Journal of Islamic Business Law
Volume 4 Issue 3 2020
ISSN (Online): 258-2658
Available online at: http://urj.uin-malang.ac.id/index.php/jibl

Urgensi Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik dalam Penanganan atas Kejahatan *Carding* di Bank X

Khoirotun Nisa
Dwi Hidayatul
Firdaus
Universitas Islam Negeri Maulana Malik Ibrahim Malang
rnisa0599@gmail.com

Abstrak:

Carding merupakan tindak pidana pencurian dengan wajah baru yang muncul seiring pesatnya laju perkembangan zaman disertai kemajuan teknologi internet yang membawa banyak dampak negatif. beberapa kasus carding yang terjadi di indonesia menimbulkan kerugian besar bagi sektor perbankan, dan hal ini melatarbelakangi pemerintah menyusun undang-undang guna mengatasi masalah carding. Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik seolah menjadi tameng bagi perbankan agar dapat terhindar dari resiko kerugian akibat carding yang suatu saat dapat terjadi, namun pada kenyataannya Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik ini belum sepenuhnya mengcover masalah carding yang masih sering terjadi, sehingga masih membutuhkan undang-undang lain dalam penegakannya. Tujuan dilakukannya penelitian ini adalah untuk mengetahui upaya yang dilakukan oleh Bank X terkait kejahatan carding yang kian hari kian meningkat, dan pasti dengan membawa banyak dampak negatif. penelitian ini memberikan gambaran bahwa Undang-Undang ITE masih cukup global dan kurang mengcover atas permasalahan-permasalahan yang terjadi, sehingga Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini masih belum cukup mampu untuk menjadi hukum tunggal dalam menyelesaikan kejahatan carding di Indonesia.

Kata Kunci : Carding; perlindungan hukum; transaksi elektronik.

Pendahuluan

Peretasan kartu kredit (*Carding*) merupakan suatu bentuk kejahatan berbasis teknologi informasi (*Cyber Crime*) berupa pembobolan kartu kredit orang lain yang digunakan untuk pembayaran atas transaksi jual beli tanpa izin dan juga tanpa sepengetahuan pemegang *credit card* yang sah.[1] Tej Paul Bhatla mendefinisikan Credit card fraud ketika seseorang menggunakan kartu kredit orang lain untuk alasan (kepentingan) pribadi sedangkan pemilik kartu dan penerbit kartu tidak menyadari fakta bahwa kartu miliknya sedang digunakan. Selanjutnya, seseorang tersebut menggunakan kartu tanpa ada hubungannya dengan pemegang kartu atau penerbit, dan tidak memiliki

[1] Suratman, *Cyber Crime (modus operandi dan penanggulangannya)* (Yogyakarta: Laksbang Presindo,

2007), 64.

niat baik untuk menghubungi pemilik kartu atau membuat pembayaran atas pembelian yang dilakukannya.[2]

Sesuai dengan *update* data hingga bulan Mei 2013, telah tercatat terjadi sekitar 1009 kasus pembobolan atau *fraud* yang dilaporkan, sedangkan untuk kalkulasi kerugian diperkirakan mencapai Rp 2,37 Milyar. Hal ini membuat peringkat pembobolan kartu kredit di Indonesia menjadi berada pada posisi kedua terendah dibandingkan negara lain di wilayah Asia pasifik.[3] Dimana pada tahun 2008 sesuai dengan data Indonesia tercatat mempunyai jumlah *carder* (pelaku *carding*) terbanyak nomor 2 di dunia setelah Ukraina, sehingga hal tersebut menjadikan Indonesia memiliki reputasi buruk yang menyebabkan *e-commerce* internasional banyak melakukan penolakan jika *IP Adress* asal Indonesia berbelanja secara legal di situs belanja internasional.[4]

Hal buruk semacam ini terjadi karena perkembangan kejahatan yang berbasis teknologi ini membawa persoalan baru di bidang hukum, dimana ketika hukum semakin jauh ketinggalan dengan pesatnya teknologi, maka ujung-ujungnya adalah ketidakmampuan hukum dalam menjangkau perkembangan kejahatan yang semakin luas dan berkembang.[5] Perkembangan teknologi memaksa pemerintah bertindak cepat dan tanggap terhadap perubahan-perbahan yang terjadi dalam masyarakat, termasuk penyimpangan-penyipangan yang terjadi, sehingga pemerintah tetap dapat mengontrol masyarakat melalui regulasi-regulasi yang diatur sedemikian rupa. Saat ini, pemerintah Indonesia telah memiliki regulasi berupa Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik, dimana undang-undang ini lahir atas dasar tuntutan keadaan yang memaksa pemerintah membentuk regulasi atas kejahatan-kejahatan menggunakan teknologi internet yang notabene merupakan hal baru dan berbeda konsep dengan kejahatan pada umumnya. Carding sendiri merupakan bagian dari kejahatan menggunakan teknologi internet dalam bidang perbankan khusunya credit card.

Berdasarkan kalkulasi kasus carding yang kian hari kian meningkat, namun tak menyurutkan keinginan nasabah untuk menggunakan kartu kredit, melainkan jumlah pengguna kartu kredit semakin meningkat meskipun banyak resiko yang sewaktu-waktu bisa terjadi, berdasarkan data, kalkulasi pengguna kartu kredit sampai awal 2013 Bank Indonesia (BI) mencatat jumlah pemegang kartu kredit telah mencapai 14.591.371 dan Rata-rata setiap orang memegang 3 kartu kredit. Adapun nilai transaksinya mencapai Rp 17,96 triliun di awal tahun 2013 lalu.[6] Hal ini terjadi mungkin saja didasari karena memang kartu kredit merupakan kebutuhan dari kelompok masyarakat tertentu, dimana kartu kredit sendiri juga menawarkan banyak kemudahan bagi penggunanya.

Kejahatan *carding* dapat terjadi dimana saja dan menimpa siapa saja. Sesuai dengan adanya kasus *carding* yang akhir-akhir ini ramai dibicarakan publik, yakni kasus carding yang dilakukan *carder* dengan cara membeli data kartu kredit melalui facebook ataupun *darkweb*, dimana data yang dimaksud disini, bisa berasal dari kebocoran data

---

[2] Said Noor Prasetyo, Rumusan Pengaturan Credit Card Fraud dalam Hukum Pidana Indonesia ditinjau dari Asas Legalitas, Legality, Vol. 24, No.1, Maret 2016-Agustus 2016, hlm. 101-119. 105.

[3] Nunuk Sulisrudatin, "Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit," *Jurnal Hukum Dirgantara,* Volume 9 no. 1(September 2018): 28.

[4] Comex Crisna Wijaya, Kejahatan Carding dalam Perspektif Undang-Undang ITE dan Hukum Islam, (Skripsi Universitas Islam Negeri Sunan Kalijaga Yogyakarta", 14.

[5] Barda Nawawi Arief, *Strategi Penanggulangan Kejahatan Telematika* (Yogyakarta: PT. Atmajaya Yogyakarta, 2010), 66.

[6] Said Noor Prasetyo, Rumusan Pengaturan Credit Card Fraud dalam Hukum Pidana Indonesia ditinjau dari Asas Legalitas, Legality, Vol. 24, No.1, Maret 2016-Agustus 2016, hlm. 101-119. 103.

perbankan, marketplace dan yang paling sering adalah saat transaksi di kasir. Melalui data yang diperoleh tersebut, nantinya pelaku dapat melakukan transaksi diberbagai *marketplace*.[7] Terkait hubungan perikatan antara bank dan nasabah, pada dasarnya bank sebagai pihak penyelenggara harus menanggung segala konsekuensi, termasuk dalam hal kerugian, sehingga bank harus berhati-hati, cermat serta bijaksana guna meminimalisir resiko-resiko yang mungkin saja terjadi, sehingga bank harus memperhatikan asas-asas perkreditan yang sehat.[8]

Berdasarkan uraian persoalan ini, maka penulis dirasa perlu melakukan penelitian terkait pemberlakuan Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik yang notabene sebagai Undang-Undang yang seharusnya memiliki peran besar dalam menindak pelaku kejahatan elektronik khususnya dalam kejahatan carding tidak berhenti sampai disitu saja, penelitian ini juga dilakukan dengan tujuan melihat bagimana implementasi Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik untuk menilai keefektivannya meskipun dalam kenyataannya terdapat banyak hambatan yang ditemukan oleh perbankan dalam proses pencegahannya.

Metode Penelitian

Penelitian ini tergolong dalam penelitian hukum empiris atau bisa disebut dengan yuridis empiris, dimana data didapatkan secara langsung daripada kondisi nyata di lapangan atau *field research* yang kemudian di komparasikan dengan hukum yang menaungi. Penelitian ini melibatkan informan yang berprofesi sebagai pegawai di unit fraud and authorization LNC yang secara khusus menangani kartu kredit di bank X. Dimana wawancara dilakukan menggunakan metode wawancara bebas terpimpin yang dalam mekanismenya peneliti menyajikan pertanyaan untuk ditanyakan kepada informan secara langsung, namun tidak menutup kemungkinan dalam proses wawancara, terdapat pertanyaan lain yang perlu ditanyakan mengenai masalah yang dikaji, hal ini dimaksudkan agar peneliti mendapatkan informasi yang valid dan luas. Penelitian ini menggunakan pendekatan deskriptif kualitatif, maksudnya data yang diperoleh baik secara lisan maupun tulisan disusun menggunakan uraian kalimat yang jelas kemudian dianalisis menggunakan regulasi perundang-undangan, sehingga terlihat adanya kesesuaian atau ketidaksesuaian antara upaya bank dengan sistem perundang-undangan. Lokasi yang dipilih dalam penelitian ini yakni di salah satu Bank di Kota Malang. Adapun data-data yang diperoleh dengan cara wawancara ini dilakukan guna memenuhi data primer, sementara untuk data skunder, didapatkan melalui regulasi-regulasi seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan lain-lain, data skunder juga didapatkan dari bahan bacaan mengenai masalah yang dikaji.

Hasil dan Pembahasan

Konsep Dasar Darding Dalam Dunia Perbankan

Carding merupakan pencurian dalam dunia perbankan akibat bocornya informasi mengenai data pribadi nasabah baik karena kelalaian atau murni kejahatan yang

[7]Boy, "Kasus Pembobolan Kartu Kredit Tiket Kekiian Bukti Praktik Carding Masih Marak," JPPN, 07 Maret 2020, diakses pada tanggal 29 April 2020, 14.57 WIB, https://m.jpnn.com/new/kasus-pembobolan-kartu-kredit-tiket-kekinian-bukti-praktik-carding-masih-marak.

[8] Etty Mulyati,*Kredit Perbankan: Aspek Hukum dan Pengembangan Usaha Mikro Kecil dalam Pembangunan Perekonomian Indonesia* (Bandung: Refika Aditama, 2016), 77.

dilakukan oleh carder dengan menggunakan teknologi internet. *carding* atau peretasan kartu kredit sebenarnya bukan pertama kali terjadi di perbankan, melainkan sudah beberapa kali terjadi dan pasti dengan memimbulkan berbagai resiko. Dalam kegiatan perbankan, resiko merupakan suatu hal yang tidak diharapkan dan tidak terbantahkan keberadaannya, dimana hal tersebut merupakan suatu keadaan yang notabene mengakibatkan adanya kerugian yang diderita korban baik kerugian finansial dengan nominal kecil maupun besar.

Adanya jenis kejahatan baru memaksa pemerintah membentuk regulasi baru guna menangani kejahatan yang terjadi. Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik merupakan undang-undang pertama yang dirumuskan oleh pemerintah Indonesia dalam menghadapi kejahatan-kejahatan yang dilakukan dengan menggunakan teknologi, dalam artian Undang-Undang tersebut merupakan tumpuhan utama dalam menegakkan hukum atas hal-hal yang berkaitan dengan cybercrime. Namun dengan adanya Undang-Undang ini tidak sepenuhnya menghentikan kejahatan carding, sebab terlalu banyak celah yang dimanfaatkan carder untuk melakukan aksinya.

Terkait pola dari kejahatan carding, pada dasarnya penulis perlu melihat dari sisi hukum, disini penulis mendasarkan pada Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik pasal 32 ayat 1 yang berbunyi:[9]

> "setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambahi, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik."

Dari pasal tersebut dapat diartikan bahwa setiap kegiatan yang dilakukan pihak ketiga dalam hal ini merujuk pada posisi *fraudster* ataupun *carder* yang berhubungan dengan otak-atik terhadap informasi atau dokumen elektronik milik orang lain tanpa disertai adanya izin, dimana hal bersebut membawa dampak pada adanya pengurangan data, penambahan data, perubahan data ataupun yang lainnya yang dilakukan dengan adanya unsur kesengajaan, sehingga pada akhirnya menimbulkan kerugian bagi perbankan maupun nasabah. Adapun modus yang banyak digunakan saat ini oleh *fraudster* ada 3. Pertama, kejahatan melalui *call fake number* yang digunakan oleh pelaku kejahatan sama dengan *number call center* bank X, dimana pelaku kejahatan mengatasnamakan oknum pegawai Bank X serta meminta OTP kepada pemegang kartu kredit. Kedua, pelaku kejahatan menggunakan nomor lama pemegang kartu yang sudah tidak aktif untuk dihidupkan (modus *recycle*) kembali dengan ke *provider*, dalam hal ini terdapat kelalaian pemegang kartu kredit untuk tidak melakukan pengkinian data ke call center Bank X. Ketiga, kasus yang paling baru terjadi adalah pelaku kejahatan memanfaatkan posisi HP pemegang kartu yang OFF untuk kemudian mendatangi *provider* untuk melakukan penggantian *sim card* dengan nomor HP milik pemegang kartu kredit akan dikuasai oleh pelau kejahatan, sedangkan nomor kartu di HP pemegang kartu kredit tidak dapat digunakan lagi.[10]

Berkembangnya teknologi berpengaruh terhadap pola pikir masyarakat, baik pola pikir positif maupun negatif. Pola pikir negatif dapat dilihat dari keadaan masa sekarang yang mana kejahatan semakin beragam dan semakin canggih. Terdapat beberapa teori

[9] Pasal 32 ayat 1Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[10] *Data wawancara* dengan penyelia manajemen resiko *unit fraud control and authorization LNC Bank X, 14 April 2020.*

untuk menggambarkan hubungan antara teknologi dan hukum, yakni teori substantif dan teori instrumental. Pertama, Teori instrumental. Teori instrumental mengartikan teknologi sebagai alat yang dikembangkan secara rasional untuk memenuhi kebutuhan tertentu, karena dikembangkan dengan prinsip rasionalitas dan efisiensi, teknologi memberikan pilihan-pilihan dan kebutuhan-kebutuhan yang rasional pula bagi masyarakat. Oleh karena itu, teknologi bersifat netral (tidak bersifat baik atupun buruk) dan terpisah dari proses ekonomi politik, sosial dan budaya. Produktivitasnya dapat diukur secara objektif, terlepas dari budaya, sehingga teknologi dapat dialihkan dari satu masyarakat ke masyarakat lain satu dengan kata lain teknologi dapat diterapkan secara universal.

Kedua, Teori substantif. Teori substantif mengartikan teknologi tidak netral karena teknologi berkaitan erat dengan kepentingan dari sebjek yang membuat teknologi tersebut. Kedua teori diatas menjunjukkan cara pandang yang berlawanan dalam mengartikan teknologi. Dimana Teori instrumental secara tidak langsung mengartikan bahwa jika terjadi penyalahgunaan teknologi, maka hal itu menjadi urusan pribadi dari pihak yang menyalahgunakan, bukan teknologinya sendiri, sedangkan untuk teori substantif dapat diartikan sekelompok kepentingan atas adanya regulasi yang dibuat oleh pihak-pihak yang tentunya berkepentingan. berdasarkan teori ini, dapat dianalogikan bahwa kemajuan teknologi memiliki pengaruh dalam kegiatan perbankan, salah satunya adalah dengan proses pembayaran dengan menggunakan kartu kredit yang lama-kelamaan menjadi suatu kebutuhan manusia, hal ini wajar terjadi, mengingat kemajuan teknologi sapat membawa manusia menuju makhluk yang semakin berkembang dalam pemikiran termasuk kebutuhan. Dengan kemajuan tersebut, saat ini banyak dimanfaatkan oleh oknum-oknum tertentu untuk melakukan penyimpangan, penyimpangan disini merujuk pada adanya kejahatan carding yang setiap tahun mengalami peningkatan jumlah, dimana kejahatan carding tersebut menjadikan kepentingan orang lain menjadi terganggu atas kepentingan oknum tersebut.

Manajemen penanganan atas kejahatan carding di bank X

Dalam upaya penanganan, Bank X yang menjadi tempat penelitian telah membentuk unit yang disebut dengan *Unit Fraud And Authorization LNC*, yang secara khusus bertugas untuk menangani apabila terjadi kejahatan carding atas nasabah di bank X, termasuk hal pemantauan dan juga mengelola resiko kerugian. Adapun prosedur dari penanganan daripada *Unit Fraud And Authorization LNC* ini adalah sebagai berikut :[11] Pengaduan. Pengaduan merupakan tindakan pertama yang harus oleh dilakukan oleh nasabah, ketika menemukan kejanggalan atas tagihan yang diterima. Pengaduan dapat dilakukan baik melalui bantuan bank BNI terdekat atau mengirim aduan via email ke *unit fraud control and authorization LNC* ataupun langsung disampaikan nasabah melalui call center BNI, untuk kemudian diinvestigasi lebih lanjut.

Unit fraud control and authorization LNC menerima berkas lengkap pengajuan sanggahan dari pemegang kartu kredit dari kantor pusat, atau mengirim surat sanggahan yang berisi kronologis peristiwa, KTP pemegang kartu serta nomor kredit miliknya, selanjutnya mengirimkan kelengkapan data tersebut melalui *email* ke Bank X. *unit fraud control and authorization LNC* menindak lanjuti laporan nasabah dengan cara melakukan investigasi mendalam. Hasil investigasi FCA Surabaya memberikan hasil laporan ke kantor pusat terkait dengan kasus tersebut dengan hasil kesimpulan bahwa

11 *Data wawancara* dengan penyelia manajemen resiko *unit fraud control and authorization LNC Bank X, 14 April 2020.*

kasus tersebut merupakan murni kejahatan carding tanpa disertai kelalaian dari pemegang kartu kredit ataukah kejahatan carding yang disertai kelalaian dari pemegang kartu kredit atau kasus tersebut bukan merupakan *carding.*

Terkait upaya penanganan lazim membahas mengenai hambatan yang ditemui oleh perbankan dalam mewujudkan kamanan dan kenyamanan bersama dalam perikatannya dengan nasabah dalam hal penggunaan kartu kredit. Sesuai dengan hasil wawancara dengan Unit FCA LNC, hambatan sampai saat ini sering ditemui tersebut diantaranya adalah *pertama,* Internal nasabah. Data internal merupakan data penting yang seharusnya hanya pihak nasabah yang mengetahui, namun berkaitan dengan pentingnya mengamankan data pribadi nasabah seperti Nomor PIN, kode OTP dan lain-lain, nasabah terkadang cenderung tanpa menyadari, mereka telah menyebarluaskan data pribadi mereka, dimana hal tersebut seakan membuka kesempatan para *carder* untuk melakukan kejahatan terkait. Hal ini sesuai dengan penuturan informan bahwa hambatan terbesar yang hingga kini belum dapat berselesaikan hingga saat ini ialah rendahnya kesadaran atas diri nasabah.

Kedua, Pengungkapan pelaku *carding.* Berkaitan dengan hambatan terkait penanganan kasus, maka sesuai dengan penuturan informan, bahwa dalam pengungkapan pelaku kejahatan terbilang tidak mudah. Menurut analisisa peneliti, hal ini disebabkan karena ranah operasi pelaku, bukan hanya melibatkan daerah-daerah dalam negeri, melainkan melewati batas-batas negara, begitu pula dalam melakukan transaksi, biasanya para *carder* membelanjakan kartu kredit palsunya ke *e-commerce* luar negeri. Selanjutnya adalah keamanan sistem, Berdasarkan banyaknya kasus yang terjadi dengan berbagai modus yang dilakukan para *carder*, dimana hampir semua kejahatan yang terjadi bersumber pada pemalsuan, maka hal ini dapat dikategorikan dalam satu bentuk kelemahan yang tidak dapat dihindarkan, meskipun sebab terbobolnya keamanan kartu kredit tidak berasal dari satu arah saja, melainkan juga dapat diakibatkan karena kelalaian dari pihak nasabah sendiri.

Upaya Pencegahan terjadinya carding di bank X

Pencegahan atas kejahatan carding, dilakukan oleh pihak perbankan sebagai upaya agar terhindar dari segala kerugian, adapun pencegahan disini merujuk pencegahan dalam bentuk preventif dan represif, sebagai berikut:[12]

1. cara represif berupa membentuk *Unit Fraud And Authorization LNC* untuk melakukan investigasi, dalam artian disini *Unit Fraud And Authorization LNC* yang berupaya menyelesaiakn masalah dalam ranah internal perbankan.
2. kerjasama dengan aparat kepolisian untuk menangani case-case yang terjadi dan tentu terkait dengan upaya penangkapan pelaku yang notabene ranah eksternal dari perbankan.
3. cara preventif berupa, pemberian edukasi kepada nasabah mengenai pentingnya pengamanan diri terkait data personal nasabah, dan juga edukasi kepada merchat agar berhati-hati dan bijak dalam bertransaksi menggunakan kartu kredit, mengingat terdapat banyak sekali modus yang digunakan oleh para carder, sesuai dengan data wawancara yang sebelumnya telah dilakukan dengan informan yang ahli dibidang penanganan kartu kredit. menurut data, modus yang

12 *Data wawancara* dengan penyelia manajemen resiko *unit fraud control and authorization LNC Bank X, 14 April 2020.*

banyak digunakan saat ini oleh *fraudster* ada 3. Pertama, kejahatan melalui *call fake number* yang digunakan oleh pelaku kejahatan sama dengan *number call center* bank X, dimana pelaku kejahatan mengatasnamakan oknum pegawai Bank X serta meminta OTP kepada pemegang kartu kredit. Kedua, pelaku kejahatan menggunakan nomor lama pemegang kartu yang sudah tidak aktif untuk dihidupkan (modus *recycle*) kembali dengan ke *provider*, dalam hal ini terdapat kelalaian pemegang kartu kredit untuk tidak melakukan pengkinian data ke call center Bank X. Ketiga, kasus yang paling baru terjadi adalah pelaku kejahatan memanfaatkan posisi HP pemegang kartu yang OFF untuk kemudian mendatangi *provider* untuk melakukan penggantian *sim card* dengan nomor HP milik pemegang kartu kredit akan dikuasai oleh pelau kejahatan, sedangkan nomor kartu di HP pemegang kartu kredit tidak dapat digunakan lagi.[13]

4. Memberikan informasi yang cukup terhadap nasabah, baik dari sisi manfaat, resiko, upaya penyelesaia jika terjadi problem, dan lain-lain.
5. Keamanan sistem, keamanan sistem dalam hal ini diwujudkan dalam bentu pembentukan devisi IT untuk mengontrol, meskipun hanya mencakup ranah internal.

Perlindungan Nasabah di Bank X

Bank sebagai badan yang menyelenggarakan produk pembayaran menggunakan kartu kredit, pasti bank mutlak siap dalam memberikan perlindungan terhadap masalah ataupun resiko apa saja yang mungkin saja terjadi, dalam pembahasan terkait bahaya carding, bank memberikan perlindungan terhadap nasabah. Perlindungan atas kerugian nasabah, di wujudkan dengan adanya jaminan penggantian kerugian atas dana yang hilang kepada nasabah yang menjadi korban kejahatan *carding*, namun hal ini tidak bersifat mutlak, melainkan dengan syarat, jika memang kejahatan tersebut murni *carding* tanpa adanya unsur kelalaian oleh nasabah, dimana ada atau tidaknya unsur kelalaian ini didasarkan pada hasil investigasi yang dilakukan oleh *Unit Fraud and Authorization LNC*, yang sebelumnya telah melalui proses pengaduan melalui *call center* dan penanganan oleh *Unit Fraud and Authorization LNC.* Dimana apabila dari hasil investigasi terbukti secara valid, transaksi murni dibobol dan nasabah tidak terbukti melakukan kelalaian menyerahkan data pribadi kepada *fraudster*, maka nasabah akan dibebaskan dari seluruh kerugian.

Berkaitan dengan pemberian ganti rugi oleh perbankan, sesuai hasil wawancara, maka terdapat 2 tolok ukur. Pertama, menggunakan analisa terkait dengan kronologis yang disampaikan oleh pemegang kartu kredit. Dari kronlogis akan diketahui apakah pemegang kartu kredit pernah memberikan OTP kepada pihak ketiga. Yang kedua, memeriksa log aktivitas traansaksi kartu kredit yang bersangkutan, kemudian akan dketahui apakah yang bersangkutan pernah menerima kode OTP melalui nomor HP pemegang kartu yang masih aktif. Disini dapat mengetahui pula apakah kode OTP dikirimkan ke nomor lama pemegang yang sudah diaktifkan kembali oleh pelaku kejahatan.

Urgensi UU ITE terhadap kejahtan Carding

[13] *Data wawancara* dengan penyelia manajemen resiko *unit fraud control and authorization LNC Bank X, 14 April 2020.*

Peran Undang-Undang ITE dalam penanganan atas praktik carding hal ini hanya berlaku sebagai pengkategorian suatu perbuatan menyimpang atau melawan hukum yang dilakukan oleh pihak ketiga. Realita yang ditemukan dalam lapangan, untuk tindakan lanjut dalam bentuk pencegahan perbankan perlu membentuk aturan tersendiri yang bisa saja bersifat internal, hal ini dilakukan sebab UU ITE tidak sepenuhnya mengcover semua hal yang seharusnya dibahas secara khusus. Salah satunya, UU ITE tidak menjelaskan proses penyidikan terhadap kejahatan yang berbasis teknologi internet yang mana proses ini disamakan dengan penyidikan dalam kejahatan atau pencurian biasa yang notabene berbeda secara karakteristik.

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya cybercrime, beberapa penyebab diantaranya adalah keterbatasan Sumber Daya Manusia yang dimiliki penegak hukum, yakni sangat langka yang intens terhadap kejahatan komputer, kejahatan yang menggunakan sarana komputer, kejahatan dunia maya. Sebab kejahatan ini memerlukan ketrampilan khusus bagi aparatur penegak hukum. Sehingga dalam hal penyelidikan dan penyidikan selalu mengalami jalan buntu atau tidak tuntas. Metode penyidikannya juga bersifat khusus, tidak semua penyidik dapat melakukannya. Harus ada anggota kepolisian yang bertugas di bidang internet atau biasa disebut polisi cyber atau cyber police.

Untuk membuktikan jejak-jejak para hacker, cracker dan phreacker dalam melakukan aksinya terutama yang berhubungan dengan program-program dan datadata komputer, sarana Polri belum memadai karena belum ada komputer forensik.Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa soft copy (image, program, dsb).Dalam hal ini Polri masih belum mempunyai fasilitas forensic computing yang memadai. Fasilitas forensic computing yang akandidirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu evidence collection, forensic analysis, expert witness.[14]

Ditinjau dari urgensi adanya perlindungan yang diberikan oleh bank kepada korban, berdasarkan pelanggaran yang dilakukan carder atas pasal 32 ayat 1 di atas maka untuk selanjutnya berlaku Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur hal tersebut dengan jelas, dimana aturan tersebut terdapat dalam Pasal 30 ayat 3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi:[15]

> "setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengaman (*cracking, hacking, ilegal acces*). Ancaman pidana pasal 46 ayat 3 setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat 3 dipidana dengan pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah)."

Pada dasarnya kejahatan *carding* dapat dikenakan sanksi yang terdapat dalam pasal ini, dimana isi pasal ini sesuai dengan realita dari mekanisme terjadinya kejahatan

[14] Nuria Siswi Enggarani, Penanggulangan Kejahatan Internet di Indonesia, Jurnal Ilmu Hukum,Vol. 15, No 2, September 2012 : 149-168. 164.
[15] Pasal 30 ayat 3Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

carding, dimana kejahatan *carding* bermula dengan adanya penjebolan suatu sistem atau dengan penerobosan maupun pencurian data secara ilegal, dengan adanya pasal tersebut, maka dimaksudkan agar mempersempit ruang gerak *carder* dalam melakukan kejahatan.

Dari semua pemaparan diatas, dapat diketahui bahwa, dalam upaya penegakan hukum atas kejahatan carding, UU ITE tidak dapat berdiri sendiri, melainkan perlu untuk didampingi oleh UU lain yang searah dengan masalah yang terjadi. Dalam proses penyelesaian masalah kejahatan kartu kredit, pihak perbankan perlu regulasi lain seperti Surat Edaran BI Nomor 16/16/DKSP tahun 2014 Tentang Tata Cara Pelaksanaan Perlindungan Konsumen Jasa Sistem Pembayaran, Peraturan BI No.16/PBI/2014 Tentang Perlindungan Konsumen Jasa Sistem Pembayaran, dan lain-lain. Hal ini terjadi karena kebijakan regulasi mengenai kejahatan kartu kredit (carding) belum sepenuhnya mengatur secara jelas mengenai kejahatan carding ini, terbukti dalam isi dari pasal-pasalnya yang tidak mengatur mengenai tindak lanjut dalam upaya pembuktian ataupun hal lain mengenai upaya penanganan oleh aparat, sehingga dalam menjerat pelaku pun, dalam prosesnya masih menggunakan Undang-Undang lain. Meskipun disatu sisi, UU ITE akan menjadi dasar hukum atas kejahatan-kejahatan elektronik yang terjadi, termasuk carding.

Undang-undang memiliki pengaruh yang kompleks dalam memberantas praktik *carding*, namun pada kenyataannya hukum belum sepenuhnya mengcover penyimpangan-penyimpangan yang terjadi, dimana dalam menyelesaikan kasus *carding*, penegak hukum mengadili dengan menggunakan KUHP dan UU ITE, dimana kedua Undang-Undang tersebut nyatanya tidak sepenuhnya sesuai, secara sederhana bisa dilihat dari satu aspek, misalnya tentang konsep kejahatan yang terjadi. *Carding* dengan pencurian biasa pada dasarnya berbeda. Namun dalam mekanisme penegakan hukumnya disamakan.

Dalam kaitannya dengan upaya pencegahan masalah ini dan pastinya sesuai dengan tinjauan UU ITE, terdapat beberapa hal yang seyogyanya penting dan perlu untuk diperjelas pengaturannya, antara lain :[16]

1. Tanggung jawab penyelenggara sistem elektronik, dimana perlu untuk dilakukan pembatasan atau limitasi.
2. Informasi elektronik atau tandatangan yang dihasilkan oleh suatu sistem informasi, termasuk print out harus dapat menjadi alat bukti yang sah di pengadilan.
3. Perlindungan hukum teradap bank sentral dan lembaga perbankan atau keuangan penerbt kartu kredit, kartu pembayaran, dan lembaga keuangan lainnya dari kemungkinan adanya gangguan dan ancaman kejahatan eletronik.
4. Ancaman pidana yang bersifat deterren terhadap tindak kejahatan elektronik (cybercrime), sehingga dapat memberikan perlindungan terhadap integritas sistem dan nilai investasi yang telah dibangun dengan alokasi sumber daya yang cukup besar.

[16] Nazarudin Tianotak, urgensi cyberlaw di Indonesia, Jurnal Sasi Vol. 17 No.4 Bulan Oktober – Desember 2011. 25

Dalam upaya pelaksanaan, agar penegakkan hukum dapat terlaksana dengan baik maka harus dipenuhi empat syarat, yaitu: (1) Adanya aturan perundang-undangan khusus yang mengatur dunia cyber. (2) Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus yang khusus menangani cyber crime. (3) Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu. (4) Kesadaran hukum dari masyarakat yang terkena peraturan. Tujuan pembentukan undang-undang yang khusus mengatur tentang dunia maya ini adalah untuk pemberatan atas tindakan pelaku agar dapat menimbulkan efek jera dan mengatur sifat khusus dari sistem pembuktian. Dengan adanya undang-undang yang khusus mengatur cybercrime maka dapat mempermudah bagi aparat penegak hukum dalam penegakan hukum.[17]

Kesimpulan

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai Undang-Undang pertama yang dirancang dengan tujuan untuk menangani kejahatan eletronik dalam hal ini adalah kejahatan carding banyak memiliki kekurangan dalam pasal-pasal didalamnya, dalam artian Undang-Undang ini masih cukup global, sebab mencampur banyak aspek-aspek dalam dunia elektronik dalam satu Undang-Undang, sehingga penulis mengartikan secara singkat, dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik kurang fokus dann kurang mengcover atas permasalahan-permasalahan yang terjadi, sehingga Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini masih belum cukup mampu untuk berdiri sendiri, melainkan harus diiringi dengan menggunakan undang-undang lain.
2. Banyaknya kalkulasi kasus yang terjadi, bukan hanya faktor undang-undang yang belum cukup mampu mengcover saja, namun tidak menutup faktor lain. Dalam penelitian ini menemukan fakta bahwa hambatan terbesar yang dialami oleh Bank X 3 yakni faktor nasabah, jangkauan dalam mengontrol dan juga faktor penangkapan pelaku. Faktor nasabah dalam penelitian ini merujuk pada kelalaian nasabah dan juga rendahnya tingkat kesadaran nasabah akan pentingnya menjaga data personal. Penangkapan pelaku juga menjadi hambatan yang cukup terlihat, dimana kejahatan carding sendiri bukan kejahatan biasa, melainkan dapat berbeda yurisdiksi.

Daftar Pustaka

Barda Nawawi Arief, *Strategi Penanggulangan Kejahatan Telematika*,Yogyakarta: PT. Atmajaya Yogyakarta, 2010.Suratman, *Cyber Crime (modus operandi dan penanggulangannya)*, Yogyakarta: Laksbang Presindo, 2007.

Comex Crisna Wijaya, Kejahatan Carding dalam Perspektif Undang-Undang ITE dan Hukum Islam, (Skripsi Universitas Islam Negeri Sunan Kalijaga Yogyakarta".

[17] Nuria Siswi Enggarani, Penanggulangan Kejahatan Internet di Indonesia, Jurnal Ilmu Hukum,Vol. 15, No 2, September 2012 : 149-168. 161.

Etty Mulyati,*Kredit Perbankan: Aspek Hukum dan Pengembangan Usaha Mikro Kecil dalam Pembangunan Perekonomian Indonesia,* Bandung: Refika Aditama, 2016.

Nazarudin Tianotak, urgensi cyberlaw di Indonesia, Jurnal Sasi Vol. 17 No.4 Bulan Oktober – Desember 2011.

Nunuk Sulisrudatin, "Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit," *Jurnal Hukum Dirgantara,* Volume 9 no. 1(September 2018): 28.

Nuria Siswi Enggarani, Penanggulangan Kejahatan Internet di Indonesia, Jurnal Ilmu Hukum,Vol. 15, No 2, September 2012 : 149-168. 164.

Said Noor Prasetyo, Rumusan Pengaturan Credit Card Fraud dalam Hukum Pidana Indonesia ditinjau dari Asas Legalitas, Legality, Vol. 24, No.1, Maret 2016-Agustus 2016, hlm. 101-119.

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

Boy, "Kasus Pembobolan Kartu Kredit Tiket Kekinian Bukti Praktik Carding Masih Marak," JPPN, 07 Maret 2020, diakses pada tanggal 29 April 2020, 14.57 WIB, https://m.jpnn.com/new/kasus-pembobolan-kartu-kredit-tiket-kekinian-bukti-praktik-carding-masih-marak.

wawancara dengan penyelia manajemen resiko *unit fraud control and authorization LNC Bank X, 14 April 2020.*