Tinjauan Yuridis terhadap Kekuatan Hukum atas Alat Bukti Kejahatan *Online* (Cybercrime) dalam Kartu Kredit Dihubungkan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Juridical Review of Legal Power on The Evidence of Evidence Online (Cybercrime) in Credit Card Connected with Law Number 11 The Year 2008 Regarding Information and Electronic Transactions

[1]Syarifah Farida Alaydrus, [2]Edi Setiadi, [3]Eka Juarsa
[1,2,3]Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Bandung,
Jl. Tamansari No.1 Bandung 40116
Email: [1]farida.alaydrus@yahoo.com, [2]edi_std@yahoo.com, [3]ekafhunisba@gmail.com

Abstract. In Indonesia, cybercrime is a crime known as a crime that cannot be seen but the consequences can be felt. A number of reports from people who have been harmed by online criminals through electronic media, especially credit cards. Making Police of the Republic of Indonesia is obliged to solve the problems that occur among the community so that cases of online crime through electronic media, especially credit cards can be minimized. The purpose of this study is to know and understand the legal power of cybercrime evidence in credit cards associated with Law Number 11 The year 2008 About Information and Electronic Transactions. As well as handling cases against cybercrime in the perspective of criminal procedure law. In this research, approach method used in this research is a normative juridical approach. Specification Research, this study is analytical descriptive. Data type, that is secondary data. Data collection is done through library research (library research) on secondary data. The data obtained in this study were analyzed using qualitative normative methods. The results of this study, the strength of electronic evidence in the form of Electronic Information and Electronic Documents in the investigation, prosecution and examination of cybercrime in the trial court has a valid evidentiary power as regulated by criminal procedure law, Electronic Information proof and Electronic Document and the print is an expansion of evidence Based on Article 184 of KUHAP. Electronic Information and Electronic Documents shall be declared valid if using Electronic System in accordance with the provisions set forth in Law Number 11 The year 2008 regarding Information and Electronic Transaction. The police of the Republic of Indonesia in the handling of cybercrime especially in the crime of misuse of credit cards is not much different from the handling of conventional crimes, the treatment is done through the stage of investigation, investigation, and examination, as has been set in the provisions of the Criminal Procedure Code and in Law Number 11 Year 2008 regarding Information and Electronic Transactions.

Keywords: Evidence Tools, Online Crime, Credit Card.

Abstrak. Di Indonesia kejahatan online (cybercrime), kejahatan tersebut dikenal sebagai kejahatan yang tidak dapat dilihat namun akibatnya dapat dirasakan. Banyaknya laporan dari masyarakat yang telah dirugikan oleh pelaku kejahatan online melalui media elektronik khususnya kartu kredit. Membuat Kepolisian Republik Indonesia berkewajiban untuk menuntaskan masalah-masalah yang terjadi dikalangan masyarakat sehingga kasus-kasus kejahatan online melalui media elektronik khususnya kartu kredit ini dapat diminimalisir. Tujuan dari penelitian ini adalah untuk mengetahui dan memahami kekuatan hukum atas alat bukti kejahatan online (cybercrime) dalam kartu kredit dihubungkan dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.Serta penanganan perkara terhadap kejahatan online (cybercrime) dalam perspektif hukum acara pidana. Dalam penelitian ini, metode pendekatan yang digunakan dalam penelitian ini adalah pendekatan yuridis normatif. Spesifikasi Penelitian, penelitian ini bersifat deksriptif analitis. Jenis data, yaitu data sekunder. Pengumpulan data dilakukan melalui studi kepustakaan (library research) terhadap data sekunder. Data yang diperoleh dalam penelitian ini dianalisis dengan menggunakan metode normatif kualitatif. Hasil penelitian ini, kekuatan alat bukti elektronik berupa Informasi Elektronik dan Dokumen Elektronik dalam penyidikan, penuntutan dan pemeriksaan kejahatan online (cybercrime) di sidang pengadilan memiliki kekuatan pembuktian yang sah sebagaimana diatur dalam hukum acara pidana, alat bukti Informasi Elektronik dan Dokumen Elektronik serta hasil cetaknya merupakan perluasan alat bukti berdasarkan Pasal 184 KUHAP. Informasi Elektronik dan Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kepolisian

Negara Republik Indonesia dalam penanganan terhadap kejahatan online (cybercrime) khususnya dalam kejahatan penyalahgunaan kartu kredit tidak jauh berbeda dengan penanganan terhadap kejahatan konvensional, peanganan tersebut dilakukan melalui tahap penyidikan, penyelidikan, dan pemeriksaan, sebagaimana yang telah di atur dalam ketentuan dalam Kitab Undang-Undangan Hukum Acara Pidana dan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kata Kunci: Alat Bukti, Kejahatan Online, Kartu Kredit.

A. Pendahuluan

Di Indonesia kejahatan online tersebut termasuk kedalam bentuk *Cybercrime*, kejahatan tersebut dikenal sebagai kejahatan yang tidak dapat dilihat namun akibatnya dapat dirasakan. Banyaknya laporan dari masyarakat yang telah dirugikan oleh pelaku kejahatan online melalui media elektronik khususnya kartu kredit. Membuat Kepolisian Republik Indonesia berkewajiban untuk menuntaskan masalah-masalah yang terjadi dikalangan masyarakat sehingga kasus-kasus kejahatan online melalui media elektronik khususnya kartu kredit ini dapat diminimalisir.

Setelah berlakunya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, ada penambahan mengenai alat bukti yang dapat dijadikan dasar bagi pertimbangan hakim. Menurut ketentuan Pasal 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dikatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah dari jenis-jenis alat bukti yang telah ditentukan dalam Pasal 184 ayat (1) KUHAP.[1]

Dewasa ini, peringkat pembobolan dan peretasan kartu kredit di Indonesia masih berada pada posisi kedua terendah dibandingkan negara lain di wilayah Asia Pasifik. Sedangkan berdasarkan data *Visa*, peringkat pembobolan (*fraud*) Indonesia berada pada posisi ketiga terendah dibandingkan dengan negara lain di Asia Tenggara. Data terakhir Bank Indonesia (BI) sebagai otoritas moneter mencatat, pada bulan Mei 2013 saja, tercatat telah terjadi 1.009 kasus pembobolan (*fraud*) yang dilaporkan dengan nilai kerugian mencapai Rp 2,37 miliar. Kejahatan kartu kredit yang paling banyak terjadi adalah pencurian indentitas dan card not present (CNP). Dengan jumlah kasus pencurian identitas sebanyak 402 kasus dan CNP 458 kasus dengan nilai masing masing Rp 1,14 miliar dan Rp 545 juta yang dialami 18 penerbit. Berangkat dari data tersebut, dengan semakin canggih teknologi semakin terbuka pula peluang melakukan tindak kejahatan tak terkecuali di dunia perbankan.[2]

B. Landasan Teori

Tinjauan Umum *Cybercrime*

Salah satu penyalahgunaan kemajuan teknologi adalah dengan berkembangnya kejahatan siber (*cybercrime*). *Cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh bidang kehidupan modern saat ini.[3] Menurut Anthony Fajri menjelaskan bahwa *cybercrime* adalah suatu kejahatan di mana tindak kejahatan hanya dapat dilakukan dengan

[1] Sutan Remy Syahdeini, *Kejahatan Tindak Pidana Komputer*, Pustaka Utama Grafiti, Jakarta, 2009, Hlm. 263.

[2] Yusuf Asyari, *Curiga saat Bayar Hotel, 18 Pembobol Kartu Kredit Ditangkap*, http://www.jawapos.com/read/2017/02/01/106376/curiga-saat-bayar-hotel-18-pembobol-kartu-kredit-ditangkap, di akses pada tanggal 12 Juni 2017.

[3] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, PT. RajaGrafindo Persada, Jakarta, 2005, hlm. 1.

menggunakan media teknologi *cyber* dan terjadi di dunia *cyber*.[4]

Jenis-jenis kejahatan yang masuk dalam kategori *cybercrime* yaitu sebagai berikut:

1. Cyber-terrorism

National Police Agency of Japan (NPA) mendefinisikan cyber terrorism sebagai electronic attacks through computer networks against critical infrastructures that have potential critical effects on social and economic activities of the nation.

2. Cyber-pornography

Penyebarluasan obscene materials termasuk pornography, indecent exposure, dan child pornography.

3. Cyber-harassment

Pelecehan seksual melalui e-mail, websites, atau chat programs.

4. Cyber-stalking

Crimes of stalking melalui penggunaan komputer dan internet.

5. Hacking

Penggunaan programming abilities dengan maksud yang bertentangan dengan hukum.

6. Carding (credit-card fraud)

Melibatkan berbagai macam aktivitas yang melibatkan kartu kredit. Carding muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

Dari jenis-jenis kejahatan *cybercrime* tersebut, kejahatan *carding* merupakan kejahatan yang dilakukan seorang *carder* atau pelaku untuk melakukan transaksi jual beli dengan menggunakan kartu kredit orang lain. Kejahatan *carding* dapat terjadi pada saat transaksi elektronik yang digunakan melalui media *internet*. Pada saat ini kejahatan *carding* merupakan tindak pidana yang tidak terlihat secara langsung, tapi dampak yang dtimbulkan nya bisa sangat besar. Karena carding merupakan kejahatan *cybercrime* yang berdasarkan aktivitas nya. Artinya *carding* ini merupakan kejahatan dengan menggunakan kartu kredit orang lain sebagai alat Transaksi Elektronik.

Tinjauan Umum Pembuktian

1. Pengertian Pembuktian

Pembuktian merupakan bagian yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian merupakan titik sentral pemeriksaan perkara dalam sidang pengadilan. Pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang untuk membuktikan kesalahan yang didakwakan kepada terdakwa. Pembuktian juga merupakan ketentuan yang mengatur alat-alat bukti yang dibenarkan undang-undang yang boleh dipergunakan hakim membuktikan kesalahan yang didakwakan.

2. Sistem Pembuktian

Hukum acara pidana merupakan suatu upaya dari penegakan hukum pidana. Penegakan hukum adalah mencakup tugas dan wewenang mempertahankan hukum terhadap seseorang atau sekelompok orang yang melanggar hukum atau melakukan perbuatan melawan hukum. Di dalam penegakan hukum pada hakikatnya tidak terlepas dengan bagaimana negara dapat menjamin atau memberikan ketentraman kepada warga masyarakat apabila tersangkut masalah hukum. Penegakan hukum akan terwujud atau tidak terwujud tergantung proses pemeriksaan di dalam persidangan, yaitu melalui

[4] Anthony Fajri, *Cyber Crime*, dalam http://students.ee.itb.ac.id/fajri/publication, diakses pada tanggal 10 Maret 2017.

pembuktian.[5]

Alat Bukti Elektronik

Perkembangan teknologi yang sangat maju menimbulkan kejahatan-kejahatan baru di masyarakat dengan menggunakan teknologi. Setelah berlakunya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik maka terjadi perluasan mengenai pembuktian khususnya mengenai pembuktian elektronik. Pemakaian data elektronik sebagai alat bukti merupakan hal yang baru menyangkut bidang hukum di Indonesia. Dalam Pasal 184 KUHAP tidak diatur mengenai penggunaan alat bukti elektronik. Selama ini alat bukti yang diakui dalam persidangan sesuai dengan ketentuan yang diatur dalam Pasal 184 KUHAP yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan ketrangan terdakwa.

Dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dijelaskan bahwa Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

C. Hasil Penelitian dan Pembahasan

Kekuatan Hukum atas Alat Bukti Kejahatan Online (*Cybercrime*) dalam Kartu Kredit Dihubungkan dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Alat bukti dalam pemeriksaan perkara kejahatan online (*cybercrime*) dalam penyidikan, penuntutan dan pemeriksaan di sidang pengadilan, diatur dalam beberapa pasal, yaitu Pasal 1 ayat (1) menjelaskan bahwa yang disebut Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Sedangkan Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya, sebagaimana yang dijelaskan dalam Pasal 1 ayat (4).

Selanjutnya mengenai keabsahan dari alat bukti elektronik, dijelaskan dalam Pasal 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Dalam Pasal 6 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjelaskan bahwa alat bukti elektronik harus berbentuk tertulis atau asli, dan dianggap sah sepanjang informasi yang tercantum di dalamnya dapat

[5] Hibnu Nugroho, *Merekonstruksi Sistem Penyidikan Dalam Peradilan Pidana (Studi Tentang Kewenangan Penyidik Menuju Pluralisme Sistem Penyidikan di Indonesia)*, Jurnal Hukum Pro Justitia, Vol. 26 No. 1, Januari 2008.

diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Selanjutnya, dalam Pasal 16 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan bahwa suatu bukti elektronik dapat memiliki kekuatan hukum jika informasinya dapat dijamin keutuhannya, dapat dipertanggungajwabkan, dapat diakses, dan dapat ditampilkan sehingga menerangkan suatu keadaan. Orang yang mengajukan suatu bukti elektronik harus dapat menujukkan bahwa informasi yang diimilikinya berasal dari sistem elektronik yang terpercaya.

Dari penjelasan dapat disimpulkan bahwa alat bukti elektronik yang diatur dalam Pasal 5, 6 dan 16 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dapat dikatakan sah dan memiliki kekuatan hukum dalam proses pembuktian di persidangan.

Akan tetapi pada kenyataannya, seringkali alat bukti elektronik ini tidak memiliki nilai kekuatan pembuktian seperti alat bukti konvensional sebagaimana yang diatur dalam KUHAP. Oleh karena itu alat bukti elektronik tersebut tidak dijadikan bahan pertimbangan oleh hakim dalam menjatuhkan putusan, dengan kata lain tidak sah. Hal tersebut dikarenakan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik belum mengatur secara detail dan terperinci mengenai persyaratan formil pengajuan alat bukti elektronik, misalnya alat bukti elektronik berupa surat. Apabila surat elektronik ini kemudian diajukan dimuka persidangan maka yang menjadi persoalan apakah pihak yang mengajukan surat elektronik sebagai alat bukti telah melakukan upaya yang patut untuk memastikan bahwa surat tersebut dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan tersebut, karena surat elektronik bersifat virtual maka rentan untuk diubah, dipalsukan atau bahkan dibuat oleh pihak yang bukan berwenang membuatnya tetapi bersikap seolah-olah sebagai pihak yang sebenarnya. Kemudian persoalan selanjutnya bagaimana apabila ternyata surat elektronik tersebut diperoleh melalui cara-cara yang bertentangan dengan aturan hukum, misalnya melalui pembobolan akun. Apakah dapat dibuktikan bahwa surat tersebut diperoleh dengan cara yang patut dan sesuai dengan hukum (*lawful*). Berdasarkan hal tersebut, maka pemerintah melakukan perubahan terhadap Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Penanganan Perkara terhadap Kejahatan Online (*Cybercrime*) dalam Perspektif Hukum Acara Pidana

Dalam penanganan perkara kejahatan online (*cybercrime*), sesuai dengan tugas dan wewenang kepolisian yang tertera dalam Undang-undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia, Kepolisian Republik Indonesia merupakan lembaga penegak hukum yang memiliki wewenanga dalam melakukan penyidikan perkara kejahatan online (*cybercrime*) dalam hal ini adalah kejahatan penyalahgunaan kartu kredit.

Penyelidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Undang-Undang untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. Dalam memulai penyidikan tindak pidana Polri menggunakan parameter alat bukti yang sah sesuai dengan Pasal 184 KUHAP yang dikaitkan dengan segi tiga pembuktian (*evidence triangle*) untuk memenuhi aspek legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi.

Dalam melaksankan kegiatan penyidikan, terdapat beberapa tahap yang dilakukan oleh kepolisian. Tahap penyelidikan merupakan tahap pertama yang

dilakukan oleh penyidik dalam melakukan penyelidikan tindak pidana serta "tahap tersulit dalam proses penyidikan", hal tersebut dikarenakan dalam tahap ini penyidik harus dapat membuktikan tindak pidana yang terjadi, serta bagaimana dan sebab-sebab tindak pidana tersebut, untuk dapat menentukan bentuk laporan polisi yang akan dibuat.

Dalam penyelidikan kasus-kasus *cybercrime* seperti penyalahgunaan kartu kredit (*carding*), metode yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkotika terutama dalam *undercover* (penyamaran) dan *control delivery* (kebebasan terkontrol). Petugas setelah menerima informasi atau laporan, yang dirugikan melakukan koordinasi dengan pihak yang mengirimkan untuk melakukan pengiriman barang. Permasalahan yang ada dalam kasus seperti ini adalah laporan yang masuk terjadi setelah pembayaran barang ternyata ditolak oleh bank dan barang sudah diterima oleh pelaku, di samping adanya kerjasama antara *carder* dengan karyawan *shipping* sehingga apabila polisi melakukan koordinasi informasi tersebut akan bocor dan pelaku tidak dapat ditangkap sebab identitas yang biasanya dicantumkan adalah palsu.

Tahap kedua kepolisian melakukan penindakan, polisi dalam mekakukan penangkapan terhadap tersangka sering kali polisi tidak dapat menentukan secara pasti siapa pelakunya, karena mereka melakukannya cukup melalui komputer yang dapat dilakukan di mana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan IP *Address* dari pelaku dan komputer yang digunakan. Penyitaan barang bukti banyak menemui permasalahan karena biasanya pelapor sangat lambat dalam melakukan pelaporan, hal tersebut membuat data serangan di *log server* sudah dihapus biasanya terjadi pada kasus deface, sehingga penyidik menemui kesulitan dalam mencari *log statistic* yang terdapat di dalam *server* sebab biasanya secara otomatis *server* menghapus *log* yang ada untuk mengurangi beban *server*. Hal ini membuat penyidik tidak menemukan data yang dibutuhkan untuk dijadikan barang bukti sedangkan data *log statistic* merupakan salah satu bukti vital dalam kasus *hacking* untuk menentukan arah datangnya serangan.

Selanjutnya, pada tahap pemeriksaan terhadap saksi dan korban banyak mengalami hambatan, hal ini disebabkan karena pada saat kejahatan berlangsung atau dilakukan tidak ada satupun saksi yang melihat (*testimonium de auditu*). Mereka hanya mengetahui setelah kejadian berlangsung karena menerima dampak dari serangan yang dilancarkan tersebut seperti tampilan yang berubah maupun tidak berfungsinya program yang ada, hal ini terjadi untuk kasus-kasus *hacking*. Untuk kasus kejahatan penyalahgunaan kartu kredit, permasalahan yang ada adalah saksi korban kebanyakan berada di luar negeri sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban. Berdasarkan penjelasan diatas sesuai sebagai mana yang diatur dalam Pasal 42, 43, dan 44 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

D. Kesimpulan

1. Kekuatan alat bukti elektronik berupa Informasi Elektronik dan Dokumen Elektronik dalam penyidikan, penuntutan dan pemeriksaan kejahatan online (*cybercrime*) di sidang pengadilan memiliki kekuatan pembuktian yang sah sebagaimana diatur dalam hukum acara pidana, alat bukti Informasi Elektronik dan Dokumen Elektronik serta hasil cetaknya merupakan perluasan alat bukti berdasarkan Pasal 184 KUHAP. Informasi Elektronik dan Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan

yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Kepolisian Negara Republik Indonesia dalam penanganan terhadap kejahatan online (*cybercrime*) khususnya dalam kejahatan penyalahgunaan kartu kredit tidak jauh berbeda dengan penanganan terhadap kejahatan konvensional, peanganan tersebut dilakukan melalui tahap penyidikan, penyelidikan, dan pemeriksaan, sebagaimana yang telah di atur dalam ketentuan dalam Kitab Undang-Undangan Hukum Acara Pidana dan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

E. Saran

1. Dalam proses pengumpulan alat bukti yang sah untuk kepentingan pemeriksaan kejahatan online (*cybercrime*) di pengadilan, Penyidik Pejabat Kepolisian Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik perlu memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data. Penggeledahan dan penyitaan terhadap sistem elektronik yang terkait dengan dugaan kejahatan online (*cybercrime*) dilakukan atas persetujuan orang yang bersangkutan serta izin ketua pengadilan negeri setempat, sebagaimana yang diatur dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
2. Dalam penanganan terhadap kejahatan online (*cybercrime*) Kepolisian Republik Indonesia harus lebih konsisten dalam menerapkan ketentuan peraturan perundang-undangan yang berlaku, dan menerapkan upaya-upaya prefentif dalam mencegah terjadinya kejahatan online (*cybercrime*) khususnya kejahatan penyalahgunaan kartu kredit yang terjadi di Indonesia, demi terwujudnya keamanan dan keadilan di dalam kehidupan Masyarakat.

Daftar Pustaka

Barda Nawawi Arief, Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, PT. RajaGrafindo Persada, Jakarta, 2005.

Sutan Remy Syahdeini, Kejahatan Tindak Pidana Komputer, Pustaka Utama Grafiti, Jakarta, 2009.

Hibnu Nugroho, Merekonstruksi Sistem Penyidikan Dalam Peradilan Pidana (Studi Tentang Kewenangan Penyidik Menuju Pluralisme Sistem Penyidikan di Indonesia), Jurnal Hukum Pro Justitia, Vol. 26 No. 1, Januari 2008.

Anthony Fajri, Cyber Crime, dalam http://students.ee.itb.ac.id/fajri/publication

Yusuf Asyari, Curiga saat Bayar Hotel, 18 Pembobol Kartu Kredit Ditangkap, http://www.jawapos.com/read/2017/02/01/106376/curiga-saat-bayar-hotel-18-pembobol-kartu-kredit-ditangkap