JURNAL

PENCEGAHAN KEJAHATAN CARDING SEBAGAI KEJAHATAN TRANSNASIONAL MENURUT HUKUM INTERNASIONAL

Untuk Memenuhi Sebagian Syarat-Syarat
Untuk Memperoleh Gelar Kesarjanaan
Dalam Ilmu Hukum

Disusun :

Novryan Alfin Kurniawan

0910111036

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

UNIVERSITAS BRAWIJAYA

FAKULTAS HUKUM

MALANG

2014

PENCEGAHAN KEJAHATAN CARDING SEBAGAI KEJAHATAN TRANSNASIONAL MENURUT HUKUM INTERNASIONAL

Novryan Alfin Kurniawan

Fakultas Hukum, Universitas Brawijaya

Email : novryank@yahoo.com

ABSTRAK

Perkembangan teknologi dan internet tidak selamanya menghasilkan hal-hal yang positif. Hal negatif yang merupakan efek sampingnya antara lain adalah kejahatan *carding* (pencurian kartu kredit) yang merupakan salah satu jenis kejahatan di dunia *cybercrime*. Hilangnya batas ruang dan waktu di dunia maya mengubah banyak hal. Seorang *carder* dapat masuk ke sebuah server tanpa izin (*unauthorized access*). Tujuannya mungkin untuk mendapatkan barang tanpa membayar atau untuk mendapatkan dana yang tidak sah dari akun kartu kredit yang didapat.

Permasalahan yang muncul adalah penerapan yurisdiksi ekstrateritorial yang tidak dapat dipergunakan secara meluas dengan paksaan atau kehendak dari Indonesia.

Penelitian ini merupakan *legal research* yang menggunakan pendekatan konseptual (*conceptual approach*) serta pendekatan perundang-undangan (*statue approach*) yang akan menelaah asas-asas hukum internasional yang terdapat di dalam *Convention on Cybercrime* dan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Berdasarkan metode yang digunakan, maka diketahui kejahatan *carding* merupakan kejahatan transnasional dan untuk mencegahnya diperlukan penerapan yurisdiksi ekstrateritorial yang didampingi dengan perjanjian internasional yaitu *Convention on Cybercrime* dan menambah beberapa pasal di dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sesuai dengan ketentuan konvensi tersebut.

ABSTRACT

The development of technology and the internet are not always bring out the positive things. Negative thing that arised is carding (credit card theft) which is one type of crime in cybercrime. The loss of the limits of space and time in the virtual world have changed many things. A carder can log in to a server without permission (unauthorized access). The goal may be to obtain goods without paying, or to obtain unauthorized funds from the obtained credit card account.

The problem that arises is the application of extraterritorial jurisdiction can not be used extensively by force or the will of Indonesia.

This is a legal research study that uses a conceptual approach (conceptual approach) as well as regulatory approach (statue approach) that will examine the principles of international law contained in the Convention on Cybercrime and Undang-undang Nomor 11 Tahun 2008 on Information and Electronic Transactions .

Based on the method used, it is known carding crime is transnational crime and necessary to prevent the application of extraterritorial jurisdiction, accompanied by an international treaty, that is the Convention on Cybercrime and adds several new provisions in the Undang-undang Nomor 11 Tahun 2008 on Information and Electronic Transactions accordance with the provisions of the convention.

I. PENDAHULUAN

Revolusi terjadi di berbagai bidang kehidupan manusia, seperti industri, budaya, pendidikan, teknologi, sistem informasi dan lain-lain. Sebagaimana yang pernah terjadi sebelumnya, revolusi kali ini juga membawa perubahan yang cepat dan cenderung mengubah nilai-nilai dan paradigma lama yang baku.

Kemajuan zaman dan perkembangan teknologi merupakan dua hal yang saling berbanding lurus. Artinya semakin maju suatu zaman, semakin berkembang pula teknologi yang digunakan dizaman tersebut. Kemajuan ini berpengaruh terhadap berbagai aspek kehidupan, baik segi positif maupun negatif.

Kecanggihan teknologi komputer telah memberikan kemudahan-kemudahan, terutama dalam membantu pekerjaan manusia. Dampak positif kemajuan teknologi informasi bisa dilihat dalam kehidupan sehari-hari. Antara lain, kemudahan dalam pekerjaan sehari-hari. Contoh yang paling sederhana, bisa kita lihat dalam program "*Word Processor*", semisal "*Microsoft Word, Open Office*, yang dengan berbagai fiturnya memberikan kemudahan-kemudahan dalam proses penuangan ide kebentuk tulisan jika dibandingkan dengan mesin ketik manual.[1]

Salah satu produk dari ilmu pengetahuan dan teknologi adalah teknologi informasi atau yang biasa dikenal dengan teknologi telekomunikasi. Teknologi telekomunikasi telah membantu umat manusia dalam berinteraksi dengan manusia yang ada pada komunitas lain dengan lebih mudah, dalam arti hal ini dapat dapat dilakukan dengan tanpa meninggalkan tempat atau komunitas di mana ia berada dan aktifitas ini dapat dilakukan di mana dan kapan saja.[2]

Sebagaimana lazimnya pembaharuan teknologi, internet selain memberi manfaat juga menimbulkan efek negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Hal itu terjadi pula untuk data dan informasi yang dikerjakan secara elektronik. Dalam jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas.

Sejalan dengan perkembangan zaman, kemajuan internet dan teknologi informasi menjadikan negara-negara di seluruh dunia seolah tanpa batas (*borderless*). Semuanya terhubung dalam satu kesatuan sistem. Akibatnya, untuk mengakses suatu alamat di negara lain, seseorang hanya perlu mengetikkan alamat *URL (Uniform Resource Locator)* yang dituju. Kemudian masukkan *user account* dan *password*, kita akan mendapatkan fasilitas-fasilitas yang disediakan oleh situs tersebut. Kemajuan ini ibaratnya pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif untuk melakukan perbuatan kriminal. Dalam menanggapi fenomena tersebut, dalam dunia hukum kemudian lahirlah apa yang dikenal dengan hukum siber atau *cyber law*.[3]

Transaksi bisnis yang dilakukan melalui internet disebut *e-commerce* (transaksi elektronik). Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.[4]

---

[1]Choirul Ihwan, 2006, **Carding Perspektif Hukum Positif dan Hukum Islam (online),** http://aristhu03.files.wordpress.com/2006/10/carding-perspektif-hukum-positif-dan-hukum-islam.pdf, (1 Juni 2013).

[2]Abdul Wahid dan Moh. Labib, **Kejahatan Mayantara (*Cyber Crime)***, Refika Aditama, Bandung, 2005, hal 23.

[3]Mansur, Dikdik M. Arief Mansur dan Elisatris Gultom, ***Cyber Law* Aspek Hukum Teknologi Informasi,** Refika Aditama, 2005, hal. 24.

[4] Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 tentang Penyelenggaraan sistem dan Transaksi Elektronik, 2012, hal 2.

Sekalipun kemajuan teknologi informasi memberikan banyak kemudahan bagi kehidupan manusia, tetapi kemajuan ini pun secara bersamaan menimbulkan berbagai permasalahan yang tidak mudah ditemukan jalan keluarnya. Salah satu permasalahan yang muncul akibat perkembangan teknologi informasi adalah lahirnya kejahatan-kejahatan yang sifatnya baru, khususnya yang menggunakan internet sebagai alat bantunya,[5] yang lebih dikenal *cybercrimes* (kejahatan dunia maya).

Akibat dari kejahatan dunia maya dapat lebih luas daripada tindak pidana konvensional, karena para pelaku tidak dibatasi oleh waktu dan geografis, oleh karena itu wilayah terjadinya tidak hanya secara lokal atau nasional tetapi juga transnasional dan internasional.

Kejahatan dunia maya yang akhir-akhir ini sering dilakukan adalah *carding*. *Carding* atau yang bisa disebut juga *credit card fraud* (penipuan kartu kredit) adalah:

> *...the fraudulent acquisition and/or use of debit and credit cards, or card details, for financial gain. Card fraud may involve acquiring legitimate cards from financial institutions by using false supporting documentation (application fraud), or stealing legitimate credit and debit cards. It may also involve phishing,1 card-not-present fraud, the creation of counterfeit cards, hacking into company databases to steal customer financial data, and card skimming.*[6]

Eksistensi *cybercrime* di dunia maya menimbulkan kesulitan tersendiri dalam proses penegakan hukum. Kesulitan yang timbul misalnya dalam menentukan tempat kejadian perkara (*locus delicti*). Tempat kejadian perkara (TKP) pada tindak pidana pencurian yang konvensional dapat dengan jelas diketahui, misalnya lokasi terakhir barang yang dicuri berada. Pihak yang merasa kehilangan dapat segera melapor kepada polisi untuk segera dilakukan olah TKP. Penyidik dapat dengan segera mengevakuasi TKP dan melakukan penyidikan dengan mengumpulkan barang-barang bukti dan petunjuk serta memanggil pihak laboratorium forensik untuk mencari sidik jari. Penyidik juga dapat mencari informasi dari saksi-saksi yang berada di sekitar TKP. Akan tetapi, tidak demikian halnya di dunia virtual atau *cyberspace*. Lokasi menjadi sulit ditentukan ketika dari negaranya, pelaku mencuri data warga negara asing. Penyidik juga mengalami kesulitan dalam mencari saksi yang melihat atau mendengar kejadian. Kesulitan lain timbul dalam hal mengumpulkan alat bukti. Pengumpulan alat bukti ini memerlukan biaya yang tidak sedikit karena harus menggunakan teknologi yang memadai dan dioperasikan oleh sumber daya manusia yang ahli.[7]

Menurut Richard Boscovich, pengacara senior dari unit *Digital Crimes Microsoft*:

> *The number one issue is that there is simply no homogenous legislation worldwide, and that's a function of nation-state, There has to be a corresponding statute in another country from which you are requesting information. If you look at international treaties, it has to be a crime in both countries for you to even get that evidence in or back to your own jurisdiction.*[8]

---

[5]Mansur, Dikdik M. Arief Mansur dan Elisatris Gultom, Ibid, hal. 22.

[6] Australian Crime Commission, 2013, ***Crimes in the Mainstream Economy: Card Fraud*** (online), http://www.crimecommission.gov.au/publications/organised-crime-australia/2013-report/crimes-mainstream-economy#top, (3 Desember 2013).

[7]Josua Sitompul, ***Cyberspace, Cybercrime, Cyberlaw:*** **Tinjauan Aspek Hukum Pidana,** PT. Tatanusa, 2012, hal 103.

[8] Lauren Moraski, 2011, ***Cybercrime Knows No Borders*** (online), http://www.infosecurity-magazine.com/view/18074/cybercrime-knows-no-borders-/, (26 November 2013).

Penanganan kejahatan transnasional mengharuskan dilakukan tidak oleh satu negara saja tapi melalui kerjasama antar negara. Kejahatan tidak lagi berhenti lagi di perbatasan. Namun dalam perjalanannya, kerjasama yang dijalin antar negara terkadang menemui kesulitan karenan terkait dengan kedaulatan sebuah negara, perbedaan budaya, bahasa serta perbedaan dalam sistem hukum.[9]

Organisasi internasional lain yang memerhatikan masalah hukum *e*-commerce ini salah satunya adalah negara-negara yang tergabung dalam Uni Eropa *(Council of Europe)* pada tanggal 23 November 2001 di kota Budapest, Hongaria telah membuat dan menyepakati *Convention on Cybercrime* yang kemudian dimasukkan dalam *european Treaty Series* dengan Nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi yang dilakukan oleh 3 (tiga) Negara Anggota *Council of Europe.* Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal *(criminal policy)* yang bertujuan untuk melindungi masyarakat dari *cyber crime,* baik melalui undang-undang domestik maupun kerjasama internasional.

Indonesia sendiri telah memiliki Undang-undang khusus untuk menangani kasus kejahatan dunia maya, yaitu Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang tersebut secara materi muatan telah dapat menjawab persoalan kepastian hukum menyangkut tindak pidana *carding, hacking* maupun *cracking* disertai dengan sanksi pidana atas tindakan-tindakan tersebut.

Dalam pencegahan kejahatan transnasional khususnya kejahatan *carding* diperlukan penggunaan prinsip-prinsip hukum internasional yang dapat diterapkan dalam pencegahan kejahatan *carding* dan perlunya tanggung jawab bersama antar negara dalam bentuk kerjasama internasional. Dari uraian latar belakang di atas maka penulis mengangkat tema tentang "**Pencegahan Kejahatan *Carding* sebagai Kejahatan Transnasional Menurut Hukum Internasional**".

II. RUMUSAN MASALAH

1. Mengapa kejahatan *carding* termasuk pada kejahatan transnasional dikaji dari perspektif hukum internasional?
2. Prinsip hukum internasional apa yang dapat mencegah kejahatan *carding* sebagai kejahatan transnasional?
3. Bagaimana perumusan norma hukum yang dapat mencegah kejahatan *carding* diharmonisasikan ke dalam undang-undang nomor 11 tahun 2008?

III. METODE PENELITIAN

Penelitian ini merupakan *legal research* dengan menggunakan pendekatan konseptual *(Conceptual Approach)* dan pendekatan perundang-undangan (*Statue Approach*). Dengan pendekatan konseptual peneliti akan menelaah asas-asas hukum internasional yang terdapat di dalam *Convention on Cybercrime* yang berguna untuk mencegah kejahatan *carding*. Pendekatan perundang-undangan digunakan untuk menelaah peraturan perundang-undangan yang berkaitan dengan pencegahan kejahatan *carding* yaitu Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan *Convention on Cybercrime* yaitu konvensi yang dibuat oleh *Council of Europe* dan terbuka bagi seluruh negara di dunia.

[9] Malikkul Shaleh, 2009, (online), http://news.unpad.ac.id/?p=29203, (18 November 2013).

Penelitian ini merupakan penelitian kepustakaan *(Library research),* yang sepenuhnya menggunakan bahan-bahan hukum (primer maupun sekunder) serta tulisan-tulisan dalam berntuk jurnal maupun artikel dalam media internet, sebagai kajian dalam menjelaskan rumusan masalah dalam penelitian ini

Bahan hukum primer dalam penelitian ini adalah peraturan perundang-undangan sebagai bahan analisis untuk penelitian ini didasarkan pada isinya yang memuat ketentuan hukum mengenai tindak pidana *cybercrime* baik yang mengatur hukum pidana formilnya maupun hukum pidana materiilnya yang meliputi:

a. *Convention on Cybercrime*, Budapest 23 November 2001
b. Kitab Undang-undang Hukum Pidana
c. Undang-undang Republik Indonesia Nomor 36 Tahun 1996 tentang Telekomunikasi
d. Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
e. Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Bahan hukum sekunder ini adalah bahan untuk penelitian yang relevan untuk mendukung dan memperjelas bahan hukum primer diatas, yang meliputi :

a. Pendapat para ahli hukum internasional mengenai prinsip-prinsip hukum internasional yang digunakan untuk mencegah kejahatan dunia maya
b. Pendapat para ahli hukum internasional mengenai kerjasama internasional dalam pencegahan kejahatan transnasional
c. Buku-buku yang membahas kejahatan dunia maya
d. Buku-buku hukum internasional.
e. Jurnal

Bahan hukum tersier dalam penelitian adalah bahan yang memberikan petunjuk terhadap bahan hukum primer dan sekunder seperti kamus hukum dan enslikopedia yang berkaitan dengan hukum internasional, khususnya mengenai *cybercrime* dan prinsip-prinsip hukum internasional.

Bahan hukum tersebut diatas yang digunakan oleh penulis dikumpulkan melalui studi kepustakaan dan mengumpulkan berbagai informasi yang terkait dengan kejahatan transnasional dan prinsip-prinsip hukum internasional yang masih relevan, serta mengumpulkan informasi penunjang mengenai pencegahan kasus *cybercrime* di Indonesia maupun di negara lain.

Teknik analisis bahan hukum dalam penulisan ini menggunakan interpretasi filosofis. Dalam penulisan ini akan menganalisis sifat kejahatan *carding* sebagai kejahatan transnasional, kemudian mengaitkan dengan asas-asas atau prinsip yang berlaku dalam hukum internasional. Analisis ini akan mencari asas hukum internasional yang dapat diterapkan dalam pencegahan kejahatan *carding*.

IV. PEMBAHASAN

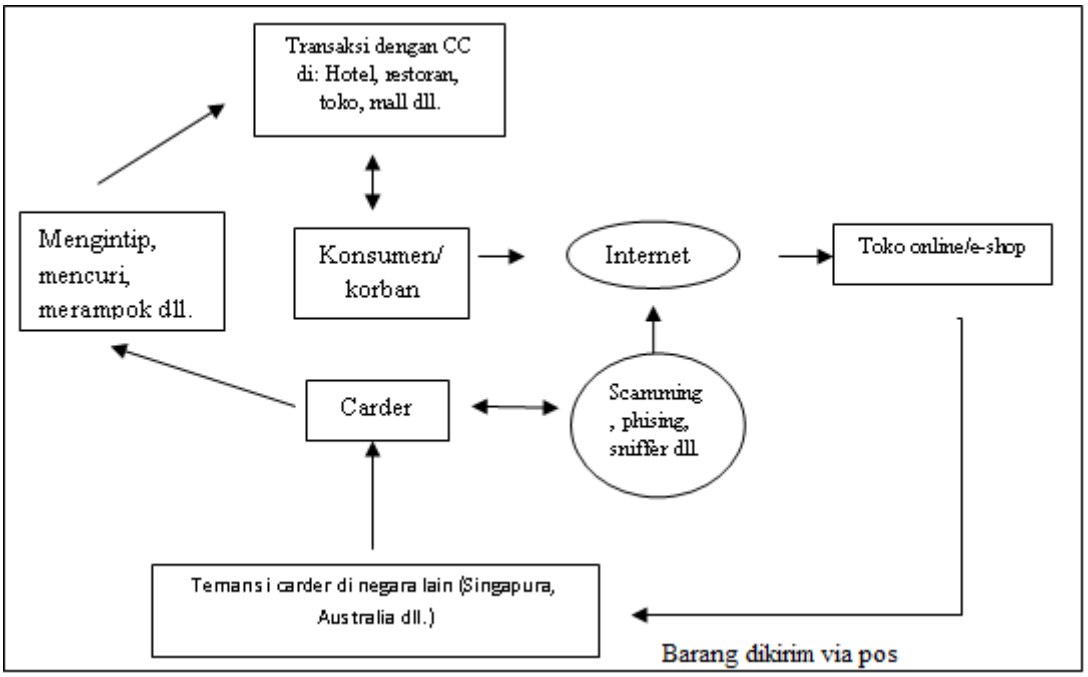
A. Kejahatan *Carding* Termasuk Pada Kejahatan Transnasional Dikaji Dari Perspektif Hukum Internasional

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.[10]

[10] 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.

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*).

Gambar 1
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.[11]

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 *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.

[11] 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).

Dari modus operandi tersebut dapat dilihat bahwa *carder* yang memanfaatkan teknologi internet dapat menjangkau para nasabah pemegang kartu kredit yang berada di luar negara dimana *carder* berada dan dapat 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.
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. Para *carder* bisa mendapatkan data-data kartu kredit dibantu oleh teman mereka di luar negeri yang bekerja di gerai ritel seperti restoran atau toko yang melayani pembayaran melalui kartu kredit. Mereka juga bisa mendapatkan data tersebut melalui forum-forum *carding* dengan memanfaatkan teknologi internet.
4. Kejahatan *carding* memiliki target yang berada di lebih dari satu negara.

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

Konvensi Wina tentang perjanjian 1969 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.

Adanya unsur-unsur internasional 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.[12]

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 terjadinya tindak pelanggaran tersebut tidak mengaturnya namun tetap merugikan pihak lain akibat tindak pelanggaran tersebut.[13]

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 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 :

---

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

[13] 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.

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."[14]

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*.

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

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*.[15] 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.

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

[14] Tsani, Mohd. Burhan, **Hukum dan Hubungan Internasional,** Liberty, Yogyakarta, 1990, hal 66-67.
[15] 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.

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, yaitu :

Computer Related Fraud : "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 : "Setiap orang dengan secara sadar menolong atau membantu pelanggaran yang ditetapkan dalam pasal 27-37"

International Co-operation, Kerjasama internasional dibutuhkan untuk proses penyidikan yang tidak berada di satu yurusdiksi 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.

V. PENUTUP

A. Kesimpulan

1. Kejahatan *carding* memiliki unsur-unsur yang sesuai dengan pasal 3 *United Nations Convention against Transnational Organized Crime*. Pertama, dilakukan di lebih dari satu negara. Kedua, dilakukan di suatu negara tetapi hal penting dari persiapan, perencanaan, pengarahan dan pengawasan dilakukan di negara lain. Ketiga, dilakukan di suatu negara tetapi melibatkan suatu kelompok kejahatan terorganisir (*organized criminal*) dimana kejahatan dilakukan di lebih satu negara. Keempat, dilakukan di suatu negara tetapi memiliki akibat di negara lain.

a. Dilakukan di lebih dari satu negara,

Pencurian data-data kartu kredit nasabah oleh para *carder* bisa dilakukan di beberapa negara.

b. Dilakukan di suatu negara tetapi hal penting dari persiapan, perencanaan, pengarahan, dan perngawasan dilakukan di negara lain,

Persiapan, perencanaan pengarahan dan pengawasan oleh pelaku kejahatan *carding* dilakukan di satu negara tetapi target kejahatan tersebut berada di luar negara dimana *carder* berada.

c. Dilakukan di suatu negara tetapi melibatkan suatu kelompok kejahatan terorganisir (*organized criminal*) dimana kejahatan dilakukan di lebih satu negara,

Para *carder* bisa mendapatkan data-data kartu kredit dibantu oleh teman mereka di luar negeri yang bekerja di gerai ritel seperti restoran atau toko yang melayani pembayaran melalui kartu kredit. Mereka juga bisa mendapatkan data tersebut melalui forum-forum *carding* dengan memanfaatkan teknologi internet.

d. Dilakukan di suatu negara tetapi memiliki akibat di negara lain

Kejahatan *carding* dapat menjangkau korban-korban yang berada di lebih dari satu negara.

2. Untuk melakukan upaya pencegahan kejahatan *carding* perlu adanya regulasi melalui suatu model norma-norma hukum internasional berupa adopsi prinsip-prinsip regulasi *cybercrime* yang bersifat global.

Dampak dari kejahatan *carding* yang melewati batas-batas yurisdiksi beberapa negara mengakibatkan masing-masing negara yang menjadi korban memiliki hak untuk menerapkan yurisdiksinya terhadap pelaku.

Maka prinsip hukum yang dapat mencegah kejahatan *carding* adalah prinsip ekstrateritorial serta didampingi dengan prinsip kerjasama internasional yang ada di dalam ketentuam-ketentuan *Convention on Cybercrime*.

3. Dalam perumusan norma hukum yang dapat mencegah kejahatan *carding* bisa mengacu pada ketentuan-ketentuan di dalam *Convention On Cybercrime*. Sebelumnya Indonesia harus meratifikasi terlebih dahulu konvensi tersebut agar terjalin kerjasama yang menjadi tujuan konvensi.

Indonesia perlu menambahkan menyesuaikan beberapa pasal dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sesuai dengan yang diatur dalam konvensi serta perlu adanya peraturan perlaksana dari Undang-undang tersebut.

B. Saran

Dalam upaya pencegahan *cybercrime* khususnya kejahatan *carding* diperlukan adanya norma hukum positif yang dapat menjangkau secara global. Indonesia memiliki beberapa alternatif strategi yang lebih efektif untuk mencegah kejahatan *carding*. Pertama, menyusun norma-norma hukum positif yang dapat menjangkau kejahatan teknologi informasi yang bersifat transnasional. Kedua, membuat regulasi melalui suatu model norma-norma hukum internasional berupa adopsi prinsip-prinsip regulasi *cybercrime* yang bersifat global. Ketiga, regulasi dibuat dengan terlebih dahulu melakukan ratifikasi atau akses terhadap *European Convention on Cybercrime*, Budapest, 2001, dan membuat peraturan implementasinya (*implementing legislation*) ke dalam instrumen hukum nasional.

DAFTAR PUSTAKA

Buku

Abdul Wahid dan Moh. Labib, **Kejahatan Mayantara (*Cyber Crime)***, Refika Aditama, Bandung, 2005.

Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer,* Jakarta: Sinar Grafika,1992.

Josua Sitompul, ***Cyberspace, Cybercrime, Cyberlaw:*** **Tinjauan Aspek Hukum Pidana,** PT. Tatanusa, 2012.

Mansur, Dikdik M. Arief Mansur dan Elisatris Gultom, ***Cyber Law*** **Aspek Hukum Teknologi Informasi,** Refika Aditama, 2005.

Tsani, Mohd. Burhan, **Hukum dan Hubungan Internasional,** Liberty, Yogyakarta, 1990.

Skripsi dan Makalah

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.

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.

Perundang-undangan

Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 tentang Penyelenggaraan sistem dan Transaksi Elektronik, 2012.

Internet

Australian Crime Commission, 2013, ***Crimes in the Mainstream Economy: Card Fraud*** (online), http://www.crimecommission.gov.au/publications/organised-crime-australia/2013-report/crimes-mainstream-economy#top, (3 Desember 2013).

Choirul Ihwan, 2006, **Carding Perspektif Hukum Positif dan Hukum Islam (online),** http://aristhu03.files.wordpress.com/2006/10/carding-perspektif-hukum-positif-dan-hukum-islam.pdf, (1 Juni 2013).

Lauren Moraski, 2011, ***Cybercrime Knows No Borders*** (online), http://www.infosecurity-magazine.com/view/18074/cybercrime-knows-no-borders-/, (26 November 2013).

Malikkul Shaleh, 2009, (online), http://news.unpad.ac.id/?p=29203, (18 November 2013).

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.

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).