

KEJAHATAN CARDING DALAM PERSPEKTIF UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (ITE) DI NEGARA REPUBLIK INDONESIA

Mohamad Rafi'ie
Fakultas Hukum, Universitas Darul Ulum, Jombang
mohrafiie.musy@gmail.com

Absrtak

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 dilakukan dengan tanpa meninggalkan tempat atau komunitas di mana ia berada dan aktifitas ini dapat dilakukan di mana dan kapan saja. 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. Dalam penelitian ini menggunakan metode penulisan normatif (*normative law research*), dengan teknik *perolehan data* dengan cara pengumpulan data melalui studi kepustakaan. 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. 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 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.

Keyword : *Kejahatan, Carding, Informasi dan Transaksi Elektronik*

CARDING CRIME THE PERSPECTIVE OF ELECTRONIC INFORMATION AND TRANSACTIONS LAW (ITE) IN COUNTRY REPUBLIC OF INDONESIA

Abstract

One of the products of science and technology is information technology or commonly known as telecommunications technology. Telecommunication technology has helped mankind in interacting with humans in other communities more easily, in the sense that this can be done without leaving the place or community where it is located and this activity can be done anywhere and anytime. This research is a legal research that uses a conceptual approach as well as a statutory approach which will examine the principles of international law contained in the Convention on Cybercrime and Law Number 11 of 2008 concerning Information and Electronic Transactions. This research uses normative law research, with data acquisition techniques by collecting data through library research. Based on the method used, it is known that carding is a transnational crime and to prevent it, it is necessary to apply extraterritorial jurisdiction accompanied by an international agreement, namely the Convention on Cybercrime and add several articles in Law Number 11 of 2008 concerning Information and Electronic Transactions in accordance with the provisions of the convention. The development of technology and the internet does not always produce positive things. Negative things which are side effects include carding crime (credit card theft) which is one type of crime in the cybercrime world. The loss of space and time limits in cyberspace changes many things. A carder can enter a server without permission (unauthorized access). The goal is to get goods without paying or to get unauthorized funds from credit card accounts obtained. The problem that arises is the application of extraterritorial jurisdiction which cannot be used widely by coercion or the will of Indonesia.

Keyword : *Crime, Carding, Information and Electronic Transactions*

A. Latar Belakang Masalah

Manusia hidup berdampingan, bahkan berkelompok-kelompok dan seiring mengadakan hubungan antar sesama. Hubungan ini terjadi berkenaan dengan kebutuhan hidup yang tidak mungkin selalu dapat dipenuhi sendiri. Kebutuhan hidup manusia bermacam-macam. Pemenuhan kebutuhan hidup tergantung dari hasil yang

diperoleh melalui daya upaya yang dilakukan untuk memperoleh kemakmuran dan kesejahteraan lahir dan batin.¹

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

¹ Djamali, R. Abdoel, *Pengantar Hukum Indonesia*, Jakarta, PT.Raja Grafindo Persada, 2011.

dalam program “*Word Processor*”, semisal “*Microsoft Word, Open Office*”, yang dengan berbagai fitur nya memberikan kemudahan-kemudahan dalam proses penuangan ide ke bentuk tulisan jika dibandingkan dengan mesin ketik manual.²

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 dilakukan dengan tanpa meninggalkan tempat atau komunitas di mana ia berada dan aktifitas ini dapat dilakukan di mana dan kapan saja dan kemajuan ilmu pengetahuan ini juga melahirkan sebuah gagasan baru dalam bertransaksi jual dan beli barang dan jasa.³

Kelebihannya, untuk mengakses suatu laman dalam internet kita hanya perlu menuliskan alamat *website* maupun *link* baik dari manapun dan kemanapun tak terbatas baik di Negara sendiri maupun 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*.⁴

Tidak terkecuali dengan kemajuan dalam ekonomi contohnya 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.⁵

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, yang lebih dikenal *cyber crime* (kejahatan dunia maya).⁶

Kenapa demikian, karna di Indonesia kini sudah memuat aturan perundang-undangan tentang informasi dan transaksi elektronik yang di dalamnya memuat seluruh aturan, kebijakan dan sanksi tegas bagi para pelanggarnya yaitu dimuat dalam peraturan Undang-Undang Republik Indonesia no 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik. Kejahatan ini potensial menimbulkan kerugian pada beberapa bidang antara lain bidang politik, ekonomi, sosial budaya, pertahanan dan keamanan yang signifikan. Bahkan di masa yang akan datang dapat mengganggu perekonomian nasional melalui jaringan infrastruktur yang berbasis teknologi elektronik seperti perbankan, telekomunikasi satelit, jaringan listrik, dan jaringan lalu lintas penerbangan dan sebagainya. Salah satu yang menarik untuk dibahas adalah kejahatan teknologi elektronik dalam perbankan khususnya di Indonesia.

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: berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet. Sebutan pelakunya adalah *Carder*. Sebutan lain untuk kejahatan jenis ini adalah *cyberfroud* alias penipuan di dunia maya. Menurut riset *Clear Commerce Inc*, perusahaan teknologi informasi yang berbasis di Texas – AS, Indonesia memiliki *carder* terbanyak kedua di dunia setelah Ukraina. Sebanyak 20 persen transaksi melalui internet dari Indonesia adalah hasil *carding*. Akibatnya, banyak

² Choirul Ihwan, *Carding Perspektif Hukum Positif dan Hukum Islam*, 2006, <http://aristhu03.files.wordpress.com/2006/10/carding-perspektif-hukum-positif-dan-hukum-islam.pdf>. (online). Diakses pada 1 agustus 2018

³ Abdul Wahid dan Moh. Labib, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung, 2005, hal. 23.

⁴ Mansur, Dikdik M. Arief Mansur, dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, 2005, hal. 24.

⁵ *Loc.cit* hal. 24.

⁶ *Loc.cit.* hal. 22.

situs belanja online yang memblokir *IP* atau *internet protocol* (alamat komputer internet) asal Indonesia. Kalau kita belanja online, formulir pembelian *online shop*.⁷

*“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.”*⁸

B. Rumusan Masalah

Berdasarkan uraian diatas maka penulis tertarik untuk mengkaji lebih jauh tentang kejahatan pencurian dengan media internet sehingga memilih untuk mengambil judul “Kejahatan Carding Dalam Perspektif Undang-Undang Informasi Dan Transaksi Elektronik (ITE) Di Negara Republik Indonesia”. adapun Rumusan Masalah 1. Bagaimana pengungkapan kejahatan *carding* di Indonesia? 2. Bagaimana ketentuan Undang-undang yang berlaku terhadap para pelaku *carding* atau *carder* di Indonesia?

C. Metode Penelitian

Penulis menggunakan metode penelitian hukum normatif (normative) atau disebut juga (*normative law research*). Metode penelitian ini juga bisa disebut metode penelitian hukum kepustakaan, yang pengertiannya sendiri merupakan metode atau cara yang dipergunakan di dalam penelitian hukum yang dilakukan dengan cara meneliti serta mengkaji studi dokumen dan berbagai bahan pustaka yang ada. Penelitian yang berfokus pada hukum normatif, dalam melakukan penulis melalui proses deduksi dan norma hukum

positif atau hukum obyektif dengan cara sistematis hukum. Sehingga penelitian hukum normatif berfokus pada inventarisasi hukum positif, asas-asas dan doktrin hukum, penemuan hukum dalam perkara *in concreto*, sistematis hukum, taraf sinkronisasi, perbandingan hukum dan sejarah hukum.⁹

Studi kepustakaan dilakukan dengan cara membaca, menelaah, mencatat membuat ulasan bahan-bahan pustaka yang ada kaitannya dengan kejahatan carding, baik bahan data primer maupun sekunder seperti bahan atau materi yang berkaitan dan menjelaskan mengenai permasalahan, buku, jurnal, dan juga literature yang terkait tentang kejahatan tindak pidana carding.

⁷ <https://balianzahab.wordpress.com/cybercrime/apa-itu-hacking-cracking-dan-defacing/>. (online) diakses pada 1 agustus 2018.

⁸ Australian Crime Commission, *Crimes in the Mainstream Economy: Card Fraud*, <http://www.crimecommission.gov.au/publications/organised-crime-australia/2013-report/crimes-mainstreameconomy/#top>, 2013, 3 Desember 2013. (online) diakses pada 1 agustus 2018.

⁹ Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*. Cet. 1. Bandung, PT. Citra Aditya Bakti, 2004, hal. 52.

PEMBAHASAN

A. Asas Peraturan Kejahatan Carding Dalam Hukum Pidana Indonesia

Carding merupakan sebuah tindak kejahatan pidana yang melawan hukum, hal ini didasarkan pada bentuk tindakan dan sebab yang terjadi dari kejahatan *carding* itu sendiri yaitu pencurian dan penyalahgunaan data dalam telekomunikasi. Dimana aturan hukumnya di Indonesia dimuat dalam KUHP (Kitab Undang-Undang Hukum Pidana) Bab XXII Tentang Pencurian pasal 362, KUHP (Kitab Undang-Undang Hukum Pidana) Bab XXV tentang perbuatan curang Pasal 378.

Kejahatan *carding* sesuai dengan yang dimuat dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Bab VII Tentang Perbuatan Yang Dilarang pada pasal 31 ayat 1 dan 2, sekaligus tinjauan dari ancaman hukum bagi para pelaku tindak pidana *carding* yang juga dimuat dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Bab XI Tentang Ketentuan Pidana pada pasal 47.¹⁰

Dalam kejahatan *carding* menerapkan asas hukum *lex specialis derogate legi generali* penjabarannya adalah asas penafsiran hukum yang menyatakan bahwa hukum yang bersifat khusus (*lex specialis*) sifatnya mengesampingkan hukum yang bersifat umum (*lex generalis*).¹¹ Menurut Bagir Manan mengenai prinsip yang harus diperhatikan dalam asas *lex specialis derogate legi generali* ada tiga, yaitu :Ketentuan-ketentuan yang didapati dalam aturan umum tetap berlaku kecuali diatur khusus dalam aturan hukum khusus.

1. Ketentuan-ketentuan *lex specialis* harus sederajat dengan ketentuan-ketentuan *lex generalis* (Undang-Undang dengan Undang-Undang).
2. Ketentuan-ketentuan *lex specialis* harus berada dalam lingkungan hukum (rezim) yang sama dengan *lex generalis*.¹²

¹⁰ Evi Lestari Situmorang, Kajian Yuridis Pembuktian Kejahatan Mayantara (Cyber Crime) Dalam Lingkum TransNasional (Studi Putusan), Universitas Utara Medan, 2014.

¹¹ <http://jokopas.blogspot.com/2013/09/asas-asas-dalam-peraturan-perundang.html>.(online) diakses pada 1 agustus 2018.

¹² Bagir Manan, *Hukum Positif Indonesia*, hal. 56.

Asas *lex specialis derogate legi generali* juga dimuat dalam KUHP (Kitab Undang-Undang Hukum Pidana) BAB VI Tentang Perbarengan Tindak Pidana Pasal 63 Ayat (2) yang berbunyi sebagai berikut :

“(2) Jika suatu perbuatan masuk dalam suatu aturan pidana yang umum, diatur pula dalam aturan pidana yang khusus, maka hanya khusus itulah yang diterapkan.”¹³

B. Kejahatan Carding Yang Telah Terjadi Di Indonesia

Dalam beberapa kasus yang telah terjadi di Indonesia tidak sediki pula kasus *carding* yang telah diungkap, namun terlepas dari seperti lama proses dari pengungkapan tersebut patutnya kepolisian beserta peradilan di negeri Indonesia sudah dapat membanggakan dimana pemberantasan kasus tersebut dan pemutusan dalam perkara tersebut telah menerapkan kebijakan yang seadil mungkin sesuai peraturan yang berlaku. Ada beberapa contoh kasus diantaranya ; Contoh dari beberapa kasus tersebut, ialah :

1. Pada September 2011, Polda Metro Jaya berhasil membongkar sindikat pemalsu Kartu Kredit dengan kerugian yang cukup besar Rp. 81 Miliar. Sindikat ini membobol data EDC kartu kredit dengan dua modus utama. Modus pertama, komplotan ini mencuri data dari pemilik EDC kartu kredit di pertokoan atau tempat-tempat transaksi lain. Kasus terbaru pencurian data EDC dari stasiun pengisian bahan bakar umum (SPBU) 3412203 Kebayoran Lama pada 18 Agustus hingga 9 September 2011. Polisi menyita ratusan kartu tanda penduduk palsu, puluhan kartu anjungan tunai mandiri palsu, belasan EDC kartu kredit, dan ijazah palsu.¹⁴
2. Pada April 2010, Aparat satuan Fiskal, Moneter, dan Devisa (Fismondev) Ditreskrimsus Polda Metro Jaya menangkap kawanan pemalsu kartu kredit. Dari kawanan

¹³ *Himpunan Tiga Kitab Utama Undang-Undang Hukum Indonesia*, Gramedia Widiasarana Indonesia, hal. 555.

¹⁴ <http://www.tempo.co/read/news/2011/09/30/064359105/Inilah-Pembobol-Kartu-Kredit-Senilai-Rp-81-Miliar>.(online) diakses pada 1 agustus 2018.

ini, polisi berhasil disita 266 kartu kredit palsu lokal dan internasional dengan total nilai Rp 2,5 miliar. Kawanannya memiliki mesin untuk mencetak kartu kredit palsu sendiri di sebuah rumah di Jalan Kartini, Mangga Besar Jakarta Pusat. Pemalsuan kartu kredit dilakukan dengan menggandakan data kartu kredit milik orang lain.

Data tersebut kemudian dimasukkan dalam kartu kredit palsu. Penangkapan kawanannya pemalsu kartu kredit ini bermula dari laporan seorang kasir di salah satu pusat perbelanjaan di Blok M yang curiga terhadap seorang pembeli yang menggunakan kartu kredit mereka yang bentuknya tidak seperti kartu kredit asli.¹⁵

3. Pada Juli 2010, Direktorat Reserse Kriminal Khusus menangkap karyawan kafe Starbucks Tebet Jakarta Selatan, DDB, 26 tahun yang terbukti melakukan pembajakan kartu kredit para pelanggannya. Pelaku mengumpulkan data kartu kredit dari konsumen tempatnya bekerja dengan cara struk diprint ulang dan dicatat kode verifikasinya. Dari situ pelaku berhasil menguasai ratusan data kartu kredit.

Data kartu kredit selanjutnya digunakan untuk membayar transaksi pembelian alat elektronik Ipad Nano dan Ipad Touch secara online di Apple Online Store Singapura hingga lebih dari 50 kali. Tersangka dijerat pasal 362 KUHP tentang penipuan dan atau pasal 378 KUHP tentang pencurian serta UU no. 11 tahun 2008 tentang ITE dengan ancaman penjara di atas lima tahun.¹⁶

C. Kejahatan Carding Ditinjau Dari KUHP

Sebagaimana yang telah penulis ulaskan dari tindak kejahatan *carding* dimana bentuk kejahatannya merupakan juga bisa diklasifikasikan

¹⁵

[\(http://www.tempo.co/read/news/2010/11/01/064288714/Kawanannya-Pemalsu-Kartu-Kredit-Ditangkap\)](http://www.tempo.co/read/news/2010/11/01/064288714/Kawanannya-Pemalsu-Kartu-Kredit-Ditangkap) diakses pada 1 agustus 2018.

¹⁶

[\(http://www.tempo.co/read/news/2010/07/19/064264510/Karyawan-Starbucks-Tebet-Bajak-Ratusan-Kartu-Kredit\)](http://www.tempo.co/read/news/2010/07/19/064264510/Karyawan-Starbucks-Tebet-Bajak-Ratusan-Kartu-Kredit), (online) diakses pada 1 agustus 2018.

kedalam bentuk tindak pidana kejahatan pencurian karena beberapa aspek hukum didalamnya yang juga disinggung di dalam KUHP.

Ini berkaitannya dengan kegiatan *carding* itu sendiri yaitu pengambilan data kartu kredit dari nasabah dengan bertujuan untuk menyalahgunakan atau memanfaatkan sebagian atau keseluruhan dari sejumlah atau keseluruhan *saldotabungannya* yang dimiliki oleh seorang nasabah kartu kredit dapat disimpulkan hal tersebut juga diatur dalam KUHP (Kitab Undang-Undang Hukum Pidana).

Tercantum di dalam BAB XXII Tentang Pencurian pasal 362 yang didalamnya diancam dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak RP. 900.00-¹⁷ (sembilan ratus rupiah), dan KUHP (Kitab Undang-Undang Hukum Pidana) Bab XXV tentang perbuatan curang Pasal 378 yang didalamnya diancam dengan pidana penjara paling lama empat tahun.¹⁸

Hal ini juga sebagai acuan bilamana kejadian atau kasus seperti ini terjadi di Indonesia dan dari adanya peraturan Perundang-Undangan beserta acara pidana khusus kurang signifikan untuk menyelesaikan kasus tersebut.

Karena acap kali beberapa kasus di Indonesia yang terkait *carding* kadangkala pihak majelis hakim memberikan putusan dengan salah satu pasal diatas dikarenakan disamping kurangnya bukti yang menguatkan pelaku juga melakukan kejahatan lain seperti disertai dengan perampokan, pemerkosaan, pembunuhan, sabotase, dan lain-lain sebagainya, yang dari sinilah kejahatan *carding* tidak semena-mena dalam putusan kasusnya diberlakukan dengan tindak pidana khusus. Kejadian seperti itu lumrah terjadi di Indonesia dikarenakan sebab dan akibat yang menyertai para pelaku *carder* dalam menjalankan aksinya melakukan kejahatan *carding*.

D. Prinsip Peraturan Dan Norma Hukum Kejahatan Carding

Kebijakan (policy) merupakan kata istilah yang digunakan sehari-hari, tetapi karena keterbiasaannya terdapat semacam kerancuan atau kebingungan dalam mendefinisikan atau menguraikan istilah tersebut. Istilah kebijakan lebih sering dan secara luas digunakan dalam kaitannya dengan tindakan-tindakan Pemerintah /penguasa

¹⁷ Kitab Undang-Undang Hukum Pidana dan Kitab Undang-Undang Hukum Acara Perdata, Efat Publshing, Hal. 278.

¹⁸ Ibid. Hal 284

serta perilaku Negara pada umumnya. Kebijakan sebenarnya dapat dirumuskan sebagai perilaku dari sejumlah pemeran baik pejabat atau perorangan, kelompok kekuatan politik atau kelompok pakar, ataupun lembaga pemerintah yang terlibat dalam suatu bidang kegiatan tertentu yang diarahkan pada permasalahan sehubungan dengan adanya hambatan-hambatan tertentu.¹⁹

Teknologi informasi dan media elektronika dinilai sebagai simbol pelopor mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial budaya, ekonomi dan keuangan. Dari sistem-sistem kecil lokal dan nasional, proses globalisasi dalam tahuntahun terakhir bergerak cepat, bahkan terlalu cepat menuju sistem *global*. Fenomena tindak pidana teknologi informasi merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. Tindak pidana teknologi informasi muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagaimana dikemukakan oleh Ronni R. Nitibaskara bahwa: “interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi semacam ini, penyimpangan hubungan sosial berupa kejahatan (*crime*) akan menyesuaikan bentuknya dengan karakter tersebut”.²⁰

Cybercrime adalah representasi dari kejahatan internasional yang menggunakan *hitech* karena ciri dan kejahatan yang paling menonjol adalah *borderless* atau tidak mengenal batas negara. Teknologi relatif tinggi artinya hanya orang-orang tertentu saja yang sanggup melakukan kejahatan ini serta open resources mediator atau dapat menjadi media untuk berbagai kejahatan antara lain kejahatan di bidang perbankan, pasar modal, seks, pembajakan hak-hak intelektual serta terorisme dan yang lebih tepat lagi termasuk transnational *crime*.²¹

Tindak pidana *cybercrime* cukup marak di Indonesia dan Kepolisian Republik Indonesia menyadari betul kerusakan yang diakibatkan oleh tindak pidana yang bersifat *borderless* ini. Untuk sementara ini, perhatian terutama diarahkan pada

tindak pidana *credit card fraud* atau yang populer dengan istilah *carding*. Penyalahgunaan kartu kredit dapat dilakukan dengan dua cara yaitu; (a) Kartu kredit sah tetapi tidak digunakan sesuai peraturan yang ditentukan dalam perjanjian yang telah disepakati oleh pemegang kartu kredit dengan bank sebagai pengelola kartu kredit. (b) Kartu kredit tidak sah/ palsu yang digunakan secara tidak sah pula. Data para *cracker* yang bermotifkan ekonomi atau sengaja menipu berbelanja pada *website-commerce* dengan menggunakan nomor-nomor kartu kredit milik orang lain, secara melawan hukum.²²

Di Indonesia sebelum diundangkannya Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur secara khusus tentang pemanfaatan teknologi informasi, sebenarnya Indonesia dalam persoalan *cybercrime* tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan-perbuatan yang berdimensi baru yang secara khusus belum diatur undang-undang.

Didalam Kitab Undang-Undang Hukum Pidana (KUHP) yang berlaku sekarang ini berasal dari *Wetboek van Strafrecht voor Nederlandsh Indie* (WvSNI) dengan berbagai perubahan untuk disesuaikan dengan keadaan Indonesia (Hindia-Belanda) saat itu. Sebagai sumber hukum pidana disamping sumber-sumber lainnya. Sistem peraturan perundang-undangan (*statutory rules*) yang ada di dalam KUHP sebagai induk aturan umum sehingga undang-undang khusus di luar KUHP terikat kepada ketentuan umum yang ada di dalam KUHP (buku 1).

KUHP terbagi atas aturan umum yang terdapat di dalam KUHP (buku 1), dan aturan khusus terdapat di dalam KUHP (Buku II dan III). Namun patut dicatat, bahwa ketentuan umum KUHP yang mengikat (yang berlaku) untuk undang-undang khusus, hanyalah Bab I sampai dengan VIII (Pasal 1 sampai dengan 85) Buku I KUHP, sepanjang undang-undang khusus tidak membuat ketentuan lain yang menyimpang. Ketentuan umum dalam Bab IX buku I KUHP (Pasal 86 sampai dengan 102) hanya berlaku untuk KUHP, tidak untuk undang-undang khusus di luar KUHP. Pasal-pasal yang dapat dikenakan dalam

¹⁹ Laica Marzuki, *Hukum dan Peraturan Kebijaksanaan (Beleidsregek)*. Yogyakarta: Tim UII Press. 2005. Hal 88.

²⁰ Tubagus Ronny Nitibaskara, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*, Jakarta: Peradaban, 2001, Hal 38

²¹ Anton, *Cyber Crime*, http://makalahcybercrimecarding.blogspot.co.id/2016/04/01_archive.html. (online) diakses pada 1 agustus 2018.

²² Rahmat Sahbani, *Kriminal Teknologi dalam* <http://karyakelompok.blogspot.co.id/2014/04/selamat-siang-pembaca-klikerkali-ini.html> diakses pada 1 agustus 2018.

KUHP yang mengkriminalisasi terhadap kejahatan dunia maya sebagaimana dijelaskan oleh Petrus Reinhard Golose adalah sebagai berikut :

1. Pasal 362 KUHP untuk kasus *carding* dimana pelaku mencuri kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *softwarecardgenerator* di internet untuk melakukan transaksi di *E-Commerce*.
2. Pasal 378 KUHP untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan.
3. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail*.
4. Pasal 331 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet. Modusnya adalah pelaku menyebarkan *e-mail* kepada teman korban tentang suatu cerita yang tidak benar atau mengirimkan *email* secara berantai melalui *mailinglist* tentang berita yang tidak benar.
5. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di internet dengan penyelenggara dari Indonesia.
6. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di internet.
7. Pasal 282 dan 311 KUHP dapat dikenakan untuk penyebaran foto atau film pribadi seseorang yang *vulgar* di internet.
8. Pasal 378 dan 362 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kredit yang nomor kartu kreditnya merupakan hasil curian.
9. Pasal 406 KUHP dapat dikenakan pada kasus *deface* suatu *website*, karena pelaku setelah berhasil memasuki *website* korban, selanjutnya melakukan

pengrusakan dengan cara mengganti tampilan asli dari *website* tersebut.²³

Dalam *Stufenbautheorie* yang dikemukakan Hans Kelsen dikatakan bahwa “peraturan hukum keseluruhannya diturunkan dari norma yang berada di puncak piramid, dan semakin ragam dan menyebar. Dengan demikian, peraturan puncak yakni Undang-Undang 1945 telah mendasari terbentuknya Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik. Penegak hukum mempunyai peranan strategis dalam penerapan hukum/efektivitas suatu aturan hukum. Setiap profesional hukum harus memiliki pengetahuan bidang hukum sebagai penentu bobot kualitas pelayanan hukum secara profesional. Penegak hukum mencakup komponen sistem peradilan pidana yang terdiri dari polisi, jaksa, hakim, advokat dan lembaga pemasyarakatan. Undang-undang atau perangkat hukum positif adalah *instrument* terakhir dalam menentukan berhasil atau tidaknya suatu penyidikan karena penerapan delik-delik hukum yang salah akan mementahkan penyidikan yang dilakukan. Walaupun penyidikannya sudah mampu dan memahami profil dan budaya para *hacker/preker* teknik-teknik serta modus operandi para *hacker/preker*, serta sudah didukung oleh *laboratorium* yang canggih sekalipun. H. Zainudin Ali mengestimasi kemungkinan-kemungkinan yang dapat dihadapi petugas penegak hukum dalam melaksanakan tugas penegakan hukum yaitu:

- a. Sampai sejauh mana petugas terikat dengan peraturan yang ada.
- b. Sampai batas-batas mana petugas berkenan memberikan kebijakan.
- c. Teladan macam apakah yang sebaiknya diberikan oleh petugas kepada masyarakat.
- d. Sampai sejauh manakah derajat sinkronisasi penugasan yang diberikan kepada para petugas sehingga memberikan batas-batas yang tepat pada wewenangnya.²⁴

²³ Petrus Reinhard Golose, *Perkembangan Cybercrime dan Upaya Penanggulangannya di Indonesia* oleh Polri, *Buletin Hukum Perbankan dan Kebanksentralan*, Volume 4 Nomor 2, Agustus 2006, hal 38-39.

²⁴ S. R Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya*, Jakarta: Alumni Ahaem, 1989, Hal 219

E. Prinsip Hukum Internasional Dalam Pencegahan Carding

Kejahatan *Cybercrime* ini telah masuk dalam daftar jenis kejahatan yang sifatnya transnasional berdasarkan *United Nation Convention Against Transnational Organized Crime (Palermo convention)* November 2000. Dalam Konvensi Wina tentang perjanjian 1969 tidak hanya sekedar merumuskan kembali atau mengkodifikasi 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. 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). Yurisdiksi 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. 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.²⁵

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 melampaui kedaulatannya (*act of sovereignty*) di dalam wilayah negara lain, kecuali dengan persetujuan negara itu sendiri. 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

²⁵ 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.

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 3.²⁶

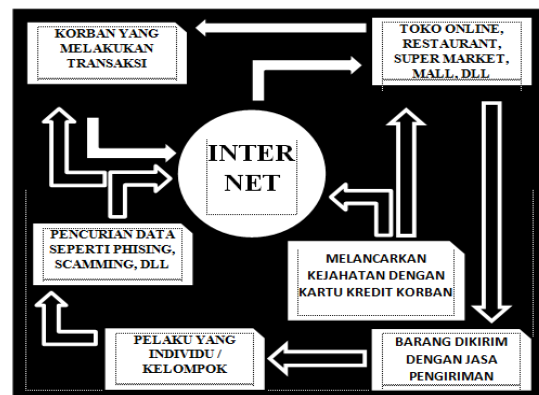
Perjanjian internasional Menurut Mohd. Burhan Tsani memiliki beberapa fungsi, itu :

- Untuk mendapatkan pengakuan umum anggota masyarakat bangsa-bangsa,
- Sarana utama yang praktis bagi transaksi dan komunikasi antar anggota masyarakat negara,
- Berfungsi sebagai sumber hukum internasional,
- Sarana pengembang kerjasama internasional secara damai.

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*.²⁷

Sebagai contoh gambaran untuk kegiatan dan alur dari kejahatan ini seperti contoh table dibawah²⁸

Tabel: Kejahatan Carding



F. Analogi Norma Hukum Internasional Dan Undang-Undang ITE

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 pengaturan *cybercrime*. 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. Dari gambar tabel di bawah ini, terdapat beberapa norma dari *Convention on Cybercrime* yang telah diadopsi ke dalam Undang-Undang 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.

²⁶ Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika, 1992, hal. 30.

²⁷ Tsani, Mohd. Burhan, *Hukum dan Hubungan Internasional*, Liberty, Yogyakarta, 1990, hal 66-67.

²⁸ Kasus Pencurian Data Kartu Kredit di Body Shop. Jakarta 2013(online), diakses pada 1 agustus 2018.

Tabel: Convention on Cybercrime

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

Maka perlu adanya penambahan pasal ke dalam UU ITE agar sesuai dengan ketentuan di dalam *Convention on Cybercrime*, 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 yurisdiksi negara saja, namun terdapat di beberapa negara. Di dalam *Convention on Cybercrime* terdapat beberapa ketentuan mengenai kerjasama 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 :

- Di wilayahnya; atau
- Di atas kapal yang berbendera pihak tersebut;
- Di atas kapal yang terdaftar menurut hukum pihak tersebut
- 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 melakukantindakan-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.

PENUTUP

A. Kesimpulan

Berdasarkan hasil kajian yang telah dijabarkan pada bab-bab sebelumnya, maka penulis dapat memberikan beberapa simpulan yaitu :

1. Penegakan hukum terhadap *carding* dalam anatomi kejahatan transnasional dilakukan karena kejahatan ini memiliki karakteristik lintas batas negara dan diakui oleh hukum internasional sebagai *transnational organized crime*. 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, pengarahannya 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. **Kelima**, Dilakukan di lebih dari satu negara, Pencurian data-data kartu kredit nasabah oleh para *carder* bisa dilakukan di beberapa negara. **Keenam**, Dilakukan di suatu negara tetapi hal penting dari persiapan, perencanaan, pengarahannya dan pengawasan dilakukan di negara lain, Persiapan, perencanaan pengarahannya dan pengawasan oleh pelaku kejahatan *carding* dilakukan di satu negara tetapi target kejahatan tersebut berada di luar negara dimana *carder* berada. **Ketujuh**, 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. **Kedelapan**, Dilakukan di suatu negara tetapi memiliki akibat di negara lain Kejahatan *carding* dapat menjangkau korban-korban yang berada di lebih dari satu negara

2. Tidak semua penegak hukum memiliki latar belakang pendidikan hukum, kurangnya mekanisme kontrol dan komponen peradilan pidana dalam setiap proses pemeriksaan perkara, penegak hukum yang menunjukan kurangnya keteladanan, penguasaan teknologi yang masih kurang, kerjasama penegak hukum antar negara yang belum efektif, hukum yang menyulitkan komunikasi dalam penegakan hukum serta rendahnya komitmen para penegak hukum di masing-masing negara untuk bekerja sama dalam menangani *carding* yang dalam negara Indonesia merupakan tindak pidana. Penegak hukum mempunyai peranan strategis dalam penerapan hukum/efektivitas suatu aturan hukum. Setiap profesional hukum harus memiliki pengetahuan bidang hukum sebagai penentu bobot kualitas pelayanan hukum secara profesional. Realisasi di lapangan, membuat kepolisian harus membuat back up anggota dan kuatnya perizinan kerjasama ekstradisi terhadap pelaku terkait penyelidikan dan penyidikan yang dilakukan diluar negeri.
3. Kepada penegak hukum khususnya Menteri Pertahanan, mulai menyusun norma-norma hukum positif yang dapat menjangkau kejahatan teknologi informasi yang bersifat transnasional. 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 Cyber crime*, Budapest, 2001, dan membuat peraturan implementasinya (*implementing legislation*) ke dalam instrumen hukum nasional.

B. Saran

Dari kesimpulan di atas maka, penulis memberikan saran;

1. Kepada Menteri Pertahanan, Tentara Negara Indonesia, Kepolisian, dalam rangka penegakan hukum terhadap *carding*, diperlukan adanya perjanjian internasional yang berlaku efektif, juga komitmen moral merupakan hal yang penting dalam penegakan hukum terhadap *carding* yang merupakan kejahatan transnasional, sebab tanpa bantuan negara lain, penegakan hukum tidak mungkin dilakukan.
2. Kepada penegak hukum khususnya hakim, format pidana penjara yang dijatuhkan kepada *carder* perlu diarahkan pada upaya resosialisasi karena biasanya *carder* jarang berteman dan bersosialisasi, agar kejahatan ini tidak terulang. 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*.

DAFTAR PUSTAKA

BUKU

Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*. Cet. 1. Bandung, PT. Citra Aditya Bakti, 2004

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.

Arrya Dwisatya Widigdha, *Carding For Beginner*, PT Elex Media Komputindo.

Bagir Manan, *Hukum Positif Indonesia*.

Djamali, R. Abdoel, *Pengantar Hukum Indonesia*, Jakarta, PT.Raja Grafindo Persada, 2011.

Laica Marzuki, *Hukum dan Peraturan Kebijaksanaan (Beleidsregek)*. Yogyakarta: Tim UII Press. 2005.

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

Peter Mahmud Marzuki, *Penelitian Hukum*, Cet. 2, Jakarta, Kencana. 2008.

Petrus Reinhard Golose, *Perkembangan Cybercrime dan Upaya Penanggulangannya di Indonesia oleh Polri*, Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006.

S. R Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya*, Jakarta: Alumni Ahaem, 1989.

Soeparna, Intan Innayatun, *Kejahatan Telematika Sebagai kejahatan Transnasional, Prospek Antisipasi dan Penanganan Kejahatan Telematika Pasca Diundangkannya UU ITE Nomor 11 Tahun 2008* Fakultas Hukum Universitas Airlangga, Surabaya, 30 Agustus 2008.

Tubagus Ronny Nitibaskara, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*, Jakarta: Peradaban, 2001.

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

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.

PERATURAN PERUNDANG-UNDANGAN

Himpunan Tiga Kitab Utama Undang-Undang Hukum Indonesia, Gramedia Widiasarana Indonesia

Internasional telecommunication Union Toolkit For Cybercrime Legislation, February 2010.

Kitab Undang-Undang Hukum Pidana dan Kitab Undang-Undang Hukum Acara Perdata, Efata Publishing.

Undang-Undang Republik Indonesia Tentang Informasi dan Transaksi Elektronik.

JURNAL

Evi Lestari Situmorang, *Kajian Yuridis Pembuktian Kejahatan Mayantara (Cyber Crime) Dalam Lingkum TransNasional (Studi Putusan)*, Universitas Utara Medan, 2014.

Leo T. Panjaitan, *Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008*, Teknik Elektro, Universitas Mercu Buana, Jakarta.

INTERNET

Anton, *Cyber Crime*,

- http://makalahcybercrimecarding.blogspot.co.id/2016/04/01_archive.html.(online) diakses pada 1 agustus 2018.
- Australian Crime Commission, *Crimes in the Mainstream Economy: Card Fraud*, <http://www.crimecommission.gov.au/publications/organised-crime-australia/2013-report/crimes-mainstreameconomy#top>, 2013, 3 Desember 2013. (online) diakses pada 1 agustus 2018.
- Choirul Ihwan, *Carding Perspektif Hukum Positif dan Hukum Islam*, 2006, <http://aristhu03.files.wordpress.com/2006/10/carding-perspektif-hukum-positif-dan-hukum-islam.pdf>. (online) 1 agustus 2018.
- Rahmat Sahbani, *Kriminal Teknologi dalam* <http://karyakelompok.blogspot.co.id/2014/04/selamat-siang-pembaca-klikerkali-ini.html> diakses pada 1 agustus 2018.
- <https://balianzahab.wordpress.com/cybercrime/ap-a-itu-hacking-cracking-dan-defacing>. (online) diakses pada 1 agustus 2018.
- <http://bisnis.liputan6.com/read/544093/kronologi-kasus-pencurian-data-kartu-kredit-di-body-shop>. (online) diakses pada 1 agustus 2018.
- <http://cybernity1.blogspot.nl/2014/04/pengertian-carding-dan-contoh-kasus.html>.(online) diakses pada 1 agustus 2018.
- <http://cybernity1.blogspot.nl/2014/04/pengertian-carding-dan-contoh-kasus.html>. (online) diakses pada 1 agustus 2018.
- <http://isparmo.web.id/2008/06/06/mengenal-dunia-hacking-sniffing/>. (online) diakses pada 1 agustus 2018.
- <http://jokopas.blogspot.com/2013/09/asas-asas-dalam-peraturan-perundang.html>.(online) diakses pada 1 agustus 2018.
- <http://www.tempo.co/read/news/2011/09/30/064359105/Inilah-Pembobol-Kartu-Kredit-Senilai-Rp-81-Miliar>.(online) diakses pada 1 agustus 2018.
- <http://www.tempo.co/read/news/2010/11/01/064288714/Kawanan-Pemalsu-Kartu-Kredit-Ditangkap>.(online) diakses pada 1 agustus 2018.
- <http://www.tempo.co/read/news/2010/07/19/064264510/Karyawan-Starbucks-Tebet-Bajak-Ratusan-Kartu-Kredit>. (online) diakses pada 1 agustus 2018.
- Kasus Pencurian Data Kartu Kredit di Body Shop. Jakarta 2013. (online), diakses pada 1 agustus 2018.