HALREV
Hasanuddin Law Review

Tindak Pidana *Credit/Debit Card Fraud* dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia

The Criminal Offense of Credit/Debit Card Fraud and the Implementation of Its Sanction on Indonesian Criminal Law

Antonius Maria Laot Kian
Sekolah Tinggi Ilmu Hukum Manokwari, Kampus Sanggeng
Jln. Karya ABRI No. 2, Sanggeng, Manokwari, 98312, Papua Barat, Indonesia.
Tel./Fax: +62-986-211585 E-mail: antoniusmarialaotkian@yahoo.com

Submitted: Jan 21, 2015; Reviewed: Mar 7, 2015; Accepted: Mar 26, 2015

Abstract: *The aims of the study are to determine the legal arrangements and the application of criminal sanctions against the crime of credit/debit card fraud in Indonesia. The type of study was a normative research by classifying the provisions relevant to the crime of credit/debit card fraud is based on Law No. 11 Year 2008 concerning Information and Electronic Transactions; otherwise it is used also Convention on Cybecrime 2001. Analysis of legal materials made through a law (statue approach) to create an ius constituendum regarding the application of criminal sanctions against crime credit/debit card fraud. The results of the research indicated that the legal arrangements and criminal sanctions against the crime of credit/debit card fraud in Indonesia is still relatively minimal. First, not integrated article that directly regulates computer related fraud. Second, not arranged in the form of criminal sanctions for actions that are restitutif culprit.*

Keywords: *Criminal Law; Cybercrime; Cyberlaw*

Abstrak: Penelitian ini bertujuan untuk mengetahui pengaturan hukum dan penerapan sanksi pidana terhadap tindak pidana credit/debit card fraud di Indonesia. Metode penelitian yang digunakan adalah penelitian normatif dengan mengelompokan ketentuan-ketentuan yang relevan dengan tindak pidana credit/debit card fraud yaitu berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; selain itu digunakan pula Convention on Cybecrime 2001. Analisis bahan hukum dilakukan melalui pendekatan perundang-undangan (*statue approach*) untuk menciptakan suatu *ius constituendum* mengenai penerapan sanksi pidana terhadap kejahatan credit/debit card fraud. Hasil penelitian menunjukan pengaturan dan sanksi pidana terhadap tindak pidana credit/debit card fraud di Indonesia masih tergolong minim. Pertama, belum dikomodasinya ketentuan yang secara langsung mengatur mengenai *computer related fraud*. Kedua, belum diaturnya sanksi pidana berbentuk tindakan yang bersifat restitutif bagi pelakunya.

Kata Kunci: Hukum Pidana; Kejahatan Siber; Hukum Siber

PENDAHULUAN

Tingkah laku jahat muncul sejak dahulu dan oleh masyarakat dianggap sebagai suatu realitas yang merugikan masyarakat. Giriraj Shah[1] mengemukakan bahwa "*crime is as old as man"*, yaitu bahwa kejahatan seusia dengan peradaban manusia, yang dimulai ketika Adam memakan buah terlarang, yang berakibat dikeluarkannya Adam dan Hawa dari firdaus. Itulah sebabnya Frank Tannenbaum[2] lalu menarik kesimpulan, bahwa "*crime is eternal as eternal its society*", kejahatan itu abadi seabadi masyarakatnya.

Pada prinsipnya, perbuatan-perbuatan yang dianggap jahat selalu bertentangan dengan moral kemanusiaan (*immoral*) atau melukai perasaan susila dalam kehidupan bersama. Dari segi subjek, kejahatan berlawanan dengan perasaan kesusilaan, dan dari segi objek, dalam hal ini masyarakat, perbuatan tersebut merugikan masyarakat, karena kejahatan menyentuh berbagai sendi kehidupan masyarakat. Larry J. Siegel[3] mengemukakan:

> *Crime touches all segments of society. Both the poor and desperate, as well as the wealthy and powerfull, engage in criminal activity. Crime cuts accross racial, class, and gender lines. It involves acts which shock the collective conscience of the nation, and acts which seems relatively harm-less human foibles. Crimes maybe comitted among friends and family members, they can also involve abso-lute strangers.*

Adanya perkembangan manusia dan masyarakat beserta teknologi yang mengikutinya, memunculkan berbagai jenis kejahatan yang sifatnya baru, yang tumbuh dalam berbagai bentuk dan tingkatan secara linear. Salah satu kejahatan yang berkembang sejalan dengan kemajuan masyarakat ialah kejahatan dalam dunia maya (*cybercrime*).

Ian Walden,[4] membagi *cybercrime* dalam kategori *computer-related crime, content-related crime,* dan *computer integrity offences*. Secara umum terdapat beberapa jenis *cybercrime* yaitu *cracking*, *phising, viruses*, *hijacking*, *credit card fraud, online gambling,* dan *attacking military defense*. Di antara berbagai jenis *cybercrime* tersebut, pembobolan kartu kredit (*credit card fraud*) merupakan kejahatan mayantara paling ditakuti dan paling sering terjadi. Dalam terminologi kriminologi, kejahatan *credit card fraud* merupakan suatu tindak pidana.

Secara global, Indonesia merupakan negara dengan tingkat pidana *credit card fraud* tertinggi kedua setelah Ukraina. Kerugian-kerugian akibat *credit card fraud* ini menjadi penyebab munculnya reaksi negatif dari negara-negara lain dalam transaksi bisnis secara *on-line*. Data dari Kepolisian Republik Indonesia menyebutkan bahwa dari rata-rata 200 kasus *cyber crime* yang ditangani, pada umumnya didominasi oleh *credit card fraud* dengan sasaran luar negeri seperti Amerika Serikat, Australia, dan Kanada, dengan pelaku berasal dari kota-kota besar seperti Yogyakarta, Bandung, Jakarta, Semarang, Medan, dan Riau.[5]

Fakta membuktikan bahwa di awal

---

1 Widodo. (2013). *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Aswaja Pressindo, hlm. 36

2 Arief Amrullah. (2006). *Kejahatan Korporasi*. Malang: Bayumedia, hlm. 82

3 Widodo. *Op.cit*., hlm. 43

4 Ian Walden. (2007). *Computer Crime and Digital Investigation*. Oxford: Oxford University Press, hlm. 103

5 Sigid Suseno. (2012). *Yurisdiksi Tindak Pidana Siber.* Bandung: Refika Aditama, hlm. 29

Februari 2008, Kepolisian Republik Indonesia berhasil membongkar sebuah jaringan pemalsuan kartu kredit dan pengedar narkoba berkelas internasional di Semarang. Modus yang digunakan oleh mafia ini adalah *wire tapping*, yakni melakukan penyadapan elekronik lewat telekomunikasi data berupa informasi rahasia seperti nomor kartu kredit, tanggal jatuh tempo dan nama pemiliknya, yang *nota bene* dapat digunakan untuk membuat ribuan kartu kredit palsu yang siap pakai. Hasilnya adalah ditemukannya lebih dari 7.000 kartu kredit palsu ditambah dengan *soft copy* data nasabah berbagai bank di Indonesia. Kejadian tersebut cukup membuat bank-bank penerbit kartu kredit kelabakan dan langsung mengambil tindakan penggantian kartu kredit secara masal.[6]

Beberapa kasus *credit card fraud* yang pernah mencoreng nama baik Indonesia sebagaimana diteliti oleh Sigid Suseno (2013) seperti yang dilakukan oleh Suprihatin binti Lusmanto dan Stevanus Budi Hasmin di Yogyakarta, serta *credit card fraud* yang dilakukan oleh Harry P. Samosir dan Noftan Ladau di Bandung. Atau sebuah kasus *credit card fraud* lainnya, yang dilakukan oleh Rizky Martin alias Steve Rass dan Texanto alias Doni Michael. Keduanya melakukan transaksi pembelian barang atas nama Tim Tamsin Invex Corp, perusahaan yang berlokasi di AS melalui internet. Keduanya menjebol kartu kredit melalui internet banking sebesar Rp. 350 juta. Keduanya telah ditangkap aparat *cybercrime* Polda Metro Jaya pada 10 Juni 2008 di sebuah warnet di kawasan Lenteng Agung, Jakarta Selatan.

Hal lain yang mengejutkan ialah pembobolan tidak hanya dilakukan terhadap kartu kredit, melainkan juga terhadap kartu ATM atau kartu debit, sehingga dapat dikatakan tindak pidan tersebut telah meluas menjadi *debit card fraud*. Pada Januari 2010, Metro TV mengabarkan bahwa terdapat 15 (limabelas) orang nasabah mengadu ke polisi dengan dugaan tentang adanya pembobolan rekening ATM BCA tanpa ada transaksi.[7] Metro TV juga mengabarkan bahwa jumlah nasabah yang mengalami pembobolan ATM sudah berjumlah 20 (duapuluh) orang dalam waktu kira-kira 10 menit.

Rangkaian kejadian pembobolan ATM atau terhadap *debit card* pun terjadi di Jakarta, terutama terhadap nasabah BCA, BNI, BRI, Bank Permata, Bank Mandiri, dan BII. Pakar Informasi dan Transaksi Elektronik (ITE), Ruby Alamsyah menjelaskan bahwa umumnya pembobolan itu dilakukan dengan bantuan *skimmer* dan *spy cam*. *Skimmer* berfungsi menggandakan data yang ada dalam ATM korban dengan menggunakan *magnetic reader*; sedangkan *spy cam* digunakan untuk mendapatkan PIN korban.[8] Berita dari ANTV menyebut juga mengenai *phone banking* (*mobile banking*) yang digunakan sebagai modus untuk membobol uang nasabah di ATM.[9] Bahkan belakangan diketahui bahwa untuk merekam PIN nasabah, para *carder* tidak menggunakan *spy cam* lagi, melainkan menggunakan *pin pad* palsu, yang desainnya sangat mirip dengan *pin pad* asli.

Maraknya tindak pidana *credit/debit card fraud* ini, membutuhkan suatu pen-

[6] Dikutip pada laman website: *http://jabar.go.id.,* diakses pada 24 Oktober 2013.

[7] Source: Metro Hari Ini, 20 Januari 2010

[8] Source: Kabar Malam TV One, 22 Januari 2010

[9] Source: Topik Malam ANTV, 24 Januari 2010

gaturan hukum yang diharapkan mampu mencegah dan mengurangi tindak pidana tersebut. Oleh karena itu, penting kiranya mengelaborasi pengaturan hukum baik implementasi maupun sanksi pidana terkait *credit/debit card fraud* di Indonesia. Berdasarkan analisis tersebut, maka yang dapat menjadi objek kajian dalam tulisan ini adalah bagaimana pengaturan hukum penerapan sanksi pidana terhadap tindak pidana *credit/debit card fraud* Indonesia?

METODE

Penelitian ini menggunakan tipe penelitian hukum normatif. Penelitian berpijak pada konstruksi norma hukum positif (peraturan perundang-undangan), dalam hal ini ketentuan yang relevan dengan tindak pidana *credit/debit card fraud* berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga mengacu pada *Convention on Cybecrime 2001*.

Adapun yang menjadi bahan hukum dalam peneltian ini terbagi atas dua, yaitu bahan hukum primer dan bahan hukum sekunder. Bahan hukum primernya adalah spesifik tentang ketentuan tindak pidana *credit/debit card fraud* dalam UU ITE dan *Convention on Cybecrime 2001*. Sedangkan bahan sekundernya adalah inventarisasi teori-teori hukum yang memiliki hubungan erat dengan legalitas perbuatan *credit/debit card fraud,* sehingga dikualifikasi sebagai perbuatan pidana beserta dengan metode pertanggungjawaban pidananya.

Beberapa pasal dalam peraturan-peraturan tersebut, terutama yang berkaitan dengan kejahatan *carding* akan dianalisis melalui pendekatan perundang-undangan (*statue approach*) untuk menciptakan suatu *ius constituendum* mengenai penerapan sanksi pidana terhadap kejahatan tersebut.

ANALISIS DAN PEMBAHASAN

Pengaturan Hukum Tindak Pidana *Credit Debit Card Fraud* di Indonesia

Menurut Ervina Lerry,[10] dalam tulisan berjudul *The World of Cybercrimes: Carding*, mengemukakan "*credit/debit card fraud covers a wide range of criminal activities involving credit/debit cards*". Selanjutnya disebutkan bahwa, "*Lost or stolen card fraud occurs when someone other than the cardholder uses such card… a similar crime is intercept fraud, in which the card is intercepted either in transit or from a mailbox while on its way from a financial institution to the legitimate customer*".

Ari Juliano Gema,[11] mengelompokkan *credit/debit card fraud* ke dalam kejahatan *Infringements of Privacy*. Disebut demikian karena kejahatan ini ditujukan terhadap informasi yang sangat pribadi dan rahasia dari seseorang yang tersimpan secara *computerized* berupa nomor kartu kredit atau nomor PIN ATM, yang apabila diketahui oleh orang lain maka dapat merugikan korban baik secara materil maupun immateril.

Sebelum diundangkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, penegakan hukum terhadap tindak pidana *credit/debit card fraud* di Indonesia dilakukan melalui Kitab Undang Undang Hukum Pidana (KUHP), yaitu Pasal 263-276 tentang

[10] Source available at: http://abba.vlsm.org, [Diakses pada 21 Januari 2010].

[11] Sumber: http://legalitas.org, [Diakses pada 2 Februari 2011].

Pemalsuan, Pasal 362-367 tentang Pencurian, dan Pasal 378-395 tentang Penipuan. Sejatinya, pasal-pasal ini merupakan antisipasi terhadap kejahatan-kejahatan konvensional, dan agak sulit untuk diterapkan pada kejahatan *cyber*.[12]

Salah satu contoh penggunaan pasal KUHP dalam penyelesaian tindak pidana *credit card fraud* ialah dapat dibaca dalam putusan Pengadilan Negeri Sleman Yogyakarta No. 94/Pid.B/2002/PN. SLMN, tanggal 24 Agustus 2002, di mana Terdakwa Petrus Pangkur (alias Bonny Diobok-obok), yang melakukan tindak pidana *credit card fraud* dijatuhkan hukuman dengan Pasal 378 (Penipuan). Dalam pledoi dinyatakan bahwa tidak adil jika terdakwa dihukum, sementara aturan hukum yang mengatur perbuatan terdakwa dalam hal ini *cybercrime* belum ada aturannya. Namun majelis berpandangan bahwa hakim harus menggali, mengikuti, dan memahami nilai-nilai yang hidup dalam masyarakat. Selain itu, hakim tidak boleh menolak perkara yang diajukan kepadanya seab hukumnya tidak ada atau kurang jelas.

Menurut hemat Penulis, *racio decidendi* putusan *a quo* sudah tepat, dasar argumentasinya bahwa meskipun belum ada hukumnya, suatu perbuatan pidana dapat dikategorikan juga sebagai suatu perbuatan tercela dan ditolak oleh masyarakat bukan saja karena perbuatan tersebut diatur dalam peraturan perundang-undangan (*mala in prohibita*) melainkan juga karena perbuatan tersebut pada dirinya sendiri memang jahat (*mala in se*). Selain itu, dalam catatan Widodo,[13] ada beberapa hal yang patut dicatat mengenai proses peradilan ini, di antaranya:

a. Hakim dapat melakukan terobosan hukum pidana yang cukup spektakuler, karena sudah membuat suatu penafsiran ekstensif, yaitu pengertian mengenai bukti surat sehingga dapat mencakup *e-mail*, terutama dalam menerapkan unsur pemalsuan, meskipun pemalsuan tersebut dilakukan di ruang maya dan antara korban dan terdakwa tidak saling kenal serta tidak saling bertemu. Paradigma hakim ini sangat progresif dan mampu mematahkan anggapan lama bahwa KUHP sudah ketinggalan zaman; hal ini dibuktikan dengan kemampuan menerapkan hukum pidana pada kasus terkait penyalahgunaan teknologi informasi.
b. Majelis hakim hanya membuktikan dan membahas secara detail tentang unsur perbuatan pidana (*criminal act*) yang didakwakan kepada terdakwa, dan tidak banyak mengkaji secara lebih detail tentang unsur pertanggungjawaban pidana (*criminal responsibility*), misalnya seberapa besar unsur kesalahannya, alasan pembenar, alasan pemaaf, dan mengapa perbuatan tersebut dapat terjadi.
c. Dalam pertimbangan untuk pemidanaan, majelis hakim sudah merujuk pada paradigma pemidanaan modern yang menjadikan jenis pidana penjara sebagai alternatif terakhir setelah jenis-jenis pidana yang lain tidak memungkinkan.
d. Majelis hakim hanya mengemuka-kan tentang hal-hal yang bersifat meringankan dan memberatkan secara umum, tanpa didukung oleh saksi ahli atau rujukan ilmiah yang memadai agar penjatuhan pidana selaras dengan kepentingan korban, kepentingan ter-pidana, dan kepentingan masyarakat, serta keadilan.

[12] Widodo. *Loc.cit.*
[13] *Ibid*. hlm. 52.

Meskipun argumentasi di atas dapat dipertanggungjawabkan, namun kebutuhan akan adanya suatu *lex specialis* mengenai *credit/debit card fraud* menjadi suatu urgensi tersendiri mengingat kompleksitas tindak pidana ini tidak dapat disamakan begitu saja dengan kejahatan konvensional lainnya karena hal ini membutuhkan suatu penafsiran hukum yang komprehensif.

Berkaitan dengan hal tersebut, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Masalahnya ialah, dalam kenyataan dewasa ini, kegiatan *cyber* tidak lagi sederhana karena selain bersifat virtual, kegiatannya pun tidak lagi dibatasi oleh teritori atau yurisdiksi suatu negara. Padahal, kerugian dapat saja terjadi baik pada pelaksana informasi dan komunikasi maupun pada orang lain yang tidak terlibat di dalamnya, meskipun berada di dalam atau pun di luar suatu negara.

Dapat dikatakan bahwa meskipun kegiatan dalam ruang *cyber* merupakan kegiatan virtual, dan alat buktinya bersifat elektronik, namun dampaknya sangat nya-ta. Ini berarti, subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara real pula. Para pelaku kejahatan di dunia *cyber* dapat dijerat secara yuridis dalam perspektif ini. Oleh karena itu, ditetapkanlah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang dalam Penjelasannya dite-gaskan "Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (*cyber space*), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata.

Pada tataran yuridis, kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja. Sebab, jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, subjek pelakunya harus dikualifi-kasikan pula sebagai orang yang telah me-lakukan perbuatan hukum secara nyata.

Hal yang patut dicermati dalam UU ITE ialah bahwa pengaturan mengenai *credit/debit card fraud* tidak diakomodasi secara khusus namun diatur berdasarkan *modus operandi* dari tindak pidana tersebut. Padahal apabila dibandingkan dengan *Convention on Cybercrime*[14] yang menjadi sumber materil utama dari undang-undang ini, terdapat perbedaan yang sangat mencolok mengenai pengaturan *credit/debit card fraud*.

Menurut Sigid Suseno[15] bahwa dalam artikel 2-10 CoC diatur tentang hukum pidana materil (*substantive criminal law*) mencakup tindak pidana terhadap kerahasiaan, keutuhan, dan ketersediaan data komputer atau sistem komputer (*illegal access, illegal interception, data interference, system interference, misuse of devise*), tindak pidana yang berkaitan dengan komputer (*computer related forgery* dan *computer related fraud*), tindak pidana yang berkaitan dengan konten (*offences related to child pornography*), dan

[14] Source: CoC, Budapest, 2001.

[15] Sigid Suseno. (2012). *Yurisdiksi Tindak Pidana Siber.* Bandung: Refika Aditama, hlm. 72

tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak-hak terkait (*offences related to infringement of copyright and related rights*). Tindak pidana *credit/debit card fraud* dalam CoC digolongkan dalam tindak pidana *computer related fraud* dalam article 8 CoC menyebutkan:

> *Commited intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion, or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*

Di Indonesia, pengaturan mengenai tindak pidana *credit/debit card fraud* diatur menurut *modus operandi*-nya. Dalam UU ITE, tindak pidana *computer related fraud* yang menjadi domain dari tindak pidana *credit/debit card fraud* diasumsikan didahului oleh beberapa tindak pidana (*modus operandi*), yang diatur dalam beberapa pasal dalam UU ITE, sebagai berikut:

Akses ilegal

Terhadap akses ilegal, diatur dalam 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.

Perbuatan yang dilarang dalam Pasal 30 tersebut memiliki sanksi pidana yang diatur dalam Pasal 46 yang ancaman pidananya berstelsel kumulatif yaitu: (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah); (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah); (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Penyadapan ilegal

Tentang penyadapan ilegal, diatur dalam Pasal 31: (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.

Perbuatan yang dilarang dalam Pasal tersebut memiliki sanksi pidana yang diatur dalam Pasal 47: Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Gangguan terhadap data komputer

Mengenai gangguan terhadap data komputer diatur dalam 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.

Menurut Josua Sitompul,[16] tujuan dari pengaturan mengenai *data interference* atau gangguan terhadap informasi atau dokumen elektronik ialah untuk menjaga kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi atau dokumen elektronik. Tindakan "mengubah" (*alteration*) adalah melakukan modifikasi informasi atau dokumen elektronik asli; di sini terkandung konsep "pengurangan" yaitu membuat informasi atau dokumen elektronik menjadi lebih sedikit dari aslinya dan konsep "penambahan" yaitu membuat informasi atau dokumen elektronik menjadi lebih banyak dari aslinya.

Terkait hal ini, dapat disangkakan bahwa jumlah kartu kredit yang sudah dilipatgandakan menjadi indikasi kemungkinan adanya pengubahan dokumen elektronik asli. Selanjutnya dokumen atau informasi elektronik tersebut dipindahkan dari sistem elektronik asal ke sistem elektronik lain yang tidak berhak. Gangguan terhadap data ini dalam hemat penulis, dapat dimaknai sebagai "perusakan" terhadap data.

Dalam konsep perusakan (*destruction*), dipahami bahwa data original tidak dapat dikembalikan lagi, dan bahkan karakter privasi dari data tersebut dapat berubah menjadi data publik yang dapat diakses oleh siapapun. Dalam penjelasan CoC ditegaskan bahwa:

> *...'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. 'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable. Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.*

[16] Josua Sitompul. (2012). *Cyberspace, Cybercrimes, Cyberlaw, Tinjauan Aspek Hukum Pidana.* Jakarta: Tatanusa, hlm. 81

Perbuatan yang dilarang ini memiliki sanksi pidana sebagaimana diatur dalam Pasal 48, yaitu: (1) Setiap orang yang memenuhi unsur sebagaimana dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.000,- (dua milyar rupiah); (2) Setiap orang yang memenuhi unsur sebagaimana dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp 3.000.000.000,- (tiga milyar rupiah); (3) Setiap orang yang memenuhi unsur sebagaimana dalam Pasal 32 ayat (3), dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 5.000.000.000,- (lima milyar rupiah).

Gangguan terhadap sistem komputer

Mengenai gangguan terhadap sistem komputer diatur dalam 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. Perbuatan yang dilarang ini memiliki sanksi pidana dalam Pasal 49 yaitu: Setiap orang yang memenuhi unsur sebagaimana dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,- (sepuluh milyar rupiah).

Gangguan terhadap sistem elektronik biasanya dilakukan melalui penyebaran virus (*worm-viruses*) dan serangan terhadap sistem atau jaringan komputer (melalui teknik *Denial of Service-DoS Attack* dan *Distributed Denial of Service-DdoS Attack*, termasuk *spamming*. Dalam berbagai kasus *credit/debit card fraud*, pada umumnya terlebih dahulu dilakukan gangguan terhadap sistem komputer melalui *spamming* karena data dan informasi elektronik nasabah berupa PIN dan nomor kartu dapat diketahui melalui teknik ini.

Apabila dianalisis secara saksama, untuk sampai pada kesimpulan bahwa tindak pidana *credit/debit card fraud*, penyidik harus membuktikan terlebih dahulu keempat tindak pidana tersebut di atas, sehingga menimbulkan adanya inefisiensi peraturan. Padahal, dalam CoC, tindak pidana *credit/debit card fraud* diatur dalam satu artikel saja (artikel 8 tentang *computer rlated fraud*. Inefisiensi peraturan dapat menjadi pemicu adanya kekosongan hukum. Asas *lex certa* menegaskan bahwa pengaturan hukum harus jelas dan tidak menimbulkan multitafsir yang diakibatkan oleh inefisiensi peraturan.

Selain mengindikasikan adanya inefisiensi peraturan, penulis berpendapat bahwa terhadap tersangka yang melakukan suatu tindak pidana *credit/debit card fraud* dapat dituntut dengan pasal yang "sangat berlebihan" (*overload indictment/prosecution*). Oleh karena itu, sebagaimana telah diatur dalam artikel 8 CoC, maka UU ITE harus dilengkapi dengan pasal yang secara langsung mengatur mengenai *computer related fraud* sebagai suatu perbuatan yang dilarang sebagai berikut:

> Setiap orang dengan sengaja dan tanpa hak, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum: (a) Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, atau menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik den-

gan cara apapun; (b) Mengganggu sistem elektronik dengan cara apapun, sehingga mengakibatkan hilangnya atau berpindahnya barang atau harta milik orang lain.

Pengaturan hukum mengenai tindak pidana *credit/debit card faud* ini penting untuk dilakukan agar efisiensi peraturan tersebut dalam hukum pidana Indonesia mampu mendukung asas *contante justisia*, yaitu suatu peradilan yang cepat, sederhana, dan biaya ringan.

Penerapan Sanksi Pidana Tindak Pidana *Credit/Debit Card Fraud* di Indonesia

Dalam konsepsi hukum pidana, pemberian sanksi atau pemidanaan merupakan hal yang utama karena suatu perbuatan dapat disebut sebagai tindak pidana apabila mengandung sanksi berupa pemidanaan. Itulah sebabnya sanksi pidana disebut sebagai *ultimum remedium*, yaitu sebagai pilihan terakhir dari semua jenis sanksi pidana. Mengenai hal ini, dalam Pasal 51 Rancangan KUHP dinyatakan bahwa tujuan pemidanaan adalah:

a. Untuk mencegah dilakukannya tindak pidana dengan menegakkan norma hukum dari pengayoman masyarakat;
b. Memasyarakatkan terpidana dengan mengadakan pembinaan sehingga menjadikannya orang baik dan berguna;
c. Menyelesaikan konflik yang ditimbulkan oleh tindak pidana, memulihkan keseimbangan dan mendatangkan rasa damai dalam masyarakat;
d. Membebaskan rasa bersalah pada pidana;
e. Tidak dimaksudkan untuk menderitakan dan tidak diperkenankan merendahkan martabat manusia.

Menurut G. P. Hoefnagels,[17] mengemukakan bahwa "sanksi dalam hukum pidana adalah semua reaksi terhadap pelanggar hukum yang ditentukan oleh undang-undang dimulai dari penahanan tersangka dan penuntutan terdakwa sampai pada penjatuhan vonis oleh hakim." Ini berarti penetapan sanksi dalam hukum pidana merupakan suatu rangkaian kebijakan dalam suatu sistem pemidanaan.

Berkaitan dengan itu, terdapat beberapa teori mengenai tujuan pemidanaan atau pemberian sanksi pidana yang umum diterima dalam hukum pidana, yaitu:

Teori absolut

Berdasarkan teori ini, pemidanaan merupakan pembalasan secara absolut atas kesalahan yang telah dilakukan, yang berorientasi pada perbuatan dan terjadinya kejahatan itu sendiri. Oleh karena itu teori ini disebut juga dengan Teori Pembalasan.[18] Terkait hal ini, secara radikal Hegel menegaskan bahwa karakter pembalasan diartikan sebagai pelenyapan. Oleh karena itu, sejalan dengan pembalasan dalam kategori Hegelian, pembalasan dalam teori ini harus dilihat sebagai suatu reaksi yang keras yang bersifat emosional dan karena itu irasional penjahat.[19]

Melalui teori ini dapat diketahui bahwa pemidanaan diberikan karena orang melakukan kejahatan (*quia peccatum*) dan bukan untuk mencapai tujuan yang lain.[20] Dengan demikian, pemidanaan merupakan suatu retribusi yang adil bagi kerugian yang sudah diakibatkan. Adapun pembagian yang

[17] Teguh Prasetyo. (2010). *Kriminalisasi dalam Hukum Pidana*. Bandung: Nusamedia, hlm. 19

[18] Erdianto Effendi. (2011). *Hukum Pidana Indonesia Suatu Pengantar*. Bandung: Refika Aditama, hlm. 62

[19] Teguh Prasetyo. *Op. Cit.* hlm. 49

[20] Frans Maramis. (2013). *Hukum Pidana Umum dan Tertulis di Indonesia*. Jakarta: PT. RajaGrafindo Persada, hlm. 21

lain mengenai teori ini: *Pertama*, teori pembalasan yang objektif, yaitu berorientasi pada pemenuhan kepuasan dari perasaan dendam dari masyarakat; *Kedua*, teori pembalasan yang subjektif, yaitu berorientasi pada pembuat kejahatan, di mana kesalahan pembuat kejahatanlah yang harus mendapat balasan.[21]

Teori relatif

Teori ini mendasarkan pandangan mengenai maksud atau tujuan dari pemidanaan yaitu untuk perlindungan masyarakat dan pencegahan terjadinya kejahatan. Pemidanaan dilakukan supaya orang jangan melakukan kejahatan (*ne peccatur*).[22] Adapun teori ini terbagi atas:[23] *Pertama, t*eori Prevensi Umum yaitu pencegahan ditujukan kepada masyarakat pada umumnya, untuk menciptakan *psychologische zwang* sehingga masyarakat takut untuk melakukan kejahatan. Dengan kata lain, pemidanaan diberikan dengan tujuan menakuti melalui hukuman yang berat. Termasuk dalam teori ini ialah pemidanaan ditujukan untuk melindungi masyarakat terhadap perbuatan-perbuatan jahat melalui pengasingan terhadap penjahat; Kedua, teori Prevensi Khusus yaitu pencegahan ditujukan kepada orang yang melakukan kejahatan supaya tidak lagi melakukan kejahatan. Dalam teori ini terdapat unsur reparasi atau memperbaiki pribadi penjahat.

Teori penyatuan/integratif

Termasuk dalam kelompok ini ialah pandangan Grotius yang mengatakan bahwa secara kodrat, siapapun yang melakukan kejahatan akan terkena derita (aspek absolut), namun dalam menetapkan berat ringannya derita yang dikenakan tergantung pada kemanfaatan sosial.[24]

Sejalan dengan teori-teori pemidanaan tersebut, Frans Maramis[25] menyebutkan bahwa sanksi dalam hukum pidana dibedakan atas sanksi pidana (*straf*) dan tindakan (*maatregel*). Sanksi pidana bersumber pada ide dasar mengapa diadakan pemidanaan, sedangkan sanksi tindakan bertolak dari ide dasar untuk apa diadakan pemidanaan itu.[26] Apabila dikaji, fokus sanksi pidana ditujukan pada perbuatan salah yang dilakukan seseorang melalui pengenaan penderitaan istimewa (*bijzonderleed*) agar muncul efek jera (unsur pembalasan), juga bersifat mencela perbuatan pelaku; sedangkan fokus sanksi tindakan lebih terarah pada upaya memberi pertolongan pada pelaku agar ia berubah (aspek kuratif/reparasi).

Terkait hal di atas, dibutuhkan keseimbangan antara sanksi pidana dan sanksi tindakan, antara *punishment* dan *treatment*, karena menurut Albert Camus sebagaimana dijelaskan Teguh Prasetyo,[27] pelaku kejahatan meskipun berlaku sebagai *human offender*, namun sebagai manusia, ia tetap bebas mempelajari nilai baru dan adaptasi baru yang bersifat mendidik. Inilah inti dari *double track system* dalam pidana, di mana kesetaraan kedudukan antara sanksi pidana dan sanksi tindakan sangat bermanfaat untuk memaksimalkan penggunaan kedua sanksi

[21] Fuad Usfa. (2004). *Pengantar Hukum Pidana.* Malang: Universitas Muhamadiyah Malang Press, hlm. 56

[22] Jan Remmelink. (2003). *Hukum Pidana*. Jakarta: Gramedia Pustaka Utama, hlm 42

[23] Frans Maramis. *Op.Cit,* hlm. 20

[24] *Ibid.,* hlm. 74

[25] *Ibid*., hlm 79

[26] Sholehuddin. (2003). *Sistem Sanksi dalam Hukum Pidana: Ide Dasar Double Track System & Implementasinya*. Jakarta: PT. RajaGrafindo Persada, hlm. 206

[27] Teguh Prasetyo. *Op.Cit.,* hlm 56

tersebut secara tepat dan proporsional, dan menghindari penerapan sanksi yang fragmentaristik.

Untuk mewujudkan sanksi pidana tersebut, dalam Pasal 10 KUHP dirincikan jenis sanksi pidana sebagai berikut:

a. Pidana Pokok, yaitu pidana mati, pidana penjara, pidana kurungan, pidana denda, hukuman tutupan;
b. Pidana Tambahan, yaitu pencabutan hak-hak tertentu, perampasan barang-barang tertentu, pengumuman putusan hakim.

Selanjutnya terkait sanksi tindakan (*maatregel*), dalam KUHP diatur sebagai berikut:

a. Perawatan dalam rumah sakit jiwa bagi pelaku yang mengalami gangguan jiwa;
b. Hukuman bersyarat
c. Bagi anak yang belum dewasa (belum berusia 16 tahun), hakim dapat memilih alternatif tindakan yaitu: penyerahan kepada orang tua/wali, penyerahan kepada pemerintah untuk dimasukkan dalam rumah pendidikan negara, penempatan di tempat bekerja negara.

Berkaitan dengan tindak pidana *credit/debit card fraud* di Indonesia, sanksi yang diterapkan terhadap terdakwa didasarkan pada UU ITE sebagai *lex specialis*. Meskipun demikian tidak tertutup kemungkinan digunakan juga KUHP sebagai *lex generalis*, tergantung pada penilaian hakim terhadap fakta persidangan dan alat bukti yang dihadirkan. Khusus untuk UU ITE, sanksi pidana yang ditekankan ialah sanksi pidana penjara dan pidana denda, sebagaimana yang ditegaskan dalam Pasal 46-Pasal 49 dari UU tersebut.

Dalam pasal-pasal tersebut, pidana penjara yang diterapkan rata-rata mencapai 6-10 tahun, sedangkan pidana denda ditetapkan dari angka 600 juta hingga mencapai 10 milyar.

Menurut hemat penulis, makna filosofis di balik pengaturan sanksi pidana terhadap tindak pidana *credit/debit card fraud* di Indonesia sangat menekankan aspek pembalasan absolut. Pembalasan absolut ini menekankan aspek retribusi yang adil terhadap pelaku tindak pidana *credit/debit card fraud* oleh karena kerugian yang terjadi. Selain itu, tersirat adanya pembalasan dendam masyarakat terhadap pelaku tindak pidana *credit/debit card fraud*. Meskipun demikian, dalam mekanisme pembalasan absolut tersebut, tersirat juga upaya untuk melindungi masyarakat dari tindak pidana *credit/debit card fraud*, sekaligus untuk mencegah terjadinya kejahatan yang serupa di kemudian hari.

Penerapan sanksi pidana yang menekankan sisi pembalasan absolut dan relatif dalam pidana penjara dan denda yang diatur oleh UU ITE menunjukkan bahwa pemidanaan di Indonesia (untuk tindak pidana *credit/debit card fraud*) sama sekali tidak mempehatikan aspek kuratif terhadap pelaku tindak pidana. Hukum pidana diciptakan untuk mengembalikan situasi harmoni dan seimbang sebagaimana awal terciptanya masyarakat (*restituo in integrum*).

Untuk mengembalikan keadaan masyarakat yang *peacefull*, hukum pidana harus memerhatikan semua aspek yang terlibat dalam satu tindak pidana, khususnya korban, pelaku, dan masyarakat secara keseluruhan. Dengan demikian, penerapan sanksi pidana yang berlatar belakang pembalasan mutlak dan relatif sebagaimana diatur dalam UU ITE, tidak akan mampu menciptakan *restitu-*

tio in integrum apabila aspek penyembuhan terhadap pelaku tindak pidana *credit/debit card fraud* tidak diperhatikan.

Idealnya, pengaturan mengenai sanksi pidana dalam UU ITE, harus menekankan juga sanksi tindakan (*maatregel*). Sanksi tindakan yang diterapkan dalam hukum pidana terfokus pada penyembuhan pelaku, yaitu agar pelaku dapat berubah dari perbuatannya yang jahat menuju pribadi yang bermanfaat bagi masyarakat. Penulis berpendapat bahwa sanksi tindakan dapat menekankan aspek pembelajaran secara positif terhadap sisi ilmiah dari tindak pidana *credit/debit card fraud*. Dengan kata lain, para pelaku dapat dididik lebih lanjut secara positif untuk dapat mengembangkan kemampuannya yang sewaktu-waktu dapat digunakan penegak hukum dan pihak perbankan untuk membantu mengungkap tindak pidana serupa di masa depan.

PENUTUP

Pengaturan hukum terhadap tindak pidana *credit/debit card fraud* di Indonesia yakni diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai *lex specialist* dari KUHP. Di antaranya, diatur dalam beberapa ketentuan: Pasal 30 (akses ilegal); Pasal 31 (penyadapan ilegal); Pasal 32 (gangguan terhadap data komputer) dan Pasal 33 (gangguan terhadap sistem komputer). Pene-rapan sanksi pidana terhadap tindak pidana *credit/debit card fraud* di Indonesia masih menggunakan filosofi pemidanaan absolut (teori balas dendam), yakni sanksi pidana yang ditekankan pada sanksi pidana penjara dan pidana denda (*vide*: Pasal 46-49 dari UU ITE).

Beranjak dari konstruksi hukum tersebut, maka UU ITE harus direvisi dengan penambahan ketentuan yang secara langsung mengatur mengenai *computer related fraud* bahwa setiap orang dilarang dengan sengaja dan tanpa hak, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum: (a) Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, atau menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik dengan cara apapun; (b) Mengganggu sistem elektronik dengan cara apapun, sehingga mengakibatkan hilangnya atau berpindahnya barang atau harta milik orang lain.

Selain mengatur ancaman pidana penjara dan denda terhadap tindak pidana *credit/debit card fraud*, seyogianya juga mengatur sanksi dalam bentuk tindakan yang bersifat restitutif, agar ke depannya mereka yang pernah menjadi pelaku tindak pidana *credit/debit card fraud* dapat membantu aparat penegak hukum mengungkap beberapa model tindak pidana yang serupa.

BIBLIOGRAFI

Arief Amrullah. (2006). *Kejahatan Korporasi*. Malang: Bayumedia.

Erdianto Effendi. (2011). *Hukum Pidana Indonesia Suatu Pengantar*. Bandung: Refika Aditama.

Frans Maramis. (2013). *Hukum Pidana Umum dan Tertulis di Indonesia*. Jakarta: PT. RajaGrafindo Persada.

Fuad Usfa. (2004). *Pengantar Hukum Pidana*. Malang: Universitas Muhamadiyah Malang Press.

Ian Walden. (2007). *Computer Crime and Digital Investigation*. Oxford: Oxford University Press.

Jan Remmelink. (2003). *Hukum Pidana*. Jakarta: Gramedia Pustaka Utama.

Josua Sitompul. (2012). *Cyberspace, Cybercrimes, Cyberlaw, Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.

Sholehuddin. (2003). *Sistem Sanksi dalam Hukum Pidana: Ide Dasar Double Track System & Implementasinya*. Jakarta: PT. RajaGrafindo Persada.

Sigid Suseno. (2012). *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama.

Teguh Prasetyo. (2010). *Kriminalisasi dalam Hukum Pidana*. Cetakan pertama. Bandung: Nusamedia.

Widodo. (2013). *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Aswaja Pressindo.

***