaan modus operandi tersebut juga didukung berbagai instrumen seperti *skimmer* atau *software* untuk generate nomor kartu kredit dan kesempatan yang relatif terbuka untuk mencuri data dari kartu kredit seperti di hotel, restaurant, *card centre* dll. sehingga identitas kartu kredit dapat diperoleh dengan mudah.[9]

Berdasarkan modus operandi yang dapat dilakukan oleh pelaku *carding*, pada dasarnya *carding* juga merupakan kejahatan murni dan bukan pelanggaran terhadap hukum administrasi. Oleh karena itu tidak tepat apabila perumusan tindak pidana *carding* dirumuskan seperti ketentuan pidana dalam Pasal 51 RUU ITE yang mengancamkan sanksi pidana terhadap pelaku pelanggaran ketentuan Pasal 34 ayat (2) RUU ITE. Lebih tepat apabila dirumuskan sebagai tindak pidana umum dalam KUHP atau dalam UU Khusus seperti dilakukan negara Phillippines dan Taiwan apabila memenuhi karakteristik sebagai tindak pidana khusus.

Dengan mengacu pada tahapan alur proses kartu kredit, ketentuan dalam Pasal 51 RUU Informasi dan Transaksi Elektronik hanya dapat menjangkau pelanggaran pada tahapan *Card embossing and delivery (courier/*recipient *or customer)* dan *Usage*. Namun demikian tidak semua modus operandi dalam tahapan tersebut dapat terjangkau, karena ketentuan Pasal 51 jo. Pasal 34 hanya mengatur perbuatan yang dilakukan oleh orang yang menggunakan kartu kredit tetapi tidak termasuk *merchant* (pedagang) atau pengelola atau penerbit yang juga dapat menjadi pelaku kejahatan kartu kredit. Dalam Pasal 34 RUU Informasi dan Transaksi Elektronik dinyatakan :

Setiap orang dilarang dengan sengaja dan melawan hukum :

a. menggunakan dan atau mengakses komputer dan atau sistem elektronik secara tanpa hak atau melampaui wewenangnya dengan maksud

memperoleh keuntungan atau memperoleh informasi keuangan dari lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya.

b. Menggunakan dan atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan.

Perumusan kejahatan kartu kredit hanya dengan mengandalkan ketentuan Pasal 51 jo. Pasal 34 RUU Informasi dan Transaksi Elektronik tentunya belum cukup melindungi masyarakat dan pihak-pihak yang berkepentingan. Masih diperlukan perumusan yang lebih representatif yang dapat menjangkau semua bentuk kejahatan kartu kredit.

Sebagai bahan perbandingan berikut pengaturan penipuan dengan menggunakan kartu kredit di Amerika Serikat dalam 15 USC *Section* 1644 *Fraudulent use of credit cards; penalties :*

(a) Use, attempt or conspiracy to use card in transaction affecting interstate or foreign commerce.

Whoever knowingly in a transaction affecting interstate or foreign commerce, uses or attempts or conspires to use any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card to obtain money, goods, services, or anything else of value wich within any one-year period has a value aggregating $1,000 or more; or

(b) Transporting, attempting or conspiring to transport card in interstate commerce.

Whoever, with unlawful or fraudulent intent, transport or attempts or conspires to transport in interstate or foreign commerce a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card knowing the same to be counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained; or

(c) Use of interstate commerce to sell or transport card.

Whoever with unlawful or fraudulent intent, uses any instrumentality of interstate or foreign commerce to sell or transport a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card knowing the same to be counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained; or

(d) Receipt, Concealment, etc. Of goods obtained by use of card.

Whoever knowingly receives, conceals, uses, or transport money, goods, services, or anything else of value (except tickets for interstate or foreign transportation) which (1) within any one-year period has a value aggregating $ 1,000 or more, (2) has moved in or is part of, or which constitute interstate or foreign commerce, and (3) has been obtained with a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card; or

(e) Receipt, concealment, etc. Of tickets for interstate or foreign transportation obtained by use of card.
Whoever knowingly receives, conceals, uses, sells, or transportation in interstate or foreign commerce one or more tickets for interstate or foreign transportation, which (1) within any one-year period have a value aggregating $ 500 or more, (2) have been purchased or obtained with one or more counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit cards; or

(f) Furnishing of money, etc., through use of card.
Whoever in transaction affecting interstate or foreign commerce furnishes money, property, services, or anything else of value, which within any one-year period has a value aggregating $ 1,000 or more, through the use of any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card knowing the same to be counterfiet, fictitious, altered, forged, lost, stolen, or fraudulently obtained shall be fined nor more than $ 10.000 or imprisoned not more than ten years, or both.

Dalam ketentuan 15 USC Section 1644 pengaturan mengenai penipuan dengan menggunakan kartu kredit lebih luas dibanding dengan pengaturan dalam RUU Informasi dan Transaksi Elektronik, yaitu meliputi perbuatan :

a. Mengetahui dalam transaksi yang menggunakan kartu kredit adanya pemalsuan, penyamaran, pengubahan, pemalsuan nama, pencurian, atau penipuan.
b. Dengan sengaja dan melawan hukum menjual atau mengangkut kartu kredit tersebut.
c. Menerima, menyembunyikan atau menggunakan kartu kredit tersebut.
d. Menerima, menyembunyikan, menjual atau mengangkut tket yang diperoleh dari kartu kredit tersebut.
e. Menyediakan uang, barang, jasa, atau sesuatu yang bernilai yang diperoleh melalui kartu kredit tersebut.
   Dalam ketentuan tersebut termasuk juga perbuatan percobaan dan permufakatan untuk perbuatan-perbuatan tersebut di atas.

Dengan pengaturan tersebut maka perbuatan-perbuatan yang termasuk kejahatan kartu kredit yang dapat dilakukan dalam tahapan alur proses kartu kredit relatif dapat terjangkau, baik dalam tahapan *source application, application processing, card embossing and delivery, usage* atau *payment to merchant*. Demikian pula pelaku kejahatan kartu kredit yang dapat dijangkau ketentuan tersebut tidak hanya pengguna kartu kredit tetapi juga pedagang, penerbit kartu kredit atau siapapun yang mengetahui adanya pemalsuan kartu kredit, penggunaan atau peredaran kartu kredit tersebut, bahkan orang yang mencoba melakukan kejahatan kartu kredit juga diancam pidana.

REKOMENDASI

Berdasarkan uraian di atas perlu kiranya dilakukan pengkajian lebih mendalam terhadap kebijakan pengaturan kejahatan kartu kredit di Indonesia baik berkaitan dengan kebijakan perumusannya maupun pengaturan bentuk-bentuk kejahatan kartu kredit. Sehingga kecenderungan yang terjadi saat ini untuk mengubah suatu UU yang baru diundangkan tidak terjadi sehingga dapat dilakukan efisiensi. Mudah-mudahan berbagai kelemahan yang masih ada dalam pengaturan *cybercrime* di Indonesia khususnya mengenai carding dapat diantisipasi oleh Tim Penyusun RUU tindak pidana di bidang teknologi informasi atau dalam Tim Penyusun Rancangan KUHP.

Akhir kata semoga karya tulis ini dapat memberikan masukan dalam rangka pengaturan carding di Indonesia.

CATATAN KAKI

[1] Lihat Peter Hoefnagels, *The Other Side of Criminology*, *An Inversion of the Concept of Crime*, Kluwer Deventer, Holland, 1972, hlm. 57.

[2] E. Brata Mandala, *Tindak Pidana Tehnologi Informasi (Cyber crime) dan Strategi Penanggulangannya*, Makalah, Jakarta, Desember 2003, hlm. 2-3. Bandingkan KC Cheng, *Regional Fraud Trends*, Makalah, Bandung, 2002.

[3] Stein Sehjolberg, *The Legal Framework – Unauthorized Access to Computer Systems, Penal Legislation* in *37 Countries*, http : // www.mossbyrett.of.no/info/legal.html, 15 Februari 2000.

[4] Gabriole Zeviar-Geese, *Across Borders, The State of Law on Cyberjurisdiction and Cybercrime on the Internet,*http :// www.law.gonzaga.edu/border...yberlaw.html, 26 Oktober 1999, hlm.5.

[5] United Nation, Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, hlm. 5; Debra Littlejohn Shinder, *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland Massachusset, 2002, hlm. 17.

[6] United Nation, *Ibid*.

[7] Debra L. Shinder, *Op.Cit.,* hlm. 19-33.

[8] Lihat Asosiasi Kartu Kredit Indonesia, *Payment Card*, Bandung, 4 April 2002, hlm. 9.

[9] VISA International, *Credit Card Fraud Trend & Legislation*, Bandung, 4 April, 2002, hlm. 13, 15.

DAFTAR PUSTAKA

Sumber Buku :

Hoefnagels, Peter, *The Other Side of Criminology*, *An Inversion of the Concept of Crime*, Kluwer Deventer, Holland, 1972,

Shinder, Debra Littlejohn, *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland Massachusset, 2002.

United Nation, Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000.

Sumber prosiding seminar :

E. Brata Mandala, *Tindak Pidana Tehnologi Informasi (Cyber crime) dan Strategi Penanggulangannya*, Makalah, Jakarta, Desember 2003.

Asosiasi Kartu Kredit Indonesia, *Payment Card*, Bandung, 4 April 2002.

VISA International, *Credit Card Fraud Trend & Legislation*, Bandung, 4 April, 2002.

Sumber internet :

Sehjolberg, Stein, *The Legal Framework – Unauthorized Access to Computer Systems, Penal Legislation in 37 Countries*, http://www.mossbyrett.of.no/info/legal.html, 15 Februari 2000.

Zeviar-Geese, Gabriole, *Across Borders, The State of Law on Cyberjurisdiction and Cybercrime on the Internet,* http://www.law.gonzaga.edu/border...yberlaw.html, 26 Oktober 1999.

Undang-undang :

Cybercrime Act 2001, No. 161, 2001.

Rancangan Undang-undang tentang Informasi dan Transaksi Elektronik, 15 Maret 2004.