BAB IV

PEMBAHASAN

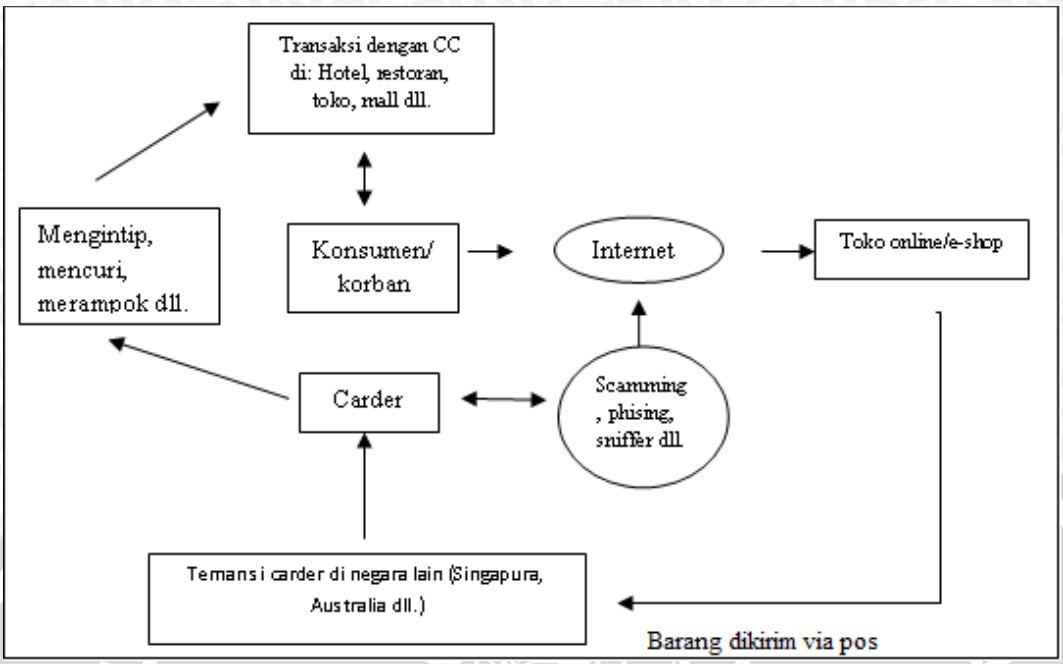
1. Kejahatan *Carding* Termasuk Pada Kejahatan Transnasional Dikaji Dari Perspektif Hukum Internasional

Kejahatan transnasional adalah kejahatan yang tidak hanya berupa kejahatan yang melintasi batas negara, tetapi termasuk juga kejahatan yang dilakukan di suatu negara, tetapi menimbulkan dampak di negara lain.[55]

Kejahatan *carding* merupakan kejahatan yang memanfaatkan teknologi internet sebagai sarana utama untuk mengakses secara tidak sah suatu sistem sebuah website untuk mendapatkan data-data para nasabah kartu kredit. Tujuannya adalah untuk membelanjakan secara tidak sah kartu kredit yang telah didapatkan ataupun untuk mendapatkan dana milik pemegang kartu kredit tersebut. Dibawah ini merupakan gambaran modus operandi yang saat ini sering dilakukan oleh para pelaku *carding* (*carder*).

[55]Soeparna, Intan Innayatun, **Kejahatan Telematika Sebagai Kejahatan Transnasional**, makalah disajikan dalam Seminar Nasional Hukum Telematika: Prospek Antisipasi dan Penanganan Kejahatan Telematika Pasca Diundangkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Fakultas Hukum Universitas Airlangga, Surabaya, 30 Agustus 2008, hal 3.

Gambar 2
Modus Operandi Carding



Sumber : Reportase Investigasi Trans7 16 November 2013

Para *carder* memilliki dua cara untuk mendapatkan data-data kartu kredit para korban, yang pertama dengan menyentuh langsung kartu kredit milik korban yang pada umumnya dilakukan di gerai ritel seperti restoran dan toko. Tindakan tersebut dilakukan oleh karyawan dengan alasan yang sah untuk memiliki kartu kredit korban, selanjutnya karyawan memanfaatkan *electronic data capture* untuk mencuri data-data yang tersimpan di dalam kartu (*skimming*). Tindakan *skimming* tersebut seperti yang terjadi di cabang *The Body Shop* Jakarta.[56]

Cara yang kedua adalah memanfaatkan teknologi internet. Salah satunya adalah *phising*, teknik ini digunakan oleh para *carder* untuk memperoleh data-data kartu kredit dengan mengarahkan korban untuk masuk ke sebuah situs

[56] Syahid, Latif, 2013, **Kronologi Kasus Pencurian Data Kartu Kredit di *Body Shop*** (online), http://bisnis.liputan6.com/read/544093/kronologi-kasus-pencurian-data-kartu-kredit-di-body-shop, (3 Desember 2013).

website jebakan yang telah dibuat menyerupai *website* asli, seperti *www.klikbca.com*. Biasanya para *carder* melakukan *phising* dengan mengirimkan sebuah email kepada para korban.

Setelah mendapatkan nomor kartu kredit beserta data-datanya, *carder* membelanjakannya di pedagang (*merchant*) online yang diinginkan. Barang yang dibeli akan dikirimkan ke alamat teman *carder* yang ada di luar negeri seperti Australia atau Singapura, hal ini dilakukan karena banyak *merchant* yang tidak berkenan mengirimkan barang ke alamat Indonesia. Setelah itu barang akan dikirimkan oleh teman *carder* ke alamat Indonesia.

Terdapat kasus lain yang dilakukan oleh seorang *hacker* berkebangsaan Rusia.

> **"The U.S. Justice Department** on Monday announced the arrest of a Russian hacker accused of running a network of online crime shops that sold credit and debit card data stolen in breaches at restaurants and retailers throughout the United States.[57]"

Pelaku bernama Roman Seleznev telah mencuri ribuan data kartu kredit dan debit para pelanggan *online shop* dan restoran di beberapa negara. Pelaku tertangkap di Maldives saat hendak kembali ke Moscow. Berita terbaru menyatakan pelaku tidak bertindak sendirian, ia memiliki jaringan di beberapa negara yang selalu berhubungan di dalam grup *chatting.*

Dari modus operandi dan contoh kasus di atas terdapat unsur-unsur bahwa *carder* yang memanfaatkan teknologi internet dapat menjangkau para nasabah pemegang kartu kredit yang berada di luar negara dimana *carder* berada dan dapat

[57] Brian Krebs, 2014, ***Feds Charge Carding kingpin in Retail*** Hacks (online), http://krebsonsecurity.com/2014/07/feds-charge-carding-kingpin-in-retail-hacks/, (18 Agustus 2014).

membelanjakan kartu kredit tersebut di toko manapun yang menyediakan pembelian secara online. Hal tersebut dapat dilakukan karena sifat dari teknologi internet yang tanpa batas (*borderless*).

Menurut pasal 3 ayat 2 United Nations Convention Against Transnational Organized Crime, suatu kejahatan dapat dikategorikan sebagai kejahatan transnasional apabila:

1. *It is committed in more than one State;*
2. It is committed in one State but a substansial part of its preparation, planning, direction or control takes place in another State;
3. It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
4. It is committed in one State but has substansial effects in another State.

Kejahatan *carding* dapat dikategorikan dalam kejahatan transnasional karena:

1. Pencurian data-data kartu kredit nasabah oleh para *carder* bisa dilakukan di beberapa negara. Dalam kasus "*The Body Shop*" terdeteksi pencurian data kartu kredit milik pelanggan tidak hanya terjadi di cabang *The Body Shop* Jakarta, namun di malaysia, filipina, bahkan India.
2. Persiapan, perencanaan pengarahan dan pengawasan oleh pelaku kejahatan *carding* dilakukan di satu negara tetapi target kejahatan tersebut berada di luar negara dimana *carder* berada.

3. Pada penangkapan yang dilakukan Polri pada kamar 208 apartemen Puri Kemayoran Jakarta Pusat[58] terungkap bahwa, pelaku berinisial S alias Ciement memiliki sindikat yang berwarganegara Malaysia dan Indonesia. Sindikat tersebut mencuri dan memalsukan kartu kredit warga negara Indonesia, Amerika, Timur Tengah.
4. Kejahatan *carding* menimbulkan dampak di negara lain. Hal ini terjadi karena target pelaku adalah nasabah pemegang kartu kredit yang berada di luar negeri, seperti pada kasus pembobolan kartu kredit yang dilakukan oleh Rizky Martin. Pelaku 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 Rp350 juta. Dua pelaku ditangkap aparat Cyber Crime Polda Metro Jaya pada 10 Juni 2008 di sebuah warnet di kawasan Lenteng Agung, Jaksel. Awal Mei 2008 lalu.[59]

2. Prinsip hukum internasional yang dapat mencegah kejahatan *carding* sebagai kejahatan transnasional

Dalam Konvensi Wina tahun 1969 telah berhasil disepakati sebuah naskah perjanjian yang lebih dikenal dengan nama *Viena Convention on the Law of Treaties* atau Konvensi Wina tentang Hukum Perjanjian tahun 1969 (Konvensi Wina 1969). Konvensi Wina ini diadakan atas prakarsa Perserikatan Bangsa-

[58] Indradi Thanos, 2013, **Pemalsuan Kartu Kredit Terbesar Di Dunia** (online), http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-ekonomi/94-pemalsuan-kartu-kredit-terbesar-di-dunia, (11 Agustus 2014).
[59] Ayu Purnama, 2014, **Carder Muda Indonesia Akhirnya Tertangkap** (online), http://hipersomniax.blogspot.com/2014/04/carder-muda-indonesia-akhirnya.html, (7 Agustus 2014).

bangsa dan naskah rancangan konvensinya disusun oleh Panitia Hukum Internasional/*International Law Commission* (yang disingkat dengan ILC), yaitu sebuah Panitia ahli dan dibentuk berdasarkan Resolusi Majelis Umum PBB No.174/II/1947.

Konvensi Wina tentang perjanjian ini tidak hanya sekedar merumuskan kembali atau mengkodifikasikan hukum kebiasaan internasional dalam bidang perjanjian, melainkan juga merupakan pengembangan secara progresif hukum internasional tentang perjanjian. Namun demikian Konvensi Wina ini masih tetap mengakui eksistensi hukum kebiasaan internasional tentang perjanjian, khususnya tentang persoalan-persoalan yang belum diatur dalam Konvensi Wina. Konvensi Wina 1969 ini erat hubungannya dalam penanggulangan kejahatan *carding*, karena kejahatan *carding* merupakan kejahatan transnasional, sehingga pencegahannya harus melibatkan atau bekerja sama dengan negara lain dengan mengadakan perjanjian internasional.

Cybercrime ini telah masuk dalam daftar jenis kejahatan yang sifatnya transnasional berdasarkan *United Nation Convention Againts Transnational Organized Crime* (Palermo convention) November 2000 dan berdasarkan Deklarasi ASEAN tanggal 20 Desember 1997 di Manila. Jenis-jenis kejahatan yang termasuk dalam *cyber crime* diantaranya adalah:

1. *Cyber-terrorism*: *National Police Agency of Japan* (NPA) mendefinisikan *cyber terrorism* sebagai *electronic attacks through computer networks against critical infrastructure that have potential critical effect on social and economic activities of the nation*.

2. *Cyber-pornography*: penyebaran obscene materials termasuk pornografi, indecent exposure, dan child pornography.
3. *Cyber Harrasment*: pelecehan seksual melalui email, website atau chat programs.
4. *Cyber-stalking*: *crimes of stalking* melalui penggunaan computer dan internet.
5. *Hacking*: penggunaan programming abilities dengan maksud yang bertentangan dengan hukum.
6. *Carding* (*credit card fund*), *carding* muncul ketika orang yang bukan pemilik kartu kredit menggunakan kartu credit tersebut secara melawan hukum.

Adanya unsur-unsur transnasional dari kejahatan *carding* tentunya akan menimbulkan masalah tersendiri, khususnya berkenaan dengan masalah yurisdiksi. Yurisdiksi adalah kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum). Yuriskdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak ikut campur tangan.

Yurisdiksi juga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum.Berdasarkan asas umum dalam hukum internasional, setiap negara memiliki kekuasaan tertinggi atau kedaulatan atas orang dan benda ada dalam wilayahnya sendiri. Oleh karena itu, suatu negara tidak boleh melakukan

tindakan yang bersifat melampui kedaulatannya (*act of sovereignty*) di dalam wialyah negara lain, kecuali dengan persetujuan negara itu sendiri.[60]

Apabila diketahui adanya pelaku kejahatan yang melarikan diri atau berada dalam wilayah negara lain, maka negara tersebut dapat menempuh cara yang sah untuk dapat mengadili dan menghukum si pelaku kejahatan. Hukum internasional tradisional telah meletakkan beberapa prinsip umum yang berkaitan dengan yurisdiksi suatu negara.

Di dalam praktiknya, yurisdiksi dapat dibedakan antara yurisdiksi perdata dan yurisdiksi pidana. Yurisdiksi perdata adalah kewenangan hukum pengadilan suatu negara terhadap perkara-perkara yang menyangkut keperdataan baik yang sifatnya nasional yaitu bila para pihak atau obyek perkaranya melulu menyangkut nasional, maupun yang bersifat internasional (perdata internasional) yaitu bila para pihak obyek perkaranya menyangkut unsur asing. Yurisdiksi pidana adalah kewenanga (hukum) pengadilan suatu negara terhadap perkara-perkara yanag menyangkut kepidanaan, baik yang tersangkut di dalamnya unsur asing maupun nasional.

Yurisdiksi suatu negara yang diakui Hukum Internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sementara komunikasi multimedia bersifat internasional, multi yursidiksi, tanpa batas, sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap teknologi informasi sebagai salah satu pemanfaatan teknologi informasi.

---

[60] Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika,1992, hal. 30.

Ada 3 ruang lingkup yurisdiksi yang dimiliki suatu negara berkenaan dengan penetapan dan pelaksanaan pengawasan terhadap setiap peristiwa, setiap orang dan setiap benda. Ketiga ruang lingkup tersebut terdiri dari:

a. Yurisdiksi untuk menetapkan ketentuan pidana (*jurisdiction to prescrebi* atau *legislative jurisdiction* atau *prespective jurisdiction*);
b. Yurisdiksi untuk menerapkan atau melaksanakan ketentuan yang telah ditetapkan oleh badan legislatif (*executive jurisdiction*);
c. Yurisdiksi untuk memaksakan ketentuan hukum yang telah dilaksanakan oleh badan eksekutif atau yang telah diputuskan oleh badan peradilan (*enforcement jurisdiction* atau *jurisdiction to ajudicate*).[61]

Huala Adolf mengemukakan bahwa yurisdiksi adalah kekuatan atau kewenangan hukum negara terhadap orang, benda atau peristiwa (hukum).[62] Yurisdiksi pidana adalah kewenangan (hukum) pengadilan suatu negara terhadap perkara-perkara yang menyangkut kepidanaan, baik yang tersangkut di dalamnya unsur asing maupun nasional.[63]

Yurisdiksi merupakan prinsip dasar dari kedaulatan negara yang dibuat berdasarkan kepentingan dari negara tersebut. Beberapa negara telah menggunakan prinsip yurisdiksi ekstrateritorial dalam hukum nasionalnya. Prinsip ekstrateritorial ini digunakan ketika dampak yang ditimbulkan dari suatu tindak pelanggaran berakibat kepada banyak pihak. Kondisi lain yang dapat menimbulkan penggunaan prinsip ekstrateritorial adalah ketika wilayah tempat

[61] Huala Adolf, Aspek-aspek Hukum Pidana Internasional, RajaGrafindo Persada, Jakarta, 1996, hal. 145.
[62] Huala Adolf, Aspek-aspek Negara Dalam Hukum Internasional edisi revisi, PT RajaGrafindo Persada, Jakarta, 2002, hal. 183.
[63] Huala Adolf, 1996, *op.cit.*, hal. 145.

terjadinya tindak pelanggaran tersebut tidak mengaturnya namun tetap merugikan pihak lain akibat tindak pelanggaran tersebut.[64]

Permasalahan yang telah dipaparkan diatas sebenarnya merupakan pemicu adanya pembentukan serta pemberlakuan Undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Penggunaan hukum pidana nasional negara tidak cukup untuk menjamin keadilan dari tiap pelanggaran yang khususnya dilakukan dengan teknologi informasi. Semakin canggihnya teknologi informasi yang membuat batas negara menjadi tidak terlihat serta perbedaan bentuk hukum pidana satu negara dengan negara lain yang menjadi alasan pemberlakuan prinsip teritorial yang melebihi wilayah negaranya sendiri, atau yang dikenal dengan ekstrateritorial.

Pemberlakuan prinsip ekstrateritorial secara materiilnya tergambar atau dapat kita lihat di dalam Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pada pasal 2, yakni bahwa pengaturan teknologi informasi yang diterapkan oleh suatu negara berlaku untuk setiap orang yang melakukan perbuatannya baik yang berada di wilayah negara tersebut maupun di luar negara apabila perbuatan tersebut memiliki akibat di Indonesia.

Butuhnya pengaturan yurisdiksi ekstrateritorial dikarenakan kejahatan *carding* dapat merugikan kepentingan orang atau negara walaupun perbuatan (*locus delicti*) dilakukan di wilayah negara lain. Oleh karena itu, peraturan mengenai pemanfaatan teknologi informasi dan komunikasi tersebut harus dapat

[64] Vera Carolina, **Penerapan Prinsip Yurisdiksi Ekstrateritorial Dalam Pemanfaatan Teknologi Informasi dan Komunikasi Serta Pelaksanaannya Di Indonesia Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik**, Bandung, Universitas Padjadjaran, hal 48.

mencakup perbuatan yang dilakukan di luar wilayah Indonesia tetapi merugikan kepentingan orang atau negara dalam wilayah Indonesia.

Berdasarkan pengertian dari pasal 2 Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut menunjukkan bahwa sebenarnya penggunaan prinsip yurisdiksi ekstrateritorial dalam menyelesaikan permasalahan hukum yang mencakup lebih dari satu wilayah teritorial suatu negara terkait penggunaan teknologi informasi dapat diterapkan selama perbuatan yang dilakukan oleh warga negara ataupun negara lain menimbulkan akibat hukum serta memberikan dampak kerugian bagi Indonesia.

Permasalahan lainnya yang timbul terkait prinsip ini yakni bentuk pemberlakuan dalam penerapan prinsip yurisdiksi ekstrateritorial tersebut. Meskipun prinsip ini terlihat di dalam Undang-undang nomor 11 tahun 2008 pasal 2, pemberlakuan prinsip ini tidak dapat dipergunakan secara meluas dengan paksaan atau kehendak dari negara pembuat undang-undang (dalam hal ini Indonesia), melainkan dibutuhkan adanya pengakuan peratifikasian yang dilakukan oleh suatu negara. Seperti contohnya di Indonesia, pemberlakuan prinsip yurisdiksi ekstrateritorial yang tercantum dalam pasal 2 tersebut tidak mengikat dan menjadi aturan hukum umum bagi negara lain selama pemberlakuan Undang-undang nomor 11 tahun 2008 tersebut hanya bagi negara Indonesia (tidak adanya peratifikasian yang dilakukan oleh negara lain).

Carding merupakan kejahatan transnasional, sehingga yurisdiksi yang berlaku adalah yurisdiksi ekstrateritorial untuk menetapkan, menerapkan dan memaksakan ketentuan hukum yang telah ditetapkan oleh suatu negara. Dalam hal penanggulangan kejahatan transnasional, dikenal asas *aut dedere aut judicare*,

yang berarti "Setiap Negara berkewajiban untuk menuntut dan mengadili pelaku tindak pidana internasional dan berkewajiban untuk bekerjasama dengan negara lain di dalam menangkap, menahan dan menuntut serta mengadili pelaku tindak pidana internasional." Asas tersebut tercantum di dalam *Convention on Cybercrime* pada pasal 24 paragraf 3.

Menurut Mohd. Burhan Tsani, "Perjanjian internasional memiliki beberapa fungsi, yaitu :

a. Untuk mendapatkan pengakuan umum anggota masyarakat bangsa-bangsa,
b. Sarana utama yang praktis bagi transaksi dan komunikasi antar anggota masyarakat negara,
c. Berfungsi sebagai sumber hukum internasional,
d. Sarana pengembang kerjasama internasional secara damai."[65]

Berdasarkan fungsi keempat dari perjanjian internasional yaitu sarana pengembang kerjasama internasional secara damai yang merupakan sarana wajib untuk mencegah terjadinya kejahatan transnasional, maka Indonesia perlu bergabung dalam *Convention on Cybercrime*.

3. Rumusan norma hukum yang dapat mencegah kejahatan *carding* diharmonisasikan ke dalam undang-undang nomor 11 tahun 2008

Dalam buku kerjasama ASEAN untuk Menanggulangi Kejahatan Lintas Negara dijelaskan bahwa asumsi dasar dari kejahatan lintas negara adalah

[65] Tsani, Mohd. Burhan, **Hukum dan Hubungan Internasional,** Liberty, Yogyakarta, 1990, hal 66-67.

pertama, merupakan gejala global yang tidak dapat diselesaikan oleh satu negara saja, melainkan harus melalui kerjasama internasional. Kedua, kejahatan ini tumbuh dan berkembang seirama dengan kemajuan teknologi informasi dan transportasi internasional. Ketiga, kejahatan tersebut disebabkan oleh kondisi sosial, politik, ekonomi, pertahanan, keamanan dan teknologi yang berkembang pesat di berbagai negara juga kebijakan dalam dan luar negeri suatu negara yang menjadi sasaran dari kejahatan ini. Keempat, kejahatan lintas negara tidak memandang ideologi, suku bangsa ataupun agama dari pelaku kejahatan ini. Kelima, dapat dilakukan oleh individu, kelompok, atau bahkan negara, baik sebagai sponsor maupun pelakunya. Keenam, tidak selalu didasari oleh motif politik semata, tetapi juga motif-motif ekonomi atau bahkan tak ada motif yang jelas.[66]

Mengingat karakteristik *cybercrime* yang bersifat *borderless* dan menggunakan teknologi tinggi sebagai media, maka kebijakan kriminalisasi di bidang teknologi harus memerhatikan perkembangan upaya penanggulangan *cybercrime* baik regional maupun internasional dalam rangka harmonisasi dan uniformitas perngaturan *cybercrime*.[67] Oleh karena itu, perlu dikaji beberapa rumusan norma yang terdapat dalam *European Convention on Cybercrime*, konvensi tersebut merupakan salah satu instrumen hukum internasional yang perlu dikaji dan dijadikan patokan dalam penyusunan suatu norma hukum positif untuk mencegah *carding* di Indonesia.

---

[66] Mattalitti, Abdurrachman, dkk. 2001. **Kerjasama ASEAN dalam Menanggulangi Kejahatan Lintas Negara**. Jakarta : Direktorat Jenderal Kerjasama ASEAN Departemen Luar Negeri Republik Indonesia. Hal. 1.

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

Untuk melakukan upaya pencegahan kejahatan *carding* perlu adanya penguatan pada Undang-undang Nomor 11 Tahun 2008. Penguatan hukum tersebut dimaksudkan untuk mengefektifkan fungsi pencegahan (preventif), sehingga kejahatan tersebut tidak lagi timbul.

Tabel 1
Perbandingan CoC dengan UU ITE

Convention on Cybercrime	**UU ITE**
Art. 2 - Illegal access	Pasal 30
Art. 3 - Illegal Interception	Pasal 31
Art. 4 - Data Interference	Pasal 32
Art. 5 - System Interference	Pasal 33
Art. 6 - Misuse of Device	Pasal 34
Art. 7 - Computer Related Forgery	Pasal 35
Art. 8 - Computer Related Fraud	Tidak diatur
Art. 9 - Offences Related to Child Pornography	Pasal 27 ayat (1)
Art. 10 - Offences Related to Infringements of Copyright and Related Rights	Tidak diatur
Art. 11 - Attempt and Aiding or Abetting	Tidak diatur
Art. 23-28 International Co-operation	Tidak diatur

Berdasarkan tabel di atas, terdapat beberapa norma dari *Convention on Cybercrime* yang telah diadopsi ke dalam UU ITE, yaitu mengenai *Illegal access, Illegal Interception, Data Interference, System Interference, Misuse of Device, Computer Related Forgery, Offences Related to Child Pornography.*

Terdapat beberapa norma yang tidak diatur oleh undang-undang ITE, yaitu mengenai penipuan, pelanggaran terhadap hak cipta, penyertaan dan kerjasama internasional. Maka perlu adanya penambahan pasal ke dalam UU ITE agar sesuai dengan ketentuan di dalam CoC.

Computer Related Fraud

Dalam modus operandi yang dilakukan oleh pelaku *carding* terdapat unsur penipuan, yaitu saat pelaku berusaha mendapatkan nomor kartu kredit dengan mengirimkan email *spam* kepada korban. Isi dari email tersebut terdapat pernyataan untuk mengarahkan korban ke sebuah situs yang dibuat oleh *carder*, dan situs tersebut dibuat seolah-olah asli, contoh : situs bank, perusahaan terkemuka dan lain-lain.

Berdasarkan fakta tersebut, pengaturan mengenai penipuan yang menggunakan sarana komputer sangat penting untuk dihadirkan dalam sistem hukum pidana di Indonesia untuk melindungi kepentingan atau nilai hukum yang sama dengan yang dimaksud dalam pengaturan penipuan secara konvensional. Dalam pasal 8 CoC diatur bahwa *computer related fraud* merupakan:

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

Maka Undang-undang informasi dan transaksi elektronik perlu ditambahkan pasal mengenai penipuan di dalam bab VII tentang perbuatan yang dilanggar : “Setiap orang dengan sengaja dan tanpa hak menyebabkan kerugian kepada seseorang dengan cara :

a. Memasukkan, mengubah, menghapus atau menahan data komputer;

b. Mengganggu fungsi sistem komputer dengan niat tidak jujur dan menipu untuk menguntungkan diri sendiri atau orang lain."

Attempt and Aiding or Abetting

Rumusan pasal 11 *CoC* mengatur tentang pidana bagi para pihak yang ikut serta untuk menolong atau membantu tindak pidana *cybercrime*. Pasal ini menetapkan semua bentuk tindakan yang secara sadar menolong atau membantu pelanggaran yang telah ditetapkan pada pasal 2 sampai 10 *CoC*.

> *Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with article 2 through 10 of the present Convention with intent that such offence be committed*

Maka menurut pasal tersebut perlu penambahan pasal di dalam Undang-undang nomor 11 tahun 2008 mengenai Perbuatan yang Dilarang, yaitu : "Setiap orang dengan secara sadar menolong atau membantu pelanggaran yang ditetapkan dalam pasal 27-37"

Dengan pasal tersebut, seorang *dropper* yaitu yang ikut membantu meneruskan kiriman barang yang dibeli oleh *carder* dari luar negeri dapat dikenai sanksi pidana.

International Co-operation

Dalam pembahasan kedua telah dijelaskan perlunya peraturan dalam tingkat internasional untuk menghadapi kejahatan transnasional, maka dalam hal

ini Undang-undang ITE tidak dapat berdiri sendiri untuk menangani kejahatan transnasional.

Kerjasama internasional dibutuhkan untuk proses penyidikan yang tidak berada di satu yurisdiksi negara saja, namun terdapat di beberapa negara. Di dalam CoC terdapat beberapa ketentuan mengenai kerjasam internasional yang dapat mempermudah proses penyidikan, yaitu :

1. Pasal 24 *Extradition*

Konvensi ini membuka penerapan prinsip yurisdiksi seluas-luasnya sehingga dapat diterapkan dalam menangani kasus cybercrime secara optimal. Pengaturan pada pasal ini berarti bahwa masing-masing pihak harus melakukan tindakan-tindakan lainnya sebagaimana diperlukan untuk menetapkan yurisdiksi atas setiap pelanggaran yang dilakukan sesuai dengan pasal 2 sampai 11 dari konvensi ini apabila pelanggaran tersebut dilakukan :

a. Di wilayahnya; atau
b. Di atas kapal yang berbendera pihak tersebut;
c. Di atas kapal yang terdaftar menurut hukum pihak tersebut
d. Oleh salah satu warga negaranya apabila pelanggaran tersebut dikenakan hukuman berdasarkan hukum pidana dimana hal tersebut dilakukan atau apabila pelanggaran tersebut dilakukan di luar yurisdiksi wilayah negara manapun

Masing-masing pihak berhak untuk tidak menggunakan atau menggunakan hanya dalam kasus-kasus atau keadaan-keadaan khusus aturan yurisdiksi yang ditetapkan dalam ayat 1.b sampai 1.d dari pasal ini atau dari setiap bagiannya.

Masing-masing pihak dapat melakukan tindakan-tindakan sebagaimana diperlukan untuk menetapkan yurisdiksi atas pelanggaran-pelanggaran yang dimaksudkan dalam pasal 24 ayat 1, dalam kasus dimana pelanggar yang diduga berada di wilayahnya dan pihaknya tidak mengekstradisi orang tersebut kepada pihak lainnya semata-mata berdasarkan kebangsaannya, setelah permohonan ekstradisi.

Konvensi ini tidak mengecualikan setiap yurisdiksi pidana yang dilaksanakan oleh salah satu pihak sesuai dengan undang-undang dalam negaranya.

Apabila terdapat lebih dari satu pihak yang menggugat yurisdiksi atas sebuah dugaan pelanggaran yang ditetapkan sesuai dengan konvensi ini, maka para pihak yang terlibat harus berkonsultasi dengan tujuan untuk menetapkan yurisdiksi yang paling sesuai untuk proses penuntutan.

2. Pasal 25 *General principal relating to mutual assistance*

Para negara anggota harus saling memberikan bantuan semaksimal mungkin untuk penyidikan-penyidikan atau penuntutan, menerapkan undang-undang dan tindak-tindakan lain yang diperlukan untuk pelaksanaan kewajiban-kewajiban yang disebutkan dalam pasal 27-35. Ketentuan tentang *mutual assistance*, termohon diperbolehkan untuk memberikan bantuan hanya jika ada kriminalitas ganda.

3. Pasal 26 *Spontaneous information*

Negara anggota berhak dalam batas dari undang-undang dan tanpa permintaan sebelumnya, meneruskan informasi yang didapat melalui kerangka penyidikannya sendiri kepada pihak lain dan pihak penyedia informasi dapat meminta agar kerahasiaan informasi tersebut dijaga atau hanya bisa digunakan atas persyaratan tertentu.

Dalam hal ini setiap negara anggota harus saling bekerjasama untuk mengumpulkan dan menginformasikan bukti elektronik yang didapat kepada negara yang sedang melakukan penyelidikan. Negara juga harus bekerjasama dengan sektor privat yaitu penyedia layanan komunikasi untuk mengumpulkan bukti elektronik.

4. Pasal 27-28 *Procedures pertaining to mutual assistance requests in the absence of applicable international agreements*

Pasal ini mengatur tentang permintaan bantuan tanpa perjanjian internasional dengan menunjuk satu otoritas sentral atau otoritas-otoritas yang bertanggung jawab untuk mengirim dan menjawab permintaan-permintaan bantuan, mengeksekusi, memberitahukan kepada otoritas yang kompeten untuk melakukan eksekusi.

5. Pasal 29-30 *Mutual assistance regarding provisional measures*

Pasal ini mengatur ketentuan-ketentuan khusus tentang pemeliharaan data yang tersimpan dalam komputer yang berlokasi di dalam wilayah pihak negara lain.

6. Pasal 31-35 *Mutual assistance regarding investigative powers*

Negara anggota diperbolehkan meminta pihak negara lain untuk mencari atau mengakses, menyita atau mengamankan data yang tersimpan dengan menggunakan sistem komputer yang berlokasi di dalam wilayah pihak termohon.