BAB II

PENGATURAN CARDING DALAM HUKUM POSITIF

2.1. *Carding* Dan Kejahatan Dunia Maya

2.1.1. Pengertian *Carding*

Carding adalah proses penerbitan nomor kartu kredit dengan cara menggunakan program *generating* untuk mencoba kemungkinan nomor-nomor dengan cara memalsukan. Bisa juga dikatakan sebagai kejahatan dengan kegiatan pembelian barang dengan cara melanggar hukum yang memanfaatkan kartu kredit hasil curian.[22] Kejahatan ini juga dikenal dengan istilah *cyberfraud* atau penipuan di dunia maya. Indonesia adalah negara yang memiliki prosentase tinggi dalam kejahatan di dunia maya.

Adapun pengertian *carding* dari beberapa sumber :

a. Menurut Doctor Crush dalam *bulletin* para *hacker* menyebutkan pengertian *carding* adalah pencurian barang yang diinginkan dengan cara berbelanja tanpa membayar.
b. Menurut IFFC (*Internet Fraud Complaint Centre* salah satu unit FBI) *carding* adalah penggunaan *credit card* (kartu kredit) atau *debit card* (kartu debit) *fraudulently* secara illegal untuk mendapatkan uang yang mana *credit card* atau *debit card* dicuri dari situs yang tidak memiliki tingkat keamanan yang tinggi atau diperoleh dengan cara mencuri identitas.

[22] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi*, Rajawali Pers, Jakarta, 2013, hlm. 34.

Carding adalah salah satu contoh dari internet *fraud*, adalah tindakan melawan hukum atau penipuan dengan cara memanfaatkan media internet atau teknologi yang didukung oleh internet. *Fraud* dalam *carding* berarti merupakan pencurian nomor kartu kredit untuk memesan sejumlah barang atau transaksi *online*, maka dari itu dikatakan bahwa *carding* merupakan perbuatan yang melawan hukum.

Perkembangan teknologi dengan kecanggihan informasi dan komunikasi membuat pelaku kejahatan dengan modus baru yang lebih canggih semakin marak terjadi, sebagai contoh adalah kejahatan dengan menggunakan komputer dan internet untuk melakukan kejahatan *carding* dengan media kartu kredit. Kartu kredit adalah fasilitas yang diberikan oleh bank berupa uang plastik yang mana pemegang kartu kredit memperoleh kredit dari bank dan pembayaran dapat dilakukan dengan cara mengangsur dengan membayar sebuah bunga (*finance charge*) ataupun pembayaran dengan sekaligus pada waktu yang telah ditetapkan.

Semakin merebaknya penyedia internet yang didukung oleh terjangkaunya biaya akses internet membuat semakin banyak pengguna dari berbagai macam kalangan mengenal dan menggunakan internet. Hal tersebut membuat para pelaku kejahatan memanfaatkan kesadaran pengguna kartu kredit yang masih rendah yang kurang paham akan dampak negatif yang ditimbulkan dari internet dengan melakukan kejahatan *carding*. Permasalahan kriminalitas jaringan komputer dan internet semakin beragam karena ruang lingkup yang semakin luas. Salah satu bentuk kejahatan di internet adalah *carding*, yang memiliki motif kriminal dan berpotensi untuk menyebabkan perang informasi bahkan kerugian.

Sebagai jenis kejahatan dengan modus baru yang memanfaatkan kecanggihan komputer dan internet, *carding* memiliki karakteristik dalam modus operandinya, yaitu :

a. *Minimize of physical contact*

   Modus utama kejahatan *carding* adalah korban tidak bertemu secara langsung dengan pelaku sehingga tidak adanya kontak fisik karena peristiwa itu berlangsung di dunia maya bahkan bisa saja terjadi antar lintas negara, tetapi kerusakan maupun kerugian yang ditimbulkan nyata. Fakta menarik dari kejahatan *carding* adalah bahwa pelaku cukup mengetahui nomor yang terdapat pada kartu kredit yang sudah didapatkan, dengan keahlian khusus pelaku akan dengan sangat mudah menggunakan kartu kredit tersebut untuk berbelanja secara *online*. Jadi fisik kartu kredit dari korban (pemilik asli) tidak perlu dicuri.

b. *Non violence* (tanpa kekerasan)

   Tidak bertemu secara langsung antara pelaku dan pemilik asli kartu kredit sebagai ancaman fisik yang menyebabkan ketakutan pada korban, sehingga korban memberikan hartanya. Dalam hal ini, pelaku cukup mengetahui nomor kartu kredit untuk bertindak.

c. *High tech* (teknologi yang canggih)

   Internet merupakan prioritas utama dalam penggunaan peralatan teknologi canggih dan penggunaan fasilitas komputer/jaringan.

d. *Global*

Kejahatan ini terjadi antar negara yang tidak memperdulikan batas-batas wilayah dan waktu.[23]

Kejahatan *carding* dapat dikatakan sebagai bentuk kejahatan dunia maya karena :

a. Karakteristik kejahatan *carding* yang menggunakan komputer dan sistem jaringan jatuh dalam bentuk kejahatan siber sesuai dengan hukum internasional.
b. Penjahat *carding* memerlukan bantuan perangkat lunak sistem komputer untuk menyerang sistem informasi dan data komputer dalam hal ini berupa informasi kartu kredit.
c. Para pelaku kejahatan *carding* dalam modus operandi dapat menyebarkan informasi atau menerima informasi tentang kepemilikan kartu kredit dengan menggunakan jaringan atau sistem komputer untuk merugikan orang lain, terutama para pengguna kartu kredit itu sendiri.[24]

Adapun macam jenis kejahatan *carding*, antara lain :

a. *Wiretapping*

Jenis *carding* ini adalah kejahatan dengan cara pelaku menyadap transaksi kartu kredit melalui jaringan komunikasi. Menggunakan

[23] Aru Malika, "*Pengaturan Hukum Internasional Terhadap Kejahatan Carding (Penggunaan Ilegal Kartu Kredit) Sebagai Bentuk Cybercrime"*, Jurnal Hukum-USU, 2018, hlm. 25.

[24] Budi Suhariyanto, *op.cit.*, hlm. 42.

sistem *wiretapping*, pelaku kejahatan siber bisa mendapatkan sejumlah data serta bisa menimbulkan jumlah kerugian yang tinggi. Tetapi kejahatan *wiretapping* ini belum ada di Indonesia.

b. *Phishing*

Merupakan kejahatan *carding* dengan modus penipuan menggunakan *email* untuk mendapatkan data pribadi korban. Ada dua modus operandi pada kejahatan *carding* ini, pertama, yaitu mengirim virus yang bisa merusak sistem komputer. Kedua, mengirim tautan *website* palsu yang menyerupai situs lembaga atau situs perusahaan asli. Di Indonesia *phishing* merupakan jenis kejahatan *carding* yang paling sering terjadi.

c. *Counterfeiting*

Counterfeiting adalah kejahatan *carding* yang dilakukan dengan cara memalsukan kartu kredit menyerupai aslinya. Mulai dari perorangan hingga sindikat yang sudah memiliki keahlian khusus, mempunyai jaringan yang luas dan memiliki dana yang besar melakukan kejahatan *carding* jenis ini. Pada beberapa situs terdapat pemanfaatan *software* yang digunakan secara umum untuk melakukan kejahatan *counterfeiting*. Contohnya adalah dengan menggunakan *software credit master* dan *credit probe*, pelaku dapat memperoleh dengan mudah nomor yang tertera pada kartu kredit korban dan menggunakan alat bantu mesin atau terminal yang dicuri dan telepon genggam untuk mengecek keaslian nomor-nomor

tersebut. Selain itu *counterfeiting* juga menggunakan alat berupa *skimming device* yang digunakan untuk menyalin data yang tercantum di *magnetic stripe* kartu kredit asli serta menggunakan peralatan-peralatan untuk meng-*intercept* jaringan telekomunikasi dan juga menggunakan terminal implants.[25]

Terdapat berbagai macam faktor utama penyebab terjadinya *carding* yang sering terjadi. Adapun faktor-faktor tersebut adalah :

a. Akses internet yang tidak terbatas

   Pemanfaatan teknologi internet dapat memungkinkan orang untuk dapat sembarangan dalam memanfaatkan teknologi internet dikarenakan kemudahan dan tidak adanya batasan dalam mengakses internet. Tanpa adanya batasan yang mengatur penggunaan internet memberikan kemudahan dan kebebasan setiap orang dalam melakukan berbagai kegiatan dengan memanfaatkan media internet. Informasi yang diberikan pun belum dapat divalidasi kebenarannya. Hal tersebut dapat disalahgunakan untuk melakukan tindak kejahatan tanpa terlacak dan tidak bertanggungjawab.

b. Kelalaian para pengguna internet

   Tindakan ini merupakan penyebab utama terjadinya kejahatan *carding*, para pengguna mulai sekarang harus memiliki kesadaran akan adanya kejahatan *cybercrime* yang mengintai pengguna internet

[25] https://www.google.com/amp/s/m.kumparan.com/amp/berita-hari-ini/kenali-jenis-jenis-carding-cybercrime-yang-menyeret-sejumlah-artis-ibu-kota-1svW5CdEPxu, diakses pada tanggal 1 Desember 2020, pukul 13.10 WIB.

setiap saat. Kesadaran setiap individu yang memanfaatkan fasilitas internet harus mulai ditanamkan akan pentingnya suatu sistem keamanan jaringan komputer agar terlindung dari kejahatan *cybercrime*.

c. Pelaku yang cerdas

Pelaku kejahatan *cybercrime* pada umumnya memiliki tingkat kecerdasan yang tinggi, memiliki tingkat keingintahuan yang tinggi dan memiliki rasa tertarik yang tinggi terhadap teknologi komputer. Pengetahuan para pelaku tentang cara kerja sistem komputer jauh di atas pengguna komputer. Inilah yang seharusnya diatasi terlebih dahulu, minimal para pengguna harus mengetahui tentang sistem keamanan jaringan komputer agar tidak dengan gampang dibodohi oleh para pelaku kejahatan *cybercrime*.

d. Faktor ekonomi

Faktor ekonomi merupakan faktor yang paling sering dijadikan alasan untuk melakukan kejahatan *carding*. Biasanya pelaku memiliki hasrat untuk membeli suatu barang yang diinginkan atau untuk memenuhi kebutuhan sehari-hari tanpa harus mengeluarkan uang karena uang yang dimiliki tidak mencukupi. Alasan utama untuk melakukan tindak kejahatan adalah keadaan ekonomi yang rendah serta dapat memberikan kesempatan bagi pelaku kejahatan.

e. Faktor usia

Para pelaku kejahatan *carding* memilki usia kurang lebih rata-rata 17 sampai 40an tahun karena memiliki kemampuan daya serap tinggi dalam menyerap suatu pengetahuan dan informasi.

f. Faktor penegak hukum

Faktor ini sering menjadi salah satu penyebab maraknya suatu kejahatan. Dilatarbelakangi oleh kurangnya pengalaman dalam menangani kejahatan yang berhubungan dengan kartu kredit oleh para penegak hukum. Secara umum hal ini terjadi karena penyidik kurang menguasai dalam hal penggunaan komputer serta sulitnya dalam hal pembuktian mengingat kasus *carding* terjadi di dunia maya.

g. Lemahnya sistem pengawasan bank

Kemajuan teknologi informasi mengharuskan lembaga perbankan untuk terus bergerak mengikuti perkembangan kejahatan yang dilakukan di dunia maya yang bertujuan agar nasabah memiliki rasa aman dan nyaman untuk bertransaksi secara *online*. Pihak bank harus terus meningkatkan kemampuannya secara berkesinambungan agar dapat mendeteksi potensi kejahatan *carding* itu sendiri.[26]

Kejahatan *carding* dilakukan secara perorangan maupun berkelompok. Modus operandi *carding* terdiri dari beberapa bagian, mulai dari penentuan titik lokasi akses internet, target korban, pencarian kartu kredit yang akan digunakan,

[26] nedr005.wordpress.com/penyebab-terjadinya-carding/, diakses pada tanggal 14 Desember 2020, pukul 20.03 WIB.

teknik *order*, mengakali pengamanan yang digunakan oleh korban, konfirmasi, pengambilan barang dan penjualan.[27]

Untuk mendapatkan data kartu kredit dapat dilakukan dengan berbagai cara, antara lain :

a. *Chatting*, adalah cara yang ampuh untuk memperoleh nomor kartu kredit dilakukan dengan cara saling berbincang dan bertukar nomor kartu kredit.
b. *Bill* atau tagihan kartu kredit. Mencari tagihan kartu kredit dari tong sampah atau dapat terjadi pihak toko (*merchant*) ataupun kasir yang memegang salinan dari *bill* dan menyalin nomor kartu kredit bisa juga menggunakan suatu alat untuk merekam data yang ada di pita magnetik kartu kredit.
c. Jebakan hadiah yang sering digunakan untuk mengajak korban dengan cara korban menyebutkan nomor kartu kredit miliknya. Cara yang dilakukan adalah menelepon atau mengirim pesan singkat pada korban. C*arder* akan menanyakan nomor yang tertera pada kartu kredit yang asli dan menjebak pemilik kartu kredit tersebut.
d. Mencuri data melalui perangkat telepon. Seperti menelepon korban dan memberikan informasi bahwa penggunaan kartu kredit sudah mencapai *limit* yang ditentukan oleh bank selaku penerbit kartu kredit. Akhirnya korban saat itu juga langsung mengajukan keluhan dan kesempatan tersebut langsung digunakan oleh penelepon untuk

[27] Budi Suhariyanto, *op.cit.*, hlm. 37.

meminta nomor kartu kredit beserta data pribadi korban untuk dicek di databasenya.

e. Kartu kredit korban diperoleh dengan cara menggunakan perangkat *surveillance*. Dengan masuk ke database milik penyedia layanan internet atau situs komersial adalah cara lain untuk mendapatkan nomor kartu kredit dengan jumlah yang banyak.[28]

f. *Sniffer* merupakan cara yang paling ampuh untuk memperoleh informasi data korban. Mendapatkan data yang dikirim oleh *website e-commerce* yang sudah diincar dengan memanfaatkan program yang memiliki fungsi melihat atau membuat *logging file* dari data yang dikirim tersebut. Untuk melakukan tindak kejahatan ini *carder* mengincar situs yang tidak memiliki tingkat keamanan yang baik.

g. Membuat virus komputer seperti yang berguna sebagai *keylogger* (*keyboard logger* yaitu program yang memiliki fungsi untuk mengamati aktifitas *keyboard*) dan virus ini dikirim melalui *email spamming*, *chatting*, *messenger* (*yahoo, MSN*) maupun di situs tertentu, *netter* akan tertarik untuk mengunduh dan membuka file tersebut. *Keylogger* mencatat semua aktifitas komputer korban dalam sebuah *file* dan akan mengirim *file* tersebut ke *email hacker*. Ketika korban masuk ke situs yang dibuat oleh *hacker* program ini akan berfungsi sebagaimana mestinya.

[28] *Ibid*., hlm. 89.

h. Membuat situs *phising*, merupakan situs palsu yang mirip dengan aslinya yang dibuat oleh *carder*. Situs *www.klikbca.com* adalah contoh yang paling sering terjadi di Indonesia.

i. Mencuri semua data langsung ke situs *e-commerce*. Cara ini terbilang sulit karena para *hacker* menggunakan metode *injection* (situs/*server* akan menjalankan sebuah *script*) diperuntukkan untuk situs yang memiliki sistem keamanan jaringan. Biasanya cara ini dilakukan oleh *hacker* yang sudah berpengalaman untuk melakukannya. Cara *injection* yang paling umum digunakan adalah *html injection* dan *SQL injection*. Diperuntukkan bagi situs yang tidak memiliki *security* atau *firewall*.[29]

Untuk alur proses transaksi menggunakan kartu kredit yang dijadikan sebagai objek pelanggaran kejahatan *carding*, antara lain :

a. *Source of applications* adalah kejahatan yang dilakukan dengan cara melakukan *fraud application*.

b. *Application processing* adalah kejahatan dengan cara melakukan *fraud application*.

c. *Card embossing and delivery (courier, recipient or customer)* yaitu melakukan kejahatan dengan cara menggunakan kartu kredit yang asli yang tidak diterima.

d. *Usage* adalah kejahatan dilakukan dengan cara pemalsuan.

[29] http://gank.vspweb.com, diakses pada tanggal 5 Desember 2020, pukul 21.57 WIB.

e. *Payment to merchant* yaitu kejahatan terjadi pada saat melakukan transaksi dengan merchant.[30]

Ruang lingkup dalam pelaksanaan kejahatan *carding* antara lain :

a. *Carder*

Carder merupakan pelaku kejahatan *carding*, dalam melancarkan aksinya *carder* menggunakan *email*, *banner* ataupun *pop-up window* untuk mengelabuhi *netter* agar masuk ke situs palsu, *netter* akan memberikan informasi data pribadinya. Teknik yang sering digunakan para *carder* dalam aksinya adalah membuat *website* dan *email* palsu atau yang biasa disebut dengan *phising* yang bertujuan untuk memperoleh informasi calon korban seperti nomor kartu kredit, *PIN (Personal Identification Number)*, atau kata sandi. Kemudian *carder* melakukan pencocokan *PIN* atau kata sandi setelah mendapatkan informasi dari korban yang akhirnya dapat melakukan transaksi dari kartu kredit tersebut. Target *carder* adalah pengguna layanan internet yang ceroboh ketika melakukan transaksi secara *online* seperti pengguna layanan internet banking atau situs-situs iklan, jejaring sosial, *online shopping* dan sejenisnya. *Carder* mengirim *email* ke korban dengan tujuan mengubah *user ID* dan *PIN* korban melalui internet. Pihak resmi seakan-akan mengirim *email* tersebut menyerupai aslinya, sehingga seringnya para korban tidak menyadari bahwa *email* tersebut palsu. *Carder* menggunakan

[30] Budi Suhariyanto, *op.cit.*, hlm. 88.

kecanggihan teknologi internet dengan tujuan menimbulkan kerusakan pada lalu lintas mayantara (*cyberspace*) demi terwujudnya tujuan untuk mengambil keuntungan dengan cara merugikan orang lain disamping membuat dan menerima informasi tersebut.

b. *Netter*

Netter merupakan pengguna internet yang adalah penerima *email* yang dikirim oleh para *carder*.

c. *Cracker*

Mencari keuntungan dan memiliki kepentingan pribadi adalah tujuan utama *cracker* dalam melakukan tindak pidana, dilakukan dengan cara memasuki dan mencari kelemahan pada sistem, dari perbuatannya tersebut seperti mencuri data, penghapusan, penipuan dan lain sebagainya.

d. Bank

Bank merupakan badan hukum yang bertugas untuk menyimpan dana dari masyarakat dan menyalurkan dana simpanan tersebut dalam bentuk kredit dan bentuk-bentuk lainnya untuk meningkatkan serta menyejahterakan hidup orang banyak. Bank adalah pihak yang memberikan fasilitas kartu kredit dan juga pihak yang menerbikan kartu debit dan merupakan pihak penyelenggara transaksi *online*, *e-commerce*, internet banking dan lain sebagainya.

Ada berbagai cara untuk melakukan kejahatan *carding* antara lain :

a. *Fraud application*

   Memanfaatkan kartu kredit asli yang diperoleh dengan menggunakan aplikasi palsu. Pelaku memalsukan data pendukung dalam proses aplikasi seperti nomor KTP, nomor paspor, rekening koran, surat keterangan penghasilan dan lainnya.

b. *Lost/stolen card*

   Memakai kartu kredit asli hasil curian. Pelaku akan menandatangani *sales draft* sekaligus meniru tanda tangan korban pada kartu kredit pada saat melakukan transaksi. Transaksi dilakukan di bawah *limit* minimal agar tidak ada otorisasi pada saa transaksi berlangsung.

c. *Totally counterfeited*

   Menggunakan kartu kredit yang seluruhnya palsu. Pelaku mencetak kartu tiruan dengan menggunakan data nomor dan pemegang kartu yang masih berlaku dengan melakukan pengaturan ulang sandi dan data baru (*reembossed dan reencoded*).

d. *Record of charge (Roc) pumping*

   Penggandaan *sales draft* yang dilakukan oleh *merchant*. Satu *sales draft* tidak ditandatangani oleh pemilik kartu kredit yang sah dan diserahkan kepada *merchant* lain untuk diisi dengan data transaksi fiktif.

e. *Altered amount*

Merubah nominal transaksi yang ada pada *sales draft* yang dilakukan oleh *merchant*.

f. *Telephone/mail ordered*

Pemanfaatan kartu kredit calon korban dengan cara memesan barang dengan media telepon atau surat dengan menggunakan nomor kartu kredit dan data pribadi pemilik kartu kredit yang sah.

g. Mengubah program *Electronic Data/Draft Capture (EDC)*

Merusak dan merubah program pada alat yang disediakan oleh bank/*EDC* yang dilakukan oleh *merchant*.

h. *Fictius merchant*

Pelaku berperan menjadi pedagang dan mengajukan aplikasi yang disertai dengan data-data palsu.[31]

Ketika melakukan kejahatan *carding*, para *carder* juga sering melakukan cara lain yaitu, setelah *carder* memperoleh data pribadi beserta nomor kartu kredit korban, *carder* akan membelanjakannya di *merchant online* yang diinginkan. Pengiriman barang yang sudah dibeli akan ditujukan ke alamat orang yang dipercaya oleh *carder* yang berlokasi di luar negeri seperti Australia atau Singapura, hal ini dilakukan karena banyaknya *merchant* yang tidak berkenan

[31] Sigid Suseno dan Syarif A. Barnawi, "*Kebijakan Pengaturan Carding Dalam Hukum Pidana Di Indonesia Vol. 6 No. 3"*, Jurnal Sosiohumaniora Fakultas Hukum Universitas Padjajaran, 2004, hlm. 254-255.

mengirimkan barang tersebut ke alamat Indonesia. Setelah itu barang hasil belanja *online* tersebut dikirimkan oleh teman *carder* ke alamat Indonesia.

Carder biasanya menghindari pemesanan dengan jumlah besar terutama untuk merk-merk terkenal dan mahal serta perlunya untuk memperhatikan jumlah barang yang dipesan dalam sekali bertransaksi, karena jika banyak dapat menimbulkan kecurigaan pada pihak *merchant*. Disamping itu para *carder* juga menghindari pembelanjaan dengan fasilitas pengiriman cepat. Hal itu dilakukan untuk menjaga kewajaran dalam penggunaan kartu kredit yang digunakan. Sehingga *merchant online* berpikiran bahwa orang memiliki fasilitas kartu kredit memperhitungkan dana yang digunakan untuk berbelanja.

Ditinjau dari modus operandi tersebut dapat diketahui bahwa *carder* dapat menjangkau para pemilik asli kartu kredit yang ada di belahan negara lain, dimana *carder* berada serta dapat melakukan transaksi menggunakan kartu kredit tersebut secara *online* dengan memanfaatkan kecanggihan teknologi internet. Karena sifat teknologi internet yang tanpa batas ruang dan waktu (*borderless*) sehingga hal tersebut dapat dilakukan.

2.1.2. Kejahatan Dalam Dunia Maya

Salah satu persoalan yang sering muncul dalam kehidupan bermasyarakat adalah kejahatan, yang sudah menjadi istilah yang tidak asing lagi bagi masyarakat. Namun pengertian dari kejahatan itu sendiri bermacam-macam, hal ini dikarenakan pengertian kejahatan itu bersumber dari alam dan nilai kehidupan

masyarakat.[32] Kejahatan mengalami perkembangan sejajar dengan perkembangan masyarakat itu sendiri. Kejahatan dapat merugikan seorang korban secara material maupun inmaterial.

Pada hakikatnya pengertian kejahatan dapat dibedakan menjadi tiga yaitu :

a. Pengertian kejahatan dengan sudut pandang yuridis

   Secara yuridis formal kejahatan merupakan tindakan yang tidak sesuai dengan moral kemanusiaan, merugikan masyarakat, bersifat sosial dan melanggar undang-undang. Di dalam KUHP tidak disebutkan dengan jelas pengertian dari kejahatan itu sendiri, tapi dapat dirumuskan bahwa kejahatan adalah perbuatan yang melanggar perumusan ketentuan-ketentuan KUHP.

b. Pengertian kejahatan sudut pandang sosiologis

   Secara sosiologis kejahatan adalah tingkah laku manusia yang berasal dari masyarakat itu sendiri, atau juga bisa disebut dengan kejahatan adalah segala bentuk ucapan, perbuatan, perilaku yang merugikan masyarakat, yang melanggar norma-norma susila dan menyerang keselamatan masyarakat itu sendiri.

c. Pengertian kejahatan dengan sudut pandang kriminologis

   Secara kriminologis kejahatan merupakan segala perbuatan manusia yang merugikan orang lain dan berakibat adanya korban perorangan maupun kelompok atau golongan-golongan masyarakat.[33]

---

[32] J.E Sahetapy, *Kriminologi dan Masalah Kejahatan*, Citra Aditya Bhakti, Bandung, 1982, hlm. 3.

[33] Topo Santoso, *Kriminologi*, Raja Grafindo Persada, Jakarta, 2001, hlm. 100.

Untuk menyebut suatu perbuatan adalah sebuah kejahatan, ada unsur-unsur pokok yang harus dipenuhi dalam suatu tindak kejahatan yaitu :

a. Adanya perbuatan yang menimbulkan sebuah kerugian;
b. Kerugian tersebut telah diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP);
c. Ada perbuatan (*criminal act*);
d. Ada maksud jahat (*criminal intent*);
e. Ada peleburan antara maksud jahat dan perbuatan jahat;
f. Harus ada perbaruan antara kerugian yang sudah diatur di dalam KUHP dengan perbuatan;
g. Terdapat sanksi pidana yang mengancam perbuatan tersebut.[34]

Kejahatan merupakan masalah utama dalam kehidupan manusia meskipun sudah ditetapkan sanksi yang mengatur jika ada seseorang melakukan kejahatan maupun pelanggaran yang tertulis dalam undang-undang. Semakin lama kejahatan semakin meningkat di kota-kota besar maupun kecil, tidak memandang status sosial korban, tidak peduli dengan waktu terjadinya kejahatan bahkan semakin hari modus kejahatan semakin beragam, sejajar dengan perkembangan teknologi yang semakin menunjang kehidupan manusia.

Kemajuan zaman dan perkembangan teknologi adalah hal yang tidak mungkin dipisahkan dari kehidupan manusia pada saat ini. Semakin maju suatu zaman, semakin berkembang pula teknologi yang digunakan. Perkembangan zaman turut serta mengubah perilaku masyarakat dan peradaban manusia secara global. Kemajuan teknologi dan ilmu pengetahuan memberikan dampak positif serta negatif dalam implementasinya. Perkembangan teknologi yang begitu cepat

[34] A.S Alam, *Pengantar Kriminologi*, Refleksi, Makassar, 2010, hlm. 18.

telah memberikan banyak kemudahan bagi manusia dalam melakukan setiap aktifitas khususnya dalam hal pekerjaan. Tetapi perkembangan teknologi juga memiliki dampak negatif jika seseorang memanfaatkan kecanggihan teknologi untuk melakukan suatu kejahatan.

Internet adalah hasil dari perkembangan teknologi yang memanfaatkan komputer sebagai sarana utama dalam pengoperasiannya. Internet memberikan kemudahan dalam berkomunikasi maupun dalam mengelola suatu bisnis. Seiring berjalannya waktu banyak juga ditemukan kejahatan dengan memanfaatkan media internet. Akibat kemajuan teknologi muncul salah satu permasalahan yaitu lahirnya kejahatan-kejahatan yang bersifat baru, khususnya kejahatan dengan memanfaatkan internet sebagai alat pendukung agar terlaksananya kejahatan tersebut[35], yang dikenal dengan istilah *cybercrime* (kejahatan dunia maya).

Pada dasarnya kejahatan siber (*cybercrime*) merupakan kegiatan yang menggunakan kecanggihan komputer dan kemajuan teknologi internet dengan sistem telekomunikasi dengan menggunakan gelombang radio aktif. Beberapa berpendapat bahwa identifikasi kejahatan siber adalah *computer crime*. Kejahatan dunia maya muncul berdampingan dengan kemajuan teknologi komunikasi dan informasi. Dalam beraktifitas cara pandang pelaku bisnis telah berubah dengan adanya perkembangan teknologi komunikasi dan informasi. Pada zaman modern saat ini kecepatan, kerahasiaan dan ketepatan adalah hal yang tidak bisa dipisahkan dalam kehidupan manusia.

---

[35] Mansur, Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005, hlm. 22.

Berikut adalah pengertian *cybercrime* menurut para ahli :

a. Menurut Wahid dan Labib, *cybercrime* adalah berbagai bentuk pemanfaatan jaringan komputer untuk melakukan tindak kriminal dan atau kejahatan yang menyalahgunakan kemudahan teknologi digital.
b. Menurut Widodo, *cybercrime* adalah kejahatan yang dilakukan dengan memanfaatkan media komputer yang pelakunya mulai dari satu orang, sekelompok orang, maupun badan hukum, atau kejahatan yang menggunakan media komputer sebagai sasaran. Kejahatan tersebut adalah jenis-jenis perbuatan yang tidak sesuai dengan peraturan perundang-undangan, yang berarti melawan hukum secara material maupun melawan hukum secara formal.
c. Menurut Organization of Europan Community Development (OECD), *cybercrime* atau kejahatan komputer adalah seluruh pengoperasian secara illegal atau tidak sah terhadap suatu data elektronik milik orang lain. Sehingga terlihat bahwa kejahatan merupakan segala kegiatan illegal dalam suatu sistem komputer.[36]

Dapat diketahui bahwa *cybercrime* tidak mengenal territorial negara maupun waktu karena korban dan pelaku berada di negara yang berbeda. Semua aksi *cybercrime* dapat dilakukan tanpa adanya orang lain yang bisa menjadi saksi mata dan memanfaatkan akses internet dengan media komputer, yang akhirnya

[36] Pengertian, Bentuk dan Tindak Pidana Cyber Crime, https://www.kajianpustaka.com/2018/03/pengertian-nentuk-dan-tindak-pidana-cyber-crime.html?m=1, diakses pada tanggal 11 November 2020, pukul 19.01 WIB.

kejahatan *cybercrime* adalah kejahatan antar negara (*transnational crime*) yang pengungkapannya melibatkan banyak negara. Mulai dari pelaku kejahatan, korban, tata cara dan tempat kejadian perkara memiliki perbedaan dengan kejahatan pada umumnya yang merupakan karakteristik dari *cybercrime*.[37]

Karakteristik *cybercrime* adalah penggunaan komputer yang didukung oleh teknologi digital. Beberapa karakteristik kejahatan *cybercrime,* yaitu :

a. Tindakan illegal, tidak berhak atau tindakan tidak etis yang terjadi di dunia maya, sehingga tidak dapat ditentukan yurisdiksi negara bagian mana yang berlaku untuk pelaku maupun korban;
b. Tindakan ini dilakukan dengan menggunakan peralatan yang berkaitan dengan internet;
c. Tindakan-tindakan ini menghasilkan kerugian material atau immaterial yang memiliki kecenderungan lebih besar dari kejahatan konvensional;
d. Para pengguna internet dan aplikasinya adalah pelaku utama kejahatan *cybercrime*;
e. Tindakan-tindakan ini sering dilakukan secara transnasional.[38]

Pada dasarnya, kejahatan siber merupakan kegiatan yang memakai media komputer atau bisa dikatakan media yang kompatibel dengan sistem telekomunikasi, baik menggunakan telepon atau menggunakan antena nirkabel.

---

[37] https://jurnal.usu.ac.id/index.php/jmpk/article/viewFile/8413/3651 diakses pada tanggal 20 Oktober 2020, pukul 19.19 WIB.

[38] Abdul Wahid dan M. Labib, *Kejahatan Mayantara (Cybercrime)*, Refika Aditama, Jakarta, 2009, hlm. 76.

Disimpulkan bahwa kejahatan dunia maya merupakan bentuk kejahatan tradisional dengan bantuan komputer dan merupakan suatu jenis kejahatan yang memanfaatkan jaringan komputer dan merugikan penggunanya.

Adapun jenis-jenis kejahatan yang termasuk dalam *cybercrime* yaitu :

a. *Identity Theft*

   Adalah jenis *cybercrime* berupa aksi pencurian identitas yang dilakukan dengan cara meretas *website* korban. Server *website* diakses oleh peretas untuk memperoleh informasi pribadi yang tersimpan. *Identity theft* terjadi pada saat korban mengakses situs abal-abal milik peretas dan korban memberikan data pribadi miliknya.

b. *Carding*

   Carding adalah jenis *cybercrime* berupa pembobolan kartu kredit. Pelaku mencuri data informasi kartu kredit dan digunakan untuk keperluan pribadi. Cara yang dilakukan pelaku dalam *carding* yaitu dengan *phising*, memasang *malware* ataupun membeli informasi.

c. *Cyber Extortion*

   Modus operandi *cyber extortion* adalah pelaku akan meminta tebusan untuk data yang telah dicuri. Kejahatan *cybercrime* ini bisa menimpa individu maupun perusahaan. Kasus *cyber extortion* yang sering terjadi adalah pemanfaatan *ransomware*. *Malware* akan masuk ke perangkat komputer korban dan mengendalikan data-data

di dalamnya. Data tersebut tidak dapat diakses oleh pemilik tanpa menggunakan *password* yang dibuat oleh pelaku.

d. *Hacking*

Hacking merupakan kejahatan dengan mengoperasikan sistem komputer milik orang lain secara illegal. *Hacker* melakukan perusakkan sistem, pencurian data pribadi, hingga menyebarluaskan data pribadi yang didapatkan ke orang lain yang tidak berhak dengan keterampilan yang dimiliki. Keuntungan finansial bukanlah hal utama untuk melakukan aksi tersebut. Rata-rata *hacker* melakukan aksinya tersebut hanya untuk menunjukkan kepintaran yang dimiliki.

e. *Spamming*

Spamming adalah suatu tindak penipuan dengan cara mengirimkan iklan atau surat elektronik yang berisi hal yang tidak sesuai dengan fakta yang ada. Biasanya korban akan disuruh untuk mengirimkan uang dengan jumlah tertentu kepada pengirim pesan *spam*.

2.2. Pengaturan *Carding* Dalam Hukum Positif

2.2.1. Pengaturan Kejahatan *Carding* Berdasarkan Kitab Undang-Undang Hukum Pidana

Sebelum adanya UU ITE pasal KUHP digunakan oleh para penegak hukum di Indonesia untuk menangkap pelaku kejahatan *carding* sehingga menyulitkan penegak hukum dalam hal pembuktian. Dalam menangani kasus *cybercrime* para penegak hukum melakukan upaya penafsiran ke dalam perundang-undangan KUHP dan khususnya undang-undang yang berhubungan

dengan perkembangan teknologi informasi. Untuk melakukan penafsiran hukum yang berhubungan dengan teknologi informasi khususnya *cybercrime* terdapat beberapa ketentuan hukum positif yang dapat dipraktekkan secara langsung. Cara yang dilakukan untuk penafsiran hukum adalah dengan cara penafsiran *eksentif* (perumpamaan dan perasaan) dan analogi. Upaya tersebut dilakukan untuk pengaturan dalam menangani kasus *cybercrime* khususnya kejahatan *carding*. Di dalam KUHP terdapat beberapa pasal yang mengkriminalisasi *cybercrime* dengan menggunakan metode *interpretasi ekstensif* terhadap pasal-pasal pada KUHP.

Metode penafsiran hukum oleh aparat hukum menjadi hal yang logis untuk menghindari terjadinya kekosongan hukum dalam suatu perkara tindak kejahatan khususnya tindak kejahatan yang berhubungan dengan teknologi informasi. Untuk mengatasi tindak pidana *cybercrime* terdapat beberapa peraturan perundang-undangan yang digunakan pada saat menerapkan ketentuan hukum positif sebelum adanya UU ITE.

Kitab Undang-Undang Hukum Pidana Indonesia belum mengatur yurisdiksi hukum untuk tindak kejahatan yang terjadi di dunia maya sehingga akan berdampak pada perlindungan hak-hak pribadi (*privacy right*) seseorang.[39] Di dunia maya perlindungan hak pribadi erat hubungannya dengan data pribadi seseorang (*personal data*) karena pada zaman ini perkembangan teknologi dengan internet mengalami kemajuan yang sangat pesat sehingga orang yang tidak

[39] Ahmad M. Ramli, *Perencanaan Hukum Nasional Bidang Teknologi Informasi dan Komunikasi*, Badan Pembinaan Hukum Nasional Republik Indonesia, Jakarta, 2009, hlm. 45.

berkepentingan dapat mengakses secara tidak bertanggungjawab atas informasi data pribadi seseorang tanpa sepengetahuan pihak yang bersangkutan.[40]

Semakin pesatnya perkembangan teknologi informasi, maka perlu diperhatikan upaya penyempurnaan dan perbaikan dalam Kitab Undang-Undang Hukum Pidana, yaitu :

a. Semakin banyaknya kejahatan-kejahatan baru karena kemajuan teknologi informasi, alat bukti yang mendukung suatu tindak kejahatan harus memiliki tingkat kesesuaian yang sama dengan perkembangan ilmu pengetahuan dan teknologi (IPTEK), dengan menambahkan jenis alat bukti yang berbasis teknologi, seperti surat elektronik (*email*) dan rekaman elektronik.
b. Pemanfaatan jaringan telematika (telekomunikasi, media dan informatika) *global* merupakan salah satu ciri dari kejahatan *cybercrime*. Kejahatan *cybercrime* memilki karakteristik tanpa batas yang berarti pelaku, korban dan tempat terjadinya tindak pidana (*locus deliti*) bisa terjadi antar negara. Oleh karena itu, pemberlakuan Kitab Undang-Undang Hukum Pidana harus diperluas kembali untuk mengantisipasi kejahatan *cybercrime*.
c. Untuk mengidentifikasi dan menilai perbuatan-perbuatan yang dapat dikenai sanksi pidana dalam perkembangan zaman yang bergerak cepat bukanlah hal yang mudah. Untuk menjerat pelaku *cybercrime* para aparat penegak hukum menggunakan lembaga penafsiran

[40] Miller et al, *Law for E-commerce*, hlm. 233.

hukum (*interpretasi*). Hal ini dimaksudkan untuk menghindari timbulnya kekosongan hukum.[41]

KUHP sebenarnya belum mengatur secara tegas mengenai kejahatan *carding*, akan tetapi *carder* tidak serta merta dapat lolos dari jerat hukum atas perbuatan yang dilakukan. Pengaturan mengenai kejahatan *carding* diatur secara tersirat menurut KUHP, yang berarti tidak secara spesifik, namun dikaitkan pada perbuatannya secara umum, seperti halnya pada pencurian.

Meskipun belum adanya regulasi khusus yang mengatur tentang tindak pidana kejahatan *carding*, maka kejahatan tersebut akan diatur oleh hukum non elektronik yang berlaku. Penjatuhan hukuman pelaku *carding* dengan pasal KUHP dimungkinkan, hanya saja perlu digunakan penafsiran ekstensif yang dilakukan oleh aparat penegak hukum karena KUHP saat ini berlaku pembentukannya ditujukan untuk mengatur perbuatan yang nyata.

Adapun pasal-pasal dalam KUHP yang mengkriminalisasi kejahatan dunia maya yaitu :

a. Pasal 362 KUHP untuk kasus *carding* yang mana pelaku hanya mencuri nomor kartu kredit milik orang lain untuk melakukan belanja *online* di *e-commerce*.
b. Pasal 378 KUHP untuk penipuan dengan modus menawarkan dan menjual barang dengan cara memasang iklan di sebuah situs sehingga menarik orang untuk membeli barang tersebut.

[41] Sofwan Jannah dan Naufal, "*Penegakkan Hukum Cyber Crime Ditinjaui Dari Hukum Positif dan Hukum Islam"*, Jurnal Hukum Vol. 2 No. 1, 2012, hlm. 77.

c. Pasal 335 KUHP untuk kasus pengancaman dan pemerasan yang dilakukan dengan media *email*.

d. Pasal 331 KUHP untuk kasus dengan modus pencemaran nama baik dengan memanfaatkan media internet. Pelaku mengirimkan email secara berantai untuk menyebarkan kebohongan melalui *mailing list (millis)*.

e. Pasal 303 KUHP dikenakan untuk menjerat pelaku permainan judi *online* dengan penyelenggara berasal dari Indonesia.

f. Pasal 282 KUHP untuk kasus penyebaran pornografi maupun situs porno yang beredar banyak di internet.

g. Pasal 282 dan 311 KUHP untuk kasus dengan modus menyebarkan foto atau film koleksi pribadi seseorang yang vulgar.

h. Pasal 378 dan 262 KUHP untuk kasus *carding*, yang mana pelaku melakukan penipuan dengan modus seolah-olah akan membeli sebuah barang dan pembayaran dengan memanfaatkan kartu kredit yang merupakan hasil curian.

i. Pasal 406 KUHP untuk kasus menghapus atau mengubah suatu *website*, pelaku memasuki *website* korban selanjutnya mengubah tampilan *website* tersebut.[42]

[42] Petrus Reinhard Golose, "*Perkembangan Cybercrime dan Upaya Penanggulangannya di Indonesia Oleh Polri"*, Bulletin Hukum Perbankan dan Kebanksentralan, Vol 4 Nomor 2, Jakarta, 2006, hlm. 38-39.

Kecanggihan teknologi komputer dan internet berkembang seiring perkembangan zaman yang berakibat berkembang pula modus kejahatan yang menghasilkan tindak pidana yang dirasa dulu tidak mungkin, dampaknya dirasakan diluar yuridiksi Indonesia. Maka dari itu penerapan pasal-pasal KUHP dirasa sudah tidak lagi sesuai untuk menangani tindak pidana teknologi informasi terlebih tindak pidana *cybercrime*.

2.2.2. Pengaturan Kejahatan *Carding* Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Indonesia belum memiliki hukum yang secara spesifik mengatur tentang kejahatan *carding*. Hingga saat ini permasalahan *e-commerce* dan *carding* memang sudah diatur di UU ITE, tetapi belum mencakup secara keseluruhan perbuatan maupun aktifitas yang dilakukan di dunia maya, tetapi dirasa sudah cukup untuk menjadi acuan dalam penanganan kejahatan *carding*.

Sebuah sistem elektronik di dalam UU ITE tentang perlindungan data pribadi mencakup pengaksesan secara illegal, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari penggunaan dan interferensi illegal. Pasal 26 UU ITE tentang perlindungan data pribadi dari pengaksesan secara tidak sah mengisyaratkan bahwa penggunaan data pribadi dalam media elektronik harus mendapatkan persetujuan dari pemilik data yang bersangkutan. Bagi pelanggar yang melanggar ketentuan tersebut dapat dituntut atas kerugian dari perbuatan tersebut.

Pasal 30 sampai Pasal 33 dan Pasal 35 mengatur tentang perlindungan data yang masuk ke dalam Bab VII mengenai Perbuatan Yang Dilarang. UU ITE

secara tegas melarang adanya pengaksesan sistem elektronik dan penerobosan sistem keamanan guna memperoleh informasi data pribadi milik orang lain. Perbuatan tersebut adalah perbuatan ilegal yang memiliki sanksi tegas bagi pelanggarnya. Penyapadan (*interception*) adalah perbuatan melawan hukum kecuali perbuatan tersebut dilakukan untuk upaya hukum oleh pihak berwajib yang memiliki ijin untuk melakukan penyadapan.

Di dalam UU ITE juga diatur untuk tidak membuka informasi orang lain dengan maksud apapun bahkan jika ada data rahasia. Perlindungan terhadap data tidak hanya mengatur akses pembukaan data saja, tetapi apabila data dapat dibuka dan diubah dengan cara apapun (manipulasi, perubahan, penghilangan, perusakkan) sehingga data tersebut mirip seperti aslinya. UU ITE juga melarang adanya tindakan yang mengakibatkan terganggunya sistem elektronik secara sistematis yang dapat menyebabkan terganggunya akses data bagi penggunanya. Perlindungan data bukan hanya tentang kerahasiaan data seseorang tetapi juga menyangkut tentang keamanan terhadap sistem elektronik dimana data tersimpan dan digunakan sebagaimana mestinya. Melindungi sistem elektronik berarti juga melindungi data itu sendiri.[43]

Jadi undang-undang yang digunakan saat ini dalam mengatur kejahatan *cybercrime* yang di dalamnya termasuk kejahatan *carding* adalah Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

---

[43] Dionysisus Damas Pradiptya, *Pengaturan Perlindungan Data di Indonesia*, Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia http://indocyberlaw.org/?p=313, diakses pada tanggal 10 Desember 2020, pukul 22.11 WIB.

Pasal yang berkaitan dengan *e-commerce* dalam UU ITE adalah Pasal 2, Pasal 9, Pasal 10, Pasal 18, Pasal 20, Pasal 21, Pasal 22, Pasal 46. Pasal 31 ayat (1) dan ayat (2) mengatur tentang *carding* secara langsung, menjelaskan tentang langkah-langkah *carder* dalam memperoleh nomor kartu kredit dengan cara *hacking* untuk menerobos sistem keamanan dan mencuri nomor-nomor kartu kredit.

Pengaturan tentang pencurian diatur di dalam Pasal 32 ayat (2) UU ITE, hal yang mendasar yang diatur dalam KUHP tentang pasal pencurian, yaitu adanya unsur memindahkan suatu barang dari tempat asalnya kepada tempat lain dengan secara illegal atau tidak memiliki hak maupun izin dari pemiliknya. Barang yang dimaksud disini adalah Informasi Elektronik dan atau Dokumen Elektronik kepada Sistem Elektronik.[44]

Pasal 32 ayat (2)

> *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak."*

Dalam hal sanksi pidana terhadap Pasal 32 ayat (2) ditentukan oleh Pasal 48 ayat (2) yang menentukan :

> *"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9*

[44] Budi Suhariyanto, *op.cit.*, hlm. 143.

(sembilan) tahun dan/atau denda paling banyak Rp. 3.000.000.000,00 (tiga milyar rupiah).”

Fokus utama pelaku dalam melakukan tindak kejahatan *cybercrime* adalah memasuki sistem jaringan perusahaan finansial, seperti penyimpanan informasi pribadi kartu kredit, komputer-komputer di bank atau situs-situs belanja *online* yang marak muncul di internet dan diharapkan dapat memberikan keuntungan langsung (uang tunai) maupun keuntungan yang diperoleh dari hasil menjual data kepada pihak ketiga (perusahaan asing).[45]

Jadi hingga saat ini kasus *carding* hanya bisa ditangani dengan ketentuan perundang-undangan lama yaitu dengan menggunakan Pasal 362 KUHP dan Pasal 31 ayat (1) dan (2) UU ITE. Agar di Indonesia kasus *carding* berkurang diperlukan penanggulangan kasus yang memerlukan regulasi khusus yang mengatur tentang kejahatan *carding*. Selain perlunya regulasi khusus juga diperlukan dukungan pengamanan sistem mulai dari perangkat lunak maupun perangkat keras, *guidelines* untuk mengatur kebijakan yang berhubungan dengan kejahatan komputer dan membutuhkan bantuan serta dukungan dari lembaga khusus.

Tindak pidana kejahatan kartu kredit juga diatur dalam Undang-Undang Nomor 11 Tahun 2008 jo Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yaitu pada Pasal 46 ayat (1). Pasal 30 ayat (1) menjelaskan tentang menggunakan atau membuka komputer dan/atau sistem elektronik secara illegal milik orang lain tanpa seizin pemiliknya.

---

[45] *Ibid.*

Maka dari itu perbuatan mengakses informasi elektronik dan menyebarkan informasi elektronik seseorang tanpa seizin pemiliknya dapat dijerat dengan hukuman dengan menggunakan Pasal 30 ayat (1) dengan sanksi pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

Tujuan dari perbuatan dijelaskan pada Pasal 30 ayat (2) Undang-Undang Nomor 19 Tahun 2016 adalah untuk mendapatkan informasi elektronik dan/atau dokumen elektronik. Secara teknis perbuatan yang melanggar dapat dilakukan dengan cara: melakukan komunikasi, mengirimkan, dan dengan sengaja menyebarkan informasi kepada orang yang tidak berkepentingan untuk menerima dan mendapatkan informasi tersebut atau dengan sadar menghalangi supaya informasi tersebut tidak dapat diterima oleh orang yang berhak menerimanya.

Di dalam Pasal 30 ayat (3) Undang-Undang Nomor 19 Tahun 2016 membahas tentang sistem pengamanan dari suatu sistem komputer. Pengertian dari sistem pengamanan yang disebutkan di dalam Pasal 30 ayat (3) adalah sistem yang melarang seseorang untuk memasuki atau mengakses ke dalam komputer atau membatasi akses komputer. Kejahatan yang dilakukan tersebut dilakukan secara sadar maupun tidak sadar, telah melanggar, menerobos, melampaui atau merusak sistem keamanan yang terdapat dalam suatu sistem elektronik yang merupakan sistem yang terdapat pada kartu kredit. Pelaku kejahatan ini dapat dipidana dengan sanksi penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).

Pasal 48 ayat (1) dan ayat (2) membahas tentang besarnya hukuman bagi pelaku kejahatan. Penjelasan Pasal 32 ayat (1) menjelaskan bahwa mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik merupakan cara-cara pelaku dalam melakukan aksi kejahatannya dibidang sistem komputer dan/atau sistem elektronik. Pada ayat (2) terdapat penambahan unsur yaitu memindahkan atau mentransfer dan pengiriman informasi diberikan kepada orang yang tidak berhak.

Pasal 51 ayat (1) dihubungkan dengan Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik membahas tentang pemalsuan data elektronik. Jika pasal ini dikaitkan dengan kejahatan kartu kredit termasuk dalam tindak pidana pemalsuan yang juga diatur dalam Pasal 35 yang terdiri dari dua unsur yaitu, unsur subjektif dan unsur objektif. Unsur subjektifnya adalah dengan sengaja yang berarti adanya subjek hukum yaitu seseorang untuk melakukan sesuatu dengan unsur kesengajaan dalam melakukan perbuatan yang merugikan. Manipulasi, penciptaan, penghilangan, perusakan informasi elektronik dan/atau dokumen elektronik adalah unsur objektifnya dengan maksud agar informasi elektronik dianggap seperti data yang asli, artinya adanya subjek atau orang untuk memenuhi unsur-unsur dengan melakukan perbuatan manipulasi, penciptaan, penghilangan, perusakan suatu informasi dan dokumen elektronik.

Diketahui bahwa karakteristik utama *cybercrime* yang memanfaatkan kecanggihan teknologi sebagai sarana dan memiliki sifat tidak mengenal tempat dan waktu kejadian sedang berlangsung, maka kebijakan kriminalisasi di bidang

teknologi harus memperhatikan perkembangan upaya penanganan kasus *cybercrime* secara menyeluruh secara regional maupun internasional dalam rangka harmonisasi dan uniformitas pengaturan *cybercrime*.[46] Diperlukannya pengkajian beberapa rumusan norma yang terdapat di *European Convention on Cybercrime*, adalah salah satu konvensi yang menjadi alat hukum internasional yang harus dikaji ulang dan menjadi acuan dalam penyusunan norma hukum positif untuk mengurangi kasus *carding* di Indonesia.

Segala macam kegiatan yang dilakukan melalui media elektronik yang juga dikenal dengan ruang siber (*cyberspace*), bersifat virtual, namun dapat disebut sebagai tindakan atau perbuatan hukum yang terjadi secara nyata dan dapat dipertanggungjawabkan secara hukum karena segala macam aktifitas di dunia maya tidak dapat didekati dengan pengukuran hukum konvensional saja sebab akan terdapat kesulitan dan berbagai macam persoalan yang lepas dari pemberlakuan hukum. Kegiatan di dunia maya merupakan kegiatan yang memiliki akibat yang sangat nyata meskipun alat bukti dari kejahatan yang dilakukan bersifat elektronik

Untuk melakukan upaya pencegahan serta pengurangan kasus kejahatan *carding* di Indonesia diperlukan penguatan pada Undang-Undang Nomor 19 Tahun 2016. Hal tersebut dilakukan dengan tujuan untuk mengefektifkan fungsi pencegahan (*preventif*), sehingga kejahatan *carding* tidak lagi timbul.

---

[46] Muhamad Amirulloh, Ida Padmanegara dan Anggraeni, Tyas Dian, "*Kajian EU Convention On Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi, Laporan Akhir Penulisan Karya Ilmiah"*, Jakarta, Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia RI, hlm. 6.