PANJI KEADILAN
Jurnal Ilmiah Nasional Mahasiswa Hukum
Universitas Muhammadiyah Bengkulu
P-ISSN: 2599-1892, E-ISSN: 2622-3724
Volume 3, Nomor 1, Januari 2020

PENAL *POLICY* DALAM UPAYA PREVENTIF KEJAHATAN *CARDING* DI INDONESIA

Nugroho Wisnu Pujoyono
Magister Ilmu Hukum Universitas Riau, email: ayahyangbaik@gmail.com

ABSTRAK

Kejahatan *carding* adalah suatu aktivitas untuk mendapatkan nomer-nomer kartu kredit orang lain yang digunakan untuk berbelanja di internet secara tidak sah atau illegal. *carding,* sebuah ungkapan mengenai aktivitas berbelanja secara maya (lewat komputer), dengan menggunakan, berbagai macam alat pembayaran yang tidak sah. Untuk mengurangi atau menghilangkan kemungkinan terjadinya suatu kejadian buruk yang tidak diinginkan di masa depan, sesuatu hal antisipasi yang dilakukan sebelum terjadinya sesuatu hal yang buruk yang tidak diinginkan maka ada upaya penal *policy* yaitu dengan cara bertindak atau kebijakan dari negara (pemerintah) untuk menggunakan hukum pidana dalam mencapai tujuan tertentu, terutama dalam menanggulangi kejahatan, memang perlu diakui bahwa banyak cara maupun usaha yang dapat dilakukan oleh setiap negara (pemerintah) dalam menanggulangi kejahatan. Rumusan Masalah Bagaimanakah penal *policy* dalam upaya preventif kejahatan *carding*, Proses hukum pidana dalam menyelesaikan kejahatan *carding.* Jenis penelitian ini adalah Penelitian hukum normatif menggunakan analisis kualitatif. Hasil penelitian yaitu penal *policy* dalam upaya preventif kejahatan *carding* di Indonesia adalah 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 agar kartu kredit tidak dibobol. Proses hukum pidana dalam menyelesaikan kejahatan *carding* yaitu Pada UU ITE dimuat tentang perbuatan yang dilarang pada Pasal 27 sampai Pasal 36. pada pasal 42 UU ITE diatur pula mengenai ketentuan penyidikan berdasar Pasal 183 KUHAP.

Kata kunci: penal policy; preventif; kejahatan; carding

ABSTRACT

Carding crime is an activity to get other people's credit card numbers that are used to shop on the internet illegally or illegally.Carding, an expression of virtual shopping activities (via computer), by using various kinds of illegal payment instruments. To reduce or eliminate the possibility of an unwanted bad event in the future, something anticipated that is done before something bad happens that is not desired then there is a Penal Policy effort that is by way of action or policy from the state (government) to use the law Crime in achieving certain goals, especially in tackling crime, it needs to be recognized that there are many ways and efforts that can be done by each country (government) in tackling crime. Formulation of the Problem How is Penal Policy in the Preventive Efforts of Carding Crimes, Criminal Legal Process in Resolving Carding Crimes. This type of research is normative legal research using qualitative analysis. The results of the study are Penal Policy in Preventive Efforts for Carding Crimes in Indonesia, it is necessary to strengthen Law Number. 11/2008. Strengthening the law is intended to streamline the preventive function, so that these crimes no longer arise so credit cards are not broken into. Criminal Legal Process in Resolving Carding Crimes, namely the ITE Law contains the prohibited acts in Article 27 to Article 36. In article 42 the ITE Law also regulates the provisions of the investigation based on Article 183 of the Criminal Procedure Code.

Keywords: *policy; preventive; crime; carding*

PENDAHULUAN

Perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK) yang cukup pesat sekarang ini sudah menjadi realita sehari-hari bahkan merupakan tuntutan masyarakat yang tidak dapat ditawar lagi. Tujuan utama perkembangan iptek adalah perubahan kehidupan masa depan manusia yang lebih baik, mudah, murah, cepat dan aman. Perkembangan iptek, terutama teknologi informasi *(information technology)* seperti internet sangat menunjang setiap orang mencapai tujuan hidupnya dalam waktu singkat, baik legal maupun illegal dengan menghalalkan segala cara karena ingin memperoleh keuntungan. Dampak buruk dari perkembangan "dunia maya" ini tidak dapat dihindarkan dalam kehidupan masyarakat modern saat ini dan masa depan. [1].

Tindak pidana atau kejahatan ini adalah sisi paling buruk di dalam kehidupan moderen dari masyarakat informasi akibat kemajuan pesat teknologi dengan meningkatnya peristiwa kejahatan komputer, informasi sampah, bias informasi, *hacker, cracker* dan sebagainya. Didalam dunia maya sangat banyak pihak-pihak yang mencari keuntungan tanpa memperdulikan segala sesuatunya entah itu merugikan orang lain, masyarakat atau pihak yang tidak tersangkut secara langsung, hukum pidana merupakan suatu peraturan yang menentukan segala perbuatan apapun yang di larang dan termasuk dalam kategori tindak pidana atau kriminal, serta menentukan sebuah hukuman yang pantas bagi pelakunya sesuai dengan peratuan perundang-undangan yang berlaku dalam suatu negara. Perkembangan jaman melahirkan kejahatan baru di bidang teknologi informasi, faktor yang mempengaruhi diantaranya;[2] *Pertama*, dari segi teknis, tidak bisa dipungkiri bahwa kemajuan teknologi (teknologi informasi) berdampak negatif bagi perkembangan masyarakat. Berhasilnya teknologi tersebut menghilangkan batas wilayah negara menjadikan dunia ini menjadi begitu sempit keterhubungan antara jaringan yang satu dengan jaringan yang lain memudahkan bagi si pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan yang satu lebih kuat daripada yang lain. Kelemahan tersebut dimanfaatkan oleh mereka yang tidak bertanggung jawab untuk melakukan kejahatan. *Kedua*, faktor sosio ekonomi,

[1] Ridhokudik. Artikel Tentang CyberLaw dalam http://ridhosukamusik.co.id/2010/10/artikel-tentang-cyber-law.html

[2] *Op. Cit,* Wisnubroto, Aloysius.

Panji Keadilan Jurnal Ilmiah Nasional Mahasiswa Hukum
P-ISSN: 2599-1892, E-ISSN: 2622-3724
Volume 3, Nomor 1, Januari 2020

cybercrime merupakan produk ekonomi. Isu global yang kemudian dihubungkan dengan kejahatan tersebut adalah keamanan jaringan *(security network).* Kemanan jaringan merupakan isu global yang digulirkan berbarengan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. *Cybercrime* berada dalam skenario besar dari kegiatan ekonomi dunia. Lihat saja pengalaman kita pada saat memasuki tahun 2000. Isu virus Y2K yang akan menghilangkan (menghapuskan) data dan informasi ternyata tidak pernah terjadi. Hal ini tentu saja menguatirkan dunia perbankan dan pasar modal. Berbondong-bondonglah para penyedia jasa tersebut untuk memberikan jaminan keamanan bahwa data dan informasi yang ada telah terbebas dari Y2K. Salah satu kejahatan *cybercrime* dengan menggunakan kartu kredit ialah *carding*.

Carding adalah suatu aktivitas untuk mrndapatkan nomer-nomer kartu kredit orang lain yang digunakan untuk berbelanja siinternet secara tidak sah atau illegal. *Carding*, sebuah ungkapan mengenai aktivitas berbelanja secara maya (lewat komputer), dengan menggunakan, berbagai macam alat pembayaran yang tidak sah. pada umumnya carding identik dengan transaksi kartu kredit, dan pada dasarnya kartu kredit yang digunakan bukan milik si carder tersebut akan tetapi milik orang lain. Artinya, para pelaku *carding* mencuri nomor-nomor kartu kredit dan tanggal *exp-date* yang biasanya didapat dari hasil carding dan lain-lain.sebuah tindakan yang diambil untuk mengurangi atau menghilangkan kemungkinan terjadinya suatu kejadian yang tidak diinginkan di masa depan. untuk suatu transaksi dan lain sebagainya merupakan kejahatan digital.[3]

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 pemegan kartu kredit dengan bank sebagai pengelola kartu kredit. (b) Kartu kredit tidak sah atau palsu yang digunakan secara tidak sah pula.[4]

Upaya preventif kejahatan *carding* dengan mengguanakan instrument hukum sangat identik dengan dunia maya, yaitu sesuatu yang tidak terlihat dan semu, Hal ini akan menimbulkan kesulitan bagi para penegak hukum terkait dengan

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

[4] Lestari, Endah. 2012. Tinjauan Yuridis Kartu Kredit di Indonesia. *Jurnal 2012. Surabaya; Universitas Narotama Surabaya*

pembuktian dan penegakan hukum atas kejahatan dunia maya. Selain itu obyek hukum *cyber* adalah data elektronik yang sangat rentan untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik.[5]

Oleh karena itu, kegiatan siber meskipun bersifat virtual dan maya dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis untuk ruang siber sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi hukum konvensional untuk dapat dijadikan objek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Karena kegiatan ini berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.

Berdasarkan uraian latar belakang diatas, penulis tertarik untuk mengkaji permasalahan tersebut dengan judul "Penal *Policy* dalam Upaya Preventif Kejahatan *Carding* di Indonesia" dengan rumusan masalah bagaimanakah penal *policy* dalam upaya preventif kejahatan *carding* di Indonesia dan bagaimanakah proses hukum pidana dalam menyelesaikan kejahatan *carding* di Indonesia.

[5] Anton, Cyber Crime, dalam http://cybercrimecarding.co.id/2016_04_01 archive.html

METODE PENELITIAN

Jenis penelitian yang digunakan dalam pokok permasalahan ini adalah penelitian hukum normatif, hal ini dimaksudkan agar peneliti sejauh mungkin dapat mengetahui apa yang menjadi alat ukur dalam membahas penelitian ini, sehingga dapat mencari setitik kebenaran tujuan dalam penelitian ini. penelitian normatif adalah penelitian terhadap kaedah dan asas hukum yang ada.

Penelitian hukum dengan menggunakan metode penelitian normatif yaitu dengan menganalisis data seeara kualitatif dengan cara menganalisis bahan-bahan hukum yang telah terkumpul dan mengelolah secara sistematis.

PEMBAHASAN

Penal *Policy* dalam Upaya Preventif Kejahatan *Carding* di Indonesia

Usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Jadi kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal. Dengan perkataan lain, dilihat dari sudut

Panji Keadilan Jurnal Ilmiah Nasional Mahasiswa Hukum
P-ISSN: 2599-1892, E-ISSN: 2622-3724
Volume 3, Nomor 1, Januari 2020

politik kriminal, maka politik hukum pidana identik dengan pengertian "kebijakan penanggulangan kejahatan dengan hukum pidana". Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya juga merupakan bagian dari usaha penegakan hukum (khususnya penegakan hukum pidana). Oleh karena itu, sering pula dikatakan bahwa politik atau kebijakan hukum pidana merupakan bagian pula dari kebijakan penegakan hukum *(law enforcement policy).*[6]

Dilihat dari kebijakan kriminal (kebijakan penanggulangan kejahatan), hukum pidana bukan merupakan sarana kebijakan yang utama/strategis. Kebijakan yang mendasar/strategis adalah mencegah dan meniadakan faktor-faktor penyebab atau kondisi yang menimbulkan kejahatan.[7]

Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cybercrime*) tentunya tidak dapat dilakukan secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistemik. Sebagai salah satu bentuk dari *high tech crime*, merupakan hal yang wajar jika upaya penanggulangan *cyber crime* (CC) jugaharus ditempuh dengan teknologi *(techno prevention).* Disamping itu diperlukan pula pendekatan budaya/ kultural, pendekatan moral/edukatif, dan bahkan global (kerjasama internasional) karena *cyber crime* dapat melampaui batas-batas negara (bersifat *transnational/transborder*).[8]

Walaupun sarana penal mempunyai keterbatasan, namun dilihat dari sudut "perencanaan kebijakan penanggulangan kejahatan dengan hukum pidana" (penal *policy*), tahap kebijakan legislasi/formulasi merupakan tahap paling strategis. Kesalahan/kelemahan kebijakan legislatif merupakan kesalahan strategis yang dapat menjadi penghambat upaya pencegahan dan penanggulangan kejahatan pada tahap aplikasi dan eksekusi.[9]

Di samping itu, usaha penanggulangan kejahatan lewat pembuatan undang-undang (hukum) pidana pada hakikatnya juga me-rupakan bagian integral dari usaha perlindungan masyarakat *(social welfare).* Oleh karena

[6] M. Cherif Bassiouni, *Op. Cit.,* hlm. 82-84.

[7] Barda Nawawi Arief, A. 2007. Kebijakan Hukum Pidana Menghadapi Perkembangan Cyber Crime di Bidang Kesusilaan (Cybersex/Cyberporn). *Makalah dalam Seminar Nasional Cybercrime dan Cybersex/Cyberporn Dalam Perspektif Hukum Teknologi dan Hukum Pidana. Kerja sama BPHN Depkumham & S2 Hukum Undip Semarang,* hlm 51.

[8] Barda Nawawi, Tindak Pidana Mayantara: *Perkembangan Cyber Crime di Indonesia*, Jakarta; RajaGrafindo Persada, 2006. hlm. 182-183.

[9] Barda Nawawi Arief, "*Kebijakan Hukum Pidana*...", *Op. Cit.* hlm. 53.

itu, wajar pulalah apabila kebijakan atau politik hukum pidana juga merupakan bagian integral dari kebijakan atau politik sosial *(social policy).*

Kebijakan sosial *(social policy)* dapat diartikan sebagai segala usaha yang rasional untuk mencapai kesejahteraan masyarakat dan sekaligus mencakup perlindungan masyarakat. Jadi di dalam pengertian "*social policy*", sekaligus tercakup di dalamnya "*social welfare policy*" dan "*social defence policy*".

Internet masuk ke Indonesia pada kisaran tahun 1990-an dan pada masa itu pula diperkirakan awal mulainya tindak kejahatan carding di Indonesia. Seperti halnya pisau, Internet merupakan pisau bermata dua. Ia bisa membawa manfaat maupun membawa keburukan. Berkat masuknya Internet ke Indonesia inilah, tindak carding pun lahir. Awalnya, *carding* dapat dilakukan dengan lebih mudah dari pada masa kini. Hal ini dikarenakan pada masa awal Internet masuk ke Indonesia, saat seorang carder ingin melakukan transaksi, mereka tidak harus memasukkan CVV, yaitu kode keamanan empat digit (pada *American Express* ada lima digit) yang tertera pada kartu kredit sebagai langkah preventif untuk meminimalkan tindak penipuan di dunia maya, sehingga carder akan lebih leluasa untuk mendapatkan barang yang mereka inginkan. Berbeda dengan transaksi pada masa kini yang kebanyakan membutuhkan CW sebagai salah satu syarat dalam bertransaksi, akibatnya gerak-gerik carder menjadi sedikit terbatasi bila ia tak memiliki CVV dari kartu kredit yang ia dapatkan.

Upaya-upaya preventif merupakan tindak lanjut dari upaya pre-emtif yang masih dalam tataran pencegahan sebelum terjadinya kejahatan. Dalam upaya preventif ditekankan adalah menghilangkan kesempatan untuk dilakukannya.Contoh ada orang ingin mencuri, melakukan pembajakan, pemalsuan dan lain-lain tetapi kesempatan itu dihilangkan dengan memberikan pengamanan dengan teknologi.Dengan demikian kesempatan itu dan tidak akan terjadi kejahatan. Jadi dalam upaya preventif kesempatan ditutup. Adapun upaya yang dilakukan agar kejahatan *carding* dalam database tidak meluas[10] :

1. Usahakanlah untuk membuat file database tidak bisa diakses melalui direktori publik, hindari meletakan file database pada *web root.*
2. Buatlah permission untuk mengakses database pada sebuah direktori khusus, hal ini akan mencegah orang lain mendownload file database.

[10]Vyctoria, 2013. *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*, Andi Yogyakarta, hlm. 210.

Panji Keadilan Jurnal Ilmiah Nasional Mahasiswa Hukum
P-ISSN: 2599-1892, E-ISSN: 2622-3724
Volume 3, Nomor 1, Januari 2020

3. Jangan gunakan database default, ubah menjadi nama lain yang anda rasa aman.
4. Hapus atau gantilah nama file yang sedikit riskin, misalnya cmd.exe, cart32.exe, atau lainnya.

Upaya preventif agar kartu kredit tidak dibobol. Bagi anda para pengguna kartu kredit, janganlah membuang kertas apapun yang tertera nomor kartu kredit anda dengan sembarang, termasuk struk belanja dan sebagainya. Sebisa mungkin potong-potonglah sekecil mungkin sebelum anda membuangnya. Khususnya untuk korporasi, penulis menyarankan untuk menggunakan paper shedder. Alat tersebut berguna untuk memotong kertas-kertas yang dirasa mengandung data atau informasi penting sebelum dibuang. Anda juga bisa menghancurkan kertas-kertas tersebut dengan membakarnya.[11]

Upaya Preventif dalam menjaga keamanan dari penipuan melalui email dan web palsu. Hal yang paling sederhana dan perlu anda lakukan adalah mengecek dengan benar nama situs yang anda buka. Jika anda menerima email dari pihak yang mengaku dari bank, sebaiknya periksa keabsahan email dengan cara sesegera mungkin menghubungi pihak bank untuk mengonfirmasi apakah email tersebut benar dari pihak bank atau bukan.[12]

Proses Hukum Pidana dalam Menyelesaikan Kejahatan *Carding* di Indonesia

Penegakan hukum tidak dapat dilepaskan dengan peranan atau fungsi peradilan[13], karenanya peradilan yang baik dan teratur serta mencukupi kebutuhan adalah suatu keharusan di dalam susunan negara hukum. Peradilan adalah salah satu urusan di dalam rumah tangga negara yang teramat penting. Segala peraturan yang diciptakan di dalam suatu negara, guna menjamin keselamatan masyarakat dan yang menuju pada tercapainya kesejahteraan rakyat, peraturan-peraturan itu tak akan memberikan faedah, apabila tidak ada suatu tahapan (instansi), yang harus memberikan isi dan kekuatan kepada kaidah-kaidah hukum, yang diletakkan di dalam undang-undang dan

[11] *Ibid*., hlm. 236.

[12] Vyctoria*., Op. Cit.* hlm. 220.

[13] Sjachran Basah, 1985, *Eksistensi dan Tolok Ukur Badan Peradilan Administrasi di Indonesia*, Alumni, hlm. 22, menyatakan: "Istilah pengadilan dan peradilan apabila dilihat dari sudut bentuk katanya, berasal dari kata dasar "adil" yang mendapat beberapa imbuhan {affix),secara sekaligus (simulfix) berupa awalan (prefix): "pe" dan "per", serta akhiran (suffix): "an". Terhadap kedua macam istilah itu, R. Subekti dan R. Tjitrorosubeno pada pokoknya menyatakan bahwa pengadilan (rechtbank) atau court menunjuk kepada badan, sedangkan peradilan (rechtspraak) atau judiciary menunjuk kepada fungsinya.

Iain-lain peraturan hukum; jikalau tidak ada pihak yang dengan keputusannya atas dasar undang-undang dapat memaksa orang mentaati segala peraturan negara, dan menjadi forum, dimana segala penduduk dapat mencari keadilan serta penyelesaian persoalan-persoalan tentang hak dan kewajibannya masing-masing menurut hukum.[14]

Dua muatan besar yang diatur dalam UU ITE ialah mengenai pengaturan tranksaksi elekronik dan mengenai tindak pidana siber. Materi UU ITE tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional.Pada UU ITE dimuat tentang perbuatan yang dilarang pada Pasal 27 sampai Pasal 36. Pada pasal 42 UU ITE diatur pula mengenai ketentuan penyidikan yang berbunyi: "penyidikan sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam undang-undang ini". Dengan demikian, sistem pembuktian yang dianut adalah sistem/teori pembuktian berdasar undang-undang secara negatif, yaitu sistem yang dianut dalam KUHAP dan berdasar Pasal 183 KUHAP, yang berbunyi sebagai berikut: "hakim tidak boleh menjatuhkan pidana kepada sesorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yangsah ia memperoleh keyakinan bajwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya".[15]

Sebagai contoh Pada tahun 2003 ada 3 laporan kepolisian yang ditangani kasus carding di Provinsi Jawa Barat. Penyidikan ini sesuai dengan kebijakansanaan Dir Reskrim Polda Jawa Barat. Dalam Pembuktian Pidana kasus penyalahgunaan kartu kredit menggunakan internet brerdasarkan urutan alat-alat bukti sebagaimana tercantum dalam pasal 184 KUHAP. Selanjutnya disampaikan pula barang bukti yang dikumpulkan penyidik.

1. Keterangan Saksi

Syarat formal keterangan saksi yang diatur dalam KUHAP ialah, antara lain, dinyatakan di persidangan dan mengucapkan sumpah atau janji sebelum saksi memberikan keterangan. Sedangkan syarat materiil untuk keterangan saksi antara lain: (1) keterangan yang diberikan ialah mengenai peristiwa yang ia dengar, lihat, dan alami sendiri dengan menyebutkan alasan pengetahuannya; (2) bukan pendapat, rekaan, maupun keterangan ahli; (3) ada lebih dari satu orang saksi yang sesuai asas *unus testis*

[14]Tresna, 1977, *Peradilan di Indonesia dari Abad ke Abad,* Pradnya Paramita, Jakarta, hlm. 108.

[15]Josua Sitompul, 2012, *Cyberspace, Cybercrimes, Cyberlaw*: *Tinjauan Aspek Hukum Pidana*, Jakarta; Tatanusa, hlm. 79.

Panji Keadilan Jurnal Ilmiah Nasional Mahasiswa Hukum
P-ISSN: 2599-1892, E-ISSN: 2622-3724
Volume 3, Nomor 1, Januari 2020

nullus testis; (4) bukan keterangan yang dia peroleh dari orang lain *(testimonium de auditu);* dan (5) adanya persesuaian antara keterangan saksi yang satu dengan yang lain dan keterangan saksi yang satu dengan alat bukti yang lain.

Pada kasus *cybercrime*, dikarenakan sifatnya yang virtual, maka pembuktian dengan menggunakan keterangan saksi tidak dapat diperoleh secara langsung. Keterangan saksi hanya dapat berupa hasil pembicaraan atau hanya mendengar orang lain. Kesaksian ini dikenal dengan *testimoniumde auditumatau hearsay evidence*, meskipun kesaksian sejenis ini tidak diperkenakan sebagai alat bukti, akan tetapi dalam praktiknya tetap dapat dipergunakan sebagai bahan pertimbangan bagi hakim untuk memperkuat keyakinannya sebelum menjatuhkan putusan. Kemungkinan yang dapat dijadikan keterangan saksi ialah melalui hasil interaksi dalam dunia *cyber*, seperti *chatting* dan e-mail antara pengguna internet, atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi.[16]

[16]Mansur, Dikdik M. Arief dan Elisatris Gultom, 2005, *Cyber Law - Aspek Hukum Teknologi Informasi*, Bandung; Refika Aditama, hlm. 116

2. Keterangan Ahli

Dalam Pasal 186 KUHAP diatur mengenai syarat formil keterangan ahli bahwa keterangan ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Yang disebut sebagai ahli ialah ahli kedokteran kehakiman dan ahli lainnya. Keterangan ahli menjadi signifikan penggunaannya jika jaksa mengajukan alat bukti elektronik untuk membuktikan kesalahan pelaku *cybercrime*. Peran keterangan ahli disini adalah untuk memberikan suatu penjelasan dalam persidangan bahwa dokumen/data elektronik yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum.

3. Alat Bukti Surat (Pasal 184 Huruf c dan Pasal187 KUHAP)

Jenis surat yang diakui berdasarkan alat bukti ialah surat yang dibuat diatas sumpah jabatan atau dikuatkan dengan sumpah sebagaimana yang tertuang dalam pasal 187 KUHAP. "Surat" dalam kasus *cybercrime* mengalami perubahan dari bentuknya yang tertulis menjadi tidak tertulis dan bersifat *on-line.* Alat bukti dalam komputer yang telah disertifikasi ada dua kategori. Pertama, bila sebuah sistem komputer yang telah disertifikasi oleh badan yang berwenang, maka hasil *print out* komputer dapat dipercaya

keotentikannya. Contohnya *receipt* yang dikeluarkan oleh suatu bank dalam transaksi ATM. Alat bukti ini mempunyai kekuatan pembuktian meskipun dalam persidangan dibutuhkan keterangan lebih lanjut. Kedua, bukti sertifikasi dari badan yang berwenang tersebut dapat dikategorikan sebagai bukti surat, karena dibuat oleh dan atau pejabat yang berwenang. Jenis alat bukti surat lainnya dapat berupa bukti elektronik yang dapat dicetak atau *print out* dan surat yang terpampang dalam layar monitor sebuah jaringan komputer. Selama kedua bukti ini dikeluarkan/dibuat oleh yang berwenang dalam sebuah sistem jaringan komputer dan sebuah sistem jaringan komputer tersebut dapat dipercaya, maka surat tersebut memiliki kekuatan pembuktian yang sama dengan alat bukti surat sebagaimana yang ditentukan dalam KUHAP.

4. Alat Bukti Petunjuk (Pasal 184 (1) huruf d dan Pasal 188 KUHAP)

KUHAP mengatur secara limitatif mengenai sumber petunjuk, yaitu bahwa petunnjuk hanya dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa. Untuk dapat dijadikan sumber petunjuk, ketiga alat bukti tersebut harus sah, dan oleh karena itu, petunjuk yang dihasilkan juga menjadi sah. Dalam *cybercrime,* pengumpulan alat bukti secara fisik akan sulit dipenuhi. Yang paling mudah dalam melakukan pengumpulan bukti-bukti adalah mencari petunjuk-petunjuk yang mengindikasi telah adanya suatu niat jahat berupa akses secara tidak sah. Misalnya dengan melihat dan mendengarkan keterangan saksi di pengadilan, atau surat elektronik atau hasil *print out data*, atau juga dari keterangan terdakwa di pengadilan.

5. Keterangan Terdakwa (Pasal 184 Huruf e dan Pasal 189 KUHAP)

Keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. Agar keterangan terdakwa dapat dinyatakan sah, syarat formil yaitu dinyatakan di sidang dan syarat materiil keterangan tersebut tentang perbuatan yang terdakwa lakukan atau ketahui atau alami sendiri harus dipenuhi. Dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik pasal 5 ayat 1 dan 2 mendeskripsikan bahwa Dokumen Elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. Selain dalam Pasal 44 Undang-undang yang sama mengatakan: "Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang

Panji Keadilan Jurnal Ilmiah Nasional Mahasiswa Hukum
P-ISSN: 2599-1892, E-ISSN: 2622-3724
Volume 3, Nomor 1, Januari 2020

pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut:

a. Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan;
b. Alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Informasi Elektronik dan Dokumen Elektronik dapat dijadikan sebagai alat bukti yang sah menurut undang-undang tentang Teknologi Informasi dan Transaksi Elektronik, walaupun sulit untuk diklasifikasikan termasuk alat bukti yang sah sebagaimana dimaksud Pasal 184 ayat (1) KUHAP. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik 12 sesuai ketentuan yang diatur dalam UU ITE.

PENUTUP

Penal *policy* dalam upaya preventif kejahatan *carding* di Indonesia adalah 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. Upaya preventif agar kartu kredit tidak dibobol. Bagi anda para pengguna kartu kredit, janganlah membuang kertas apapun yang tertera nomor kartu kredit anda dengan sembarang, termasuk struk belanja dan sebagainya. Sebisa mungkin potong-potonglah sekecil mungkin sebelum anda membuangnya. Adapun upaya yang dilakukan agar kejahatan *carding* dalam database tidak meluas sebagai berikut: (a). Usahakanlah untuk membuat file database tidak bisa diakses melalui direktori publik, hindari meletakan file database pada web *root*. (b). Buatlah *permission* untuk mengakses database pada sebuah direktori khusus, hal ini akan mencegah orang lain mendownload file database. (c). Jangan gunakan database default, ubah menjadi nama lain yang anda rasa aman. (d). Hapus atau gantilah nama file yang sedikit riskin, misalnya cmd.exe, cart32.exe, atau lainnya.

Proses hukum pidana dalam menyelesaikan kejahatan *carding* di Indonesia yaitu Pada UU ITE dimuat tentang perbuatan yang dilarang pada Pasal 27 sampai Pasal 36. Pada pasal 42 UU ITE diatur pula mengenai ketentuan penyidikan yang berbunyi: "penyidikan sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan

ketentuan dalam undang-undang ini". Dengan demikian, sistem pembuktian yang dianut adalah sistem/teori pembuktian berdasar undang-undang secara negatif, yaitu sistem yang dianut dalam KUHAP dan berdasar Pasal 183 KUHAP, yang berbunyi sebagai berikut: "hakim tidak boleh menjatuhkan pidana kepada sesorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bajwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya. kasus penyalahgunaan kartu kredit menggunakan internet brerdasarkan urutan alat-alat bukti sebagaimana tercantum dalam pasal 184 KUHAP. Selanjutnya disampaikan pula barang bukti yang dikumpulkan penyidik.

DAFTAR PUSTAKA

Buku

Barda Nawawi, 2006. Tindak Pidana Mayantara: *Perkembangan Cyber Crime di Indonesia*, Jakarta; RajaGrafindo Persada.

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

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

Sjachran Basah, 1987. *Hukum Acara Pengadilan Dalam Lingkungan Peradilan Administrasi*, Rajawali Pers.

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

Tresna, 1977, Peradilan di Indonesia dari Abad ke Abad, Pradnya Paramita, Jakarta,

Vyctoria, 2013. *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*, Andi Yogyakarta

Jurnal

Barda Nawawi Arief, A. 2007. Kebijakan Hukum Pidana Menghadapi Perkembangan Cyber Crime di Bidang Kesusilaan (Cybersex/Cyberporn). *Makalah dalam Seminar Nasional Cybercrime dan Cybersex/Cyberporn Dalam Perspektif Hukum Teknologi dan Hukum Pidana. Kerja sama BPHN Depkumham & S2 Hukum Undip Semarang*.

Lestari, Endah. Tinjauan Yuridis Kartu Kredit Di Indonesia. *Jurnal 2012. Surabaya; Universitas Narotama Surabaya.*

Panji Keadilan Jurnal Ilmiah Nasional Mahasiswa Hukum
P-ISSN: 2599-1892, E-ISSN: 2622-3724
Volume 3, Nomor 1, Januari 2020

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

Sumber Lain

Anton, Cyber Crime dalam situs http://cybercrimercarding.ac.id/2016 archive.html

Ridhokudik. Artikel Tentang CyberLaw dalam http://universitasgajahmada artikel cyber crime.com.