ANALISA KASUS CYBERCRIME BIDANG PERBANKAN BERUPA MODUS PENCURIAN DATA KARTU KREDIT

Oleh :

Nunuk Sulisrudatin

Dosen Tetap Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma Jakarta,
dan aktif di Lembaga Konsultasi dan Bantuan Hukum (LKBH) Fakultas Hukum Unsurya
Email : bununux@gmail.com

Abstrak :

Kemajuan di bidang teknologi informasi dan komputer yang didukung dengan semakin lengkapnya infrastruktur informasi secara global, telah mengubah pola dan cara kegiatan masyarakat dalam berbagai aspek. Bagi perekonomian, kemajuan di bidang teknologi tersebut telah menciptakan efisiensi yang luar biasa. Bagi perbankan, hal tersebut telah mengubah strategi dan pola kegiatannya. Tidak dapat dibayangkan apabila perbankan yang mengelola jutaan nasabahnya harus melakukan kegiatannya tersebut secara manual dan tanpa bantuan komputer. Namun demikian, di sisi lain, perkembangan teknologi yang begitu cepat tidak dapat dipungkiri telah menimbulkan ekses negatif, yaitu berkembangnya kejahatan yang lebih canggih yang dikenal sebagai Cybercrime, bahkan lebih jauh lagi adalah dimanfaatkannya kecanggihan teknologi informasi dan komputer oleh pelaku kejahatan perbankan untuk tujuan pencurian data kartu kredit para nasabah**.**

PENDAHULUAN

Bank sebagai lembaga ekonomi melakukan dua kegiatan pokok, yaitu menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya ke masyarakat dalam bentuk kredit atau bentuk lain dalam rangka meningkatkan taraf hidup masyarakat. Sebagai tempat perputaran uang, bank memiliki kedudukan yang rentan terhadap penyalahgunaan kewenangan, baik oleh pihak bank sendiri maupun oleh pihak luar yang memanfaatkan bank sebagai tempat untuk menyembunyikan hasil kejahatannya. Akan tetapi terdapat kegiatan perbankan memiliki motif tertentu sehingga melampaui atau tidak sesuai dengan ketentuan yang berlaku. Kegiatan semacam ini disebut kejahatan perbankan atau tindak pidana perbankan. Tindak pidana perbankan yang dapat dilakukan dalam serangkaian kegiatan perbankan tersebut berkaitan dengan sistem keamanan dalam menjalankan setiap aktivitasnya. Sistem keamanan tidak hanya menyangkut sumberdaya manusianya saja, akan tetapi juga infrastruktur yang sampai sekarang terus berkembang.

Kejahatan perbankan lahir dan tumbuh seiring dengan kemajuan ilmu pengetahuan dan teknologi yang dicapai oleh manusia. Kejahatan tersebut termasuk dalam kategori kejahatan kelas "elite". Dikatakan "elite", karena tidak semua orang dapat melakukannya. Kejahatan kelas "elite" ini tidak membutuhkan tenaga fisik yang banyak. Kemampuan pikir merupakan faktor yang penting untuk mencapai hasil yang berlipat ganda. Semakin maju dan berkembang peradaban

umat manusia, akan semakin mewarnai bentuk dan corak kejahatan yang akan muncul ke permukaan. Oleh karena itu setelah komputer merajelela di berbagai belahan dunia, maka orangpun lalu disibukkan dan direpotkan pula dengan efek samping yang ditimbulkannya yaitu berupa kejahatan komputer (*cyber crime*).

Apabila kita berbicara mengenai kejahatan berteknologi tinggi seperti kejahatan Internet atau cybercrime, seolah-olah hukum itu ketinggalan dari peristiwanya (*het recht hink achter de feiten aan*). Seiring dengan berkembangnya pemanfaatan Internet, maka mereka yang memiliki kemampuan dibidang komputer dan memiliki maksud-maksud tertentu dapat memanfaatkan komputer dan Internet untuk melakukan kejahatan atau "kenakalan" yang merugikan pihak lain. **TB. Ronny R. Nitibaskara** menyebutkan *cyber crime* sebagai kejahatan yang terjadi melalui atau pada jaringan komputer di dalam internet.[1] Tapi pada dasarnya, istilah *cyber crime* merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya *(cyberspace)* dan tindakan yang menggunakan komputer.[2] Secara sederhana cybercrime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk didalamnya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit (*carding*), *confidence fraud*, penipuan identitas, pornografi anak, dan lain-lain.

Indonesia tercatat sebagai negara yang kasus *cybercrime*-nya paling banyak. Mabes Polri merilis kerugian dari aktivitas kejahatan perbankan menyasar sistem pembayaran di Indonesia. Kerugian mencapai angka Rp. 33 miliar selama periode 2012-2015. "Periode 2012-2015 akumulasi Rp 33 miliar, pelakunya 497 orang," menurut Direktur Tindak Pidana Ekonomi dan Khusus Bareskrim Mabes Polri (Dirtipideksus) Bareskrim Polri, Brigjen Victor Simanjuntak saat acara seminar pencegahan kejahatan dunia maya di BI, Jakarta, Selasa (28/4/2015).[3] Berdasarkan data selama dua tahun terakhir, Subdirektorat Cyber Crime Bareskrim Polri telah menerima 101 laporan pencurian uang nasabah dari 35 negara dengan total kerugian mencapai puluhan miliar rupiah. Modus operandi yang dilaporkan juga beragam, mulai dari penipuan penjualan barang, penipuan dengan memalsukan alamat email, penipuan lewat penanaman saham, membajak ATM nasabah hingga memanipulasi mesin ATM agar dapat dibobol.[4]

Akan tetapi, kejahatan jenis ini seringkali tidak terpantau dan bahkan dalam banyak hal aparat penegak hukum justru kalah terampil dari pelakunya, baik itu yang berkenaan dengan objek yang menjadi sasaran kejahatan maupun masalah pembuktian dalam proses peradilan. Contoh *cybercrime* dalam transaksi perbankan yang menggunakan sarana internet sebagai basis transaksi adalah sistem layanan kartu kredit dan layanan perbankan online (*online banking*). Dalam sistem layanan yang pertama, yang perlu diwaspadai adalah tindak kejahatan

[1] Widodo, *Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana kerja sosial dan Pidana Pengawasan Bagi Pelaku Cyber crime*, (Yogyakarta: Laksbang Mediatama, 2009), hal. 23.

[2] Dikdik M Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi,* (Bandung: Refika Aditama, 2009), hal. 7.

[3] Feby Dwi Sutianto, *Cyber Crime Perbankan Makin Lihai, Kerugian Capai Rp 33 Miliar*, www.detikinet.com, (Jakarta: Selasa, 28 April 2015).

[4] Fabian Januarius Kuwado, *Waspada, Rekening Nasabah di Indonesia Rentan Dibobol*, www.kompas.com, (Jakarta: Selasa, 21 April 2015).

yang dikenal dengan istilah *carding*. Prosesnya adalah, pelaku *carding* memperoleh data kartu kredit korban secara tidak sah (*illegal interception*) dan kemudian menggunakan kartu kredit tersebut untuk berbelanja di toko online (*forgery*). Modus ini dapat terjadi kemungkinan akibat lemahnya sistem autentifikasi yang digunakan dalam memastikan identitas pemesan barang di toko online.

Namun demikian, peringkat pembobolan kartu kredit di Indonesia masih berada pada posisi kedua terendah dibandingkan negara lain di wilayah Asia Pasifik. Sedangkan berdasarkan data Visa, peringkat *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.[5]

Dapat diketahui salah satu kasus pencurian data kartu kredit yang berhasil diungkap oleh pihak kepolisian yaitu tertangkapnya bandit penipuan kartu kredit, berinisial BA (37) dan AL (37). Direktur Kriminal Umum Polda Metro Jaya Kombes Pol Khrisna Murti mengatakan, kedua pelaku berhasil menggasak uang dari bank swasta lewat kartu kredit korban sebanyak ratusan juta rupiah. Sedangkan pihak bank selaku korban mengalami kerugian Rp600 juta untuk periode Januari hingga Mei 2015. Atas perbuatannya, para tersangka dikenakan Pasal 379 dan Pasal 362 KUHP dengan ancaman hukuman penjara paling lama empat dan lima tahun. [6]

Modus operandi kedua pelaku, yaitu dengan membeli daftar nasabah yang berisi data pemegang kartu kredit salah satu bank swasta dari pihak marketing. Mereka beralasan menawarkan asuransi jiwa, yang dilakukan pelaku BA. Setelah berhasil mendapatkan daftar data pribadi pemegang kartu kredit, tersangka BA menghubungi nomor telepon pengguna kartu kredit yang berada di dalam data tersebut dan mengaku dari *credit card* pusat bank swasta. Kemudian kepada para korban, BA menjelaskan dan menggunting kartu kredit korban dengan modus akan menggantinya dengan kartu kredit baru dengan limit yang lebih besar tanpa biaya administrasi. Kemudian salah satu pelaku, yakni AL berperan sebagai kurir untuk mengambil kartu kredit korban berikut fotokopi KTP dengan alasan untuk menyesuaikan data dan memberikan tanda terima dengan logo salah satu bank atas nama pemilik kartu kredit. Pelaku BA membuat KTP palsu dengan data identitas fotokopi KTP korban yang akan dipergunakan pada saat melakukan transaksi di toko untuk membeli barang-barang mewah.[7]

Sehubungan dengan apa yang diuraikan di atas, maka dengan semakin canggih teknologi semakin terbuka pula peluang melakukan tindak kejahatan tidak terkecuali di dunia perbankan. Hal tersebut membuktikan bahwa terdapatnya perubahan (pergeseran) wajah pelaku kejahatan di Indonesia, yang disebabkan

[5] Novita Intan Sari, *Kasus-kasus pembobolan kartu kredit yang menggemparkan*, www.merdeka.com, (Jakarta: Sabtu, 5 Desember 2015)

[6] Raiza Andini, *Bandit Kartu Kredit Ditangkap, Dua Orang Diburu*, www.news.com, (Jakarta: Minggu, 7 Juni 2015)

[7] Ibid

oleh perkembangan pembangunan nasional kita. Pergeseran dimaksud adalah tentang kejahatan yang dilakukan oleh korporasi. Pelaku kejahatan di sini bukanlah manusia, tetapi adalah suatu kesatuan yang disamakan dengan manusia seperti berbagai kejahatan perbankan menyangkut cybercrime salah satunya adalah pencurian data kartu kredit (*fraud*). Motif kejahatan ini dinilai karena adanya faktor pekerjaan dan adanya peluang atau kesempatan untuk memperdayai korban hingga bersedia memberikan kartu kredit miliknya.

KEJAHATAN PERBANKAN

Kejahatan di bidang perbankan adalah kejahatan apapun yang menyangkut perbankan, misalnya seseorang merampok bank adalah kejahatan di bidang perbankan, begitu pula pengalihan rekening secara tidak sah adalah kejahatan di bidang perbankan, jadi pengertiannya sangat luas. Sedangkan kejahatan perbankan adalah bentuk perbuatan yang telah diciptakan oleh undang-undang perbankan yang merupakan larangan dan keharusan, misalnya larangan mendirikan bank gelap dan pembocoran rahasia bank. Perbedaan isitlah ini menyebabkan atau berpengaruh terhadap penegakan hukum. Kejahatan perbankan akan ditindak melalui ketentuan pidana yang diatur dalam undang-undang perbankan, sedangkan kejahatan di bidang perbankan ditindak melalui undang-undang di luar undang-undang perbankan.[8]

Terdapat dua istilah kejahatan perbankan yang seringkali dipakai secara bergantian walaupun maksud dan ruang lingkupnya bisa berbeda. Pertama, adalah "Tindak Pidana Perbankan" dan kedua, "Tindak Pidana di Bidang Perbankan". Tindak pidana perbankan mengandung pengertian tindak pidana itu semata-mata dilakukan oleh bank atau orang bank, sedangkan tindak pidana di bidang perbankan tampaknya lebih netral dan lebih luas karena dapat mencakup tindak pidana yang dilakukan oleh orang di luar dan di dalam bank.[9] Istilah "tindak pidana di bidang perbankan" dimaksudkan untuk menampung segala jenis perbuatan melanggar hukum yang berhubungan dengan kegiatan-kegiatan dalam menjalankan usaha bank. Tidak ada pengertian formal dari tindak pidana di bidang perbankan. Ada yang mendefinisikan secara popular, bahwa tindak pidana perbankan adalah tindak pidana yang menjadikan bank sebagai sarana (*crimes through the bank*) dan sasaran tindak pidana itu (*crimes against the bank*).

UU No. 10 Tahun 1998 tidak merumuskan pengertian tentang tindak pidana perbankan. UU ini hanya mengkategorikan beberapa perbuatan yang termasuk ke dalam kejahatan dan di satu pihak bisa dikategorikan sebagai suatu pelanggaran. Akan tetapi ada juga yang membedakan pengertian tindak pidana perbankan dengan tindak pidana di bidang perbankan. Tindak pidana di bidang perbankan adalah segala jenis perbuatan melanggar hukum yang berhubungan dengan kegiatan dalam menjalankan usaha bank, baik bank sebagai sasaran maupun sebagai sarana, sedangkan tindak pidana perbankan (*banking crime*) merupakan tindak pidana yang dilakukan oleh bank.[10]

Adapun karakteristik dalam tindak pidana perbankan adalah bank bisa sebagai korban maupun sebagai pelaku. Bank sebagai korban misalnya dalam hal

[8] Edi Setiadi dan Rena Yulia, *Hukum Pidana Ekonomi*, (Yogyakarta: Graha Ilmu, 2010), hal. 140.

[9] Marjono Reksodiputro, *Kemajuan Pembangunan Ekonomi dan Kejahatan*, (Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum, 1994), hal. 74.

[10] Edi Setiadi dan Rena Yulia, Op.cit, hal. 140.

penipuan, pemalsuan surat-surat bank, dan bank sebagai pelaku misalnya perbuatan *window dressing*, menetapkan suku bunga berlebihan, memberikan kartu kredit yang tidak wajar, menjalankan usaha bank dalam bank, menjalankan usaha bank tanpa ijin serta menjalankan usaha yang menyerupai bank. Untuk menentukan seseorang atau korporasi menjadi korban atau tidak, perlu diketahui terlebih dahulu perbuatan seperti apakah yang disebut sebagai kejahatan atau tindak pidana. Beberapa perbuatan pidana yang bisa dikategorikan sebagai kejahatan perbankan dan telah diatur dalam perundang-undangan adalah:

1. Dalam KUHP Buku II Bab X tentang Pemalsuan Mata Uang dan Uang Kertas, yaitu Pasal 244, 245, 246, 249, dan 250.
2. Dalam UU No. 7 Tahun 1992 jo UU No 10 Tahun 1998
   a. Tindak pidana berkaitan dengan perizinan (Pasal 46)
   b. Tindak pidana berkaitan dengan rahasia bank (Pasal 47 dan 47a)
   c. Tindak pidana berkaitan dengan pengawasan bank (Pasal 48)
   d. Tindak pidana berkaitan dengan kegiatan usaha bank (Pasal 49)
   e. Tindak pidana berkaitan dengan pihak terafiliasi (Pasal 50)
   f. Tindak pidana berkaitan dengan pemegang saham (Pasal 50a)
3. Tindak Pidana yang diatur dalam UU Tentang Bank Sentral.

CYBER CRIME

Memang tidak dapat dibantahkan bahwa penggunaan teknologi internet banyak memberikan bantuan untuk menyelesaikan persoalan yang rumit secara efektif dan efisien. Hanya saja, kecanggihan teknologi ini juga berpotensi membuat orang cenderung melakukan perbuatan yang bertentangan dengan norma-norma sosial yang berlaku. Penggunaan teknologi internet telah membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial suatu negara yang dahulu ditetapkan sangat esensial sekali yaitu dunia maya, dunia yang tanpa batas atau realitas virtual (*virtual reality*). Inilah sebenarnya yang dimaksud dengan *Borderless World*.[11]

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dunia internasional.[12] Dalam arti sempit *cybercrime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, *cybercrime* mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunaanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime)*.[13] Dengan demikian *cybercrime* meliputi kejahatan, yaitu yang dilakukan:

1. Dengan menggunakan saranasarana dari sistem atau jaringan komputer (*by means of a computer system or network*) ;
2. Di dalam sistem atau jaringan komputer (*in a computer system or network*) ; dan
3. Terhadap sistem atau jaringan komputer (*against a computer system or network*).

[11] Agus Raharjo, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Aditya Bahkti, 2002), hal.5.

[12] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia,* (Jakarta: PT Raja Grafindo Persada, 2007), hal.1

[13] Barda Nawawi Arief, *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan*, (Bandung: Citra Aditya Bakti, 2001), hal. 249-250.

Dari definisi tersebut, maka dalam arti sempit *cybercrime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, *cybercrime* mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime*). Kegiatan yang potensial menjadi target *cybercrime* dalam kegiatan perbankan antara lain adalah:

1. Layanan pembayaran menggunakan kartu kredit pada situs-situs toko online.
2. Layanan perbankan online (*online banking*).

Dapat diketahui terdapat beberapa jenis-jenis dari cybercrime bila dilihat dari aktivitasnya, yaitu sebagai berikut:

1. *CARDING* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet. Sebutan pelakunya adalah "*carde*r". Sebutan lain untuk kejahatan jenis ini adalah *cyberfroud* alias penipuan di dunia maya.
2. *HACKING* adalah menerobos program komputer milik orang/pihak lain. *Hacker* adalah orang yang gemar ngoprek komputer, memiliki keahlian membuat dan membaca program tertentu dan terobsesi mengamati keamanan (*security*)-nya.
3. *CRACKING* adalah hacking untuk tujuan jahat. Sebutan untuk "*cracker*" adalah "*hacker*" bertopi hitam *(black hat hacker*). Berbeda dengan "*carde*r" yang hanya mengintip kartu kredit, "*cracker*" mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, "*hacker*" lebih fokus pada prosesnya. Sedangkan "cracker" lebih fokus untuk menikmati hasilnya.
4. *DEFACING* adalah kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs Menkominfo dan Partai Golkar, BI baru-baru ini dan situs KPU saat pemilu 2004 lalu. Tindakan *deface* ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat, untuk mencuri data dan dijual kepada pihak lain.
5. *PHISING* adalah kegiatan memancing pemakai komputer di internet *(user*) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (*password*) pada suatu website yang sudah di-*deface*. Phising biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password yang vital.
6. *SPAMMING* adalah pengiriman berita atau iklan lewat surat elektronik (*e-mail*) yang tak dikehendaki. *Spam* sering disebut juga sebagai *bulk e-mail* atau *junk e-mail* alias "sampah".
7. *MALWARE* adalah program komputer yang mencari kelemahan dari suatu *software*. Umumnya *malware* diciptakan untuk membobol atau merusak suatu *software* atau *operating system*. *Malware* terdiri dari berbagai macam, yaitu: virus, worm, trojan horse, adware, browser hijacker, dll.[14]

Sedangkan jenis – jenis cybercrime bila berdasarkan modus operandinya adalah:

1. *Unauthorized Access to Computer System and Service*, kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer

[14] *Jenis-Jenis Cybercrime*, www.ecommerce.com

secara tidak sah tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

2. *Illegal Contents*, merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
3. *Data Forgery* merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless document melalui Internet.
4. *Cyber Espionage* merupakan kejahatan yang memanfaatkan jaringan Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran.
5. *Cyber Sabotage and Extortion*, kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya atau berjalan sebagaimana yang dikehendaki oleh pelaku.
6. *Offense against Intellectual Property*, kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh, peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
7. *Infringements of Privacy*, kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM.[15]

Direktur Departemen Kebijakan dan Pengawasan Sistem Pembayaran BI Ida Nuryanti mengatakan ada sejumlah modus kejahatan perbankan atau cybercrime yang sering kali terjadi yaitu berupa malware, phishing, dan skimming. "Malware, yaitu sinkonisasi token, dimana sistem di bank baik tapi yang diserang yakni device media komunikasi yang sering digunakan pengguna. Phishing merupakan upaya pencurian informasi nasabah berupa user id, kata sandi atau password rekening maupun kartu kredit. "Jadi ada website yang mirip dengan website aslinya dimana kita diminta memasukan nomor rekening beserta password. Sedangkan skimming adalah tindak pencurian data nasabah dengan menggunakan alat perekam data. Biasanya kejahatan ini terjadi di mesin anjungan tunai mandiri dan EDC. "Dengan chip belum terbukti bisa diskimming. Kartu kredit sudah ada chipnya, sekarang yang masih proses itu kartu debit beralih chip.[16]

MODUS PENCURIAN DATA KARTU KREDIT

Sebagai bentuk kejahatan yang dapat dikategorikan baru, karakteristik *cybercrime* berbeda dengan kejahatan (tradisional)

[15] Ibid

[16] Yanita Petriella, *Ini Modus Kejahatan Perbankan Yang Berbasis Cyber Crime*, www.bisnis.com, (Jakarta: Rabu, 3 Juni 2015).

lainnya. Secara umum dapat diketahui yang menjadi ciri-ciri kejahatan ini adalah:

1. *Non-violence* (tanpa kekerasan);
2. Sedikit melibatkan kontak fisik;
3. Menggunakan peralatan (*equipment*) dan teknologi;
4. Memanfatkan jaringan telematika (telekomunikasi, media dan informatika) global.[17]

Dalam hal bank sebagai korban, pada umumnya bisa dilihat pada KUHP pasal-pasal 263, 264 dan 378, sedangkan dalam hal bank sebagai pelaku, maka bisa dilihat pada undang-undang perbankan. Modus operandi dalam hal bank sebagai korban tidak begitu banyak, biasanya hanya dalam bentuk pemalsuan dokumen, penggelapan dan korupsi, pelakunya biasanya orang, bukan korporasi. Apabila pelakunya adalah bank (sebagai korporasi), modus operandinya bisa bermacam-macam. Kejahatan ini dikategorikan sebagai *criminal banking* dan selalu dilakukan secara *organized*. Dalam hal ini kegiatan perbankan hanyalah merupakan kamuflase karena seluruh kegiatannya adalah memang *systemic violation of the law for the purposes of making a profit*. Anatomi *criminal banking* biasanya yang paling popular adalah *money laundering dan window dressing*.[18]

Sebagaimana telah disebutkan ekses negatif yang diahirkan dari perkembangan bentuk-bentuk *cybercrime* ialah berkembangnya modus operandi dari kejahatan tradisional yang mempergunakan ruang virtual dalam melakukan kejahatan. Dalam fokus *cybercrime* pada penelitian ini terletak pada bentuk kejahatan tradisional yang memasuki ruang virtual dengan bantuan peralatan komputer dan teknologi internet. Contoh *cybercrime* dalam transaksi perbankan yang menggunakan sarana Internet sebagai basis transaksi adalah sistem layanan kartu kredit dan layanan perbankan *online* (*online banking*). Dalam sistem layanan yang pertama, yang perlu diwaspadai adalah tindak kejahatan yang dikenal dengan istilah *carding*. Prosesnya adalah sebagai berikut, pelaku *carding* memperoleh data kartu kredit korban secara tidak sah (*illegal interception*), dan kemudian menggunakan kartu kredit tersebut untuk berbelanja di toko *online* (*forgery*). Modus ini dapat terjadi akibat lemahnya sistem autentifikasi yang digunakan dalam memastikan identitas pemesan barang di toko *online*.

Kegiatan yang kedua yaitu perbankan *online* (*online banking*). Modus yang pernah muncul di Indonesia dikenal dengan istilah *typosite* yang memanfaatkan kelengahan nasabah yang salah mengetikkan alamat bank *online* yang ingin diaksesnya. Pelakunya sudah menyiapkan situs palsu yang mirip dengan situs asli bank *online* (*forgery*). Jika ada nasabah yang salah ketik dan masuk ke situs bank palsu tersebut, maka pelaku akan merekam *user ID* dan *password* nasabah tersebut untuk digunakan mengakses ke situs yang sebenarnya (*illegal access*) dengan maksud untuk merugikan nasabah. Adapun cara Kerja Modus Pencurian Data Kartu kredit / credit card

1. Membeli data nasabah dari oknum Bank senilai 20.000 rupiah.
2. Kemudian si pelaku menelpon satu persatu nasabah kartu kredit dengan mengatas namakan pihak bank dengan alasan penawaran upgrade paket.
3. Kemudian apabila si korban sudah setuju maka mereka akan mendatangkan kurir ke pihak korban.
4. Kemudian setelah kurir datang mereka akan meminta data lengkap, seperti

[17]Tb. Ronny Rahman Nitibaskara, *Ketika Kejahatan Berdaulat*, (Jakarta:Peradaban, 2001), hal. 45.
[18]Edi Setiadi dan Rena Yulia, Op.cit, hal 143-144.

KTP, dan kartu kredit yang nantinya akan di scan atau bahasa umumnya di foto copy secara bolak balik ktp dan kartu kredit.

5. Kemudian setelah selesai si pelaku akan membuat duplikat kartu kredit anda dan mereka akan datang kembali kepada anda dan memberikan kartu kredit yang baru dengan datang ke tempat anda tinggal, dan si pelaku akan datang dan mengunting kartu kredit anda agar anda terlihat lebih percaya.
6. Apa yang mereka gunting itu adalah kartu kredit yang palsu dan yang asli sudah mereka kantongi.[19]

Sedangkan yang dimaksud dengan *fraud* dalam kartu kredit, adalah *Fraud* berarti tindakan melanggar hukum yang dilakukan seseorang atau sekelompok orang untuk mendapatkan keuntungan finansial dari penggunaan kartu kredit yang bukan menjadi hak miliknya. Dan salah satu tindakan kejahatan yang umum dilakukan adalah pencurian data kartu kredit, atau yang biasa disebut dengan istilah *phishing*.[20] Orang atau komplotan yang melakukan *phishing* biasanya mengincar 4 digit nomor di belakang kartu kredit, dan nomor PIN-nya. Informasi ini kemudian digunakan oleh pelaku untuk bertransaksi atas nama nasabah. terdapat empat teknik yang umum atau sering dilakukan pelaku pencurian data kartu kredit, yaitu sebagai berikut:

1. Menelpon untuk memperbaharui data diri kartu kredit
   Pelaku akan menelpon dan mengaku sebagai perwakilan dari pihak Bank atau surveyor yang ingin memperbaharui data kartu kredit. Modus ini juga bisa dilakukan via E-Mail, dimana pelaku menanyakan hal yang sama seperti diatas.
2. Transaksi di toko online palsu
   Modus lain yang sering digunakan adalah membuat situs belanja online palsu. Karena apabila melakukan pembayaran kartu kredit pada situs online yang tidak terpercaya, kemungkinan tujuan mereka adalah mencuri data kartu kredit.
3. *Skimming*
   Teknik *skimming* dilakukan dengan menggunakan alat penyalin informasi. Umumnya, alat ini ditempelkan pada mesin ATM Bank. Namun juga dapat dilakukan pada mesin EDC kartu kredit dengan metode yang sama.
4. Menggunakan koneksi Wi-Fi palsu
   Pelaku menggunakan sebuah alat seperti reuter internet, yang dapat menciptakan koneksi internet Wi-Fi palsu di gadget calon korban. Ketika calon korban telah terkoneksi dengan koneksi ini, si pelaku dapat dengan mudah melihat informasi yang tersimpan dalam *browsing history* korban. Salah satu informasi yang biasanya dicari pelaku adalah informasi transaksi kartu kredit.

UPAYA PENCEGAHAN TINDAK PIDANA

Kejahatan atau tindak pidana merupakan perbuatan menimbulkan penderitaan, sehingga harus dicegah atau ditanggulangi. Akan tetapi mencegah atau menanggulangi kejahatan tidaklah mudah atau disamakan begitu saja langkahnya untuk setiap kejahatan. Kejahatan atau tindak pidana perbankan misalnya, tak bisa dicegah atau ditanggulangi dengan cara-cara biasa sebagaimana tindak pidana pada umumnya. Pembobolan bank yang terjadi pada umumnya melibatkan orang dalam bank (pihak interent/pihak

[19]Toto Haryanto, *Modus Baru Pencurian Kartu Kredit Terungkap*, www.totoharyato.com, (Jakarta: Senin 15 Juni 2015).
[20] Waspadai 4 Modus Pencurian Data Kartu Kredit!, www.helomoney.com, (April 6, 2015

terafiliasi) yang tentunya mengetahui seluk beluk mekanisme dan system keamanan bank yang bersangkutan. Keterlibatan orang dalam ini ada yang memang murni inisiatif dan kerjasama antar orang dalam, ada juga kolaborasi antara orang dalam bank dengan orang luar bank (eksteren), atau bahkan benar-benar pembobolan yang dilakukan oleh orang luar bank dengan merusak sistem pada sebuah bank dengan melakukan *hacker* menggunakan fasilitas internet.[21]

Kejahatan atau tindak pidana perbankan memiliki karakteristik yang khas, yang membedakan dengan tindak pidana lain, sehingga harus dicegah dan ditanggulangi dengan cara-cara yang khas pula. Oleh karena keadaan yang seperti itu, maka kendala selalu muncul dalam upaya mencegah dan menanggulangi kejahatan perbankan. Adapun terdapat beberapa kendala dalam penanganan tindak pidana perbankan, yaitu:

1. Belum adanya kesamaan pandang tentang penggunaan dokumen fotokopi sebagai barang bukti dan dalam menetapkan undang-undang atau ketentuan yang dilanggar dalam tindak pidana bank;
2. Tingkat pemahaman para penegak hukum terhadap kegiatan/operasional perbankan yang berbeda-beda dan belum merata serta lemahnya koordinasi dalam penanganan kasus perbankan;
3. Belum efektifnya tindak lanjut penanganan kasus yang telah diserahkan oleh Bank Indonesia kepada penyidik;
4. Terdapat beberapa kasus yang sulit diungkapkan modus operandinya yang antara lain disebabkan oleh pesatnya kemajuan atau perkembangan teknologi informasi.

Pencegahan dan penanggulangan tindak pidana dalam kerangka kebijakan kriminal dapat dilakukan dengan 2 (dua) cara, yaitu penal (*penal policy*) dan non penal (*non penal policy*). *Penal policy* lebih ditekankan kepada upaya represif dari penegak hukum yang didahului dengan ketersediaan undang-undangnya. *Penal policy* menjadi tugas polisi, jaksa, hakim, dan tentunya Bank Indonesia dalam hal pelanggaran administrasi. Sedangkan *non-penal policy*, menjadi tugas dari aparat penegak hukum, bank Indonesia, bank pemerintah maupun swasta dan masyarakat. Adapun pengaturan tindak pidana *cyber* di Indonesia juga dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana *cyber* ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana ("KUHP") sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana *cyber* dalam arti luas. Demikian juga tindak pidana dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana maupun tindak pidana perbankan serta tindak pidana pencucian uang.

Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana *cyber* diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE"). Sama halnya seperti *Convention on Cybercrimes*, UU ITE juga tidak memberikan definisi mengenai *cybercrimes*, tetapi membaginya menjadi beberapa pengelompokkan yang mengacu pada *Convention on Cybercrimes*:

[21]Sutan Remy Sjahdeini, *Himpunan Tulisan Kapita Selekta Hukum Perbankan, jilid 1*, (Jakarta: UI Press, 2006), hal. 20

1. Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:
   a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yaitu:
      1) Kesusilaan (Pasal 27 ayat [1] UU ITE);
      2) Perjudian (Pasal 27 ayat [2] UU ITE);
      3) Penghinaan atau pencemaran nama baik (Pasal 27 ayat [3] UU ITE);
      4) Pemerasan atau pengancaman (Pasal 27 ayat [4] UU ITE);
      5) Berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat [1] UU ITE);
      6) Menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat [2] UU ITE);
      7) Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);
   b. Dengan cara apapun melakukan akses illegal (Pasal 30 UU ITE);
   c. Intersepsi illegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 UU ITE);
2. Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:
   a. Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference* – Pasal 32 UU ITE);
   b. Gangguan terhadap Sistem Elektronik (*system interference* – Pasal 33 UU ITE);
3. Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE);
4. Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);
5. Tindak pidana tambahan (*accessoir* Pasal 36 UU ITE); dan
6. Perberatan – perberatan terhadap ancaman pidana (Pasal 52 UU ITE). [22]

Dapat diketahui selain mengatur tindak pidana *cyber* materil, UU ITE mengatur tindak pidana *cyber* formil, khususnya dalam bidang penyidikan. Pasal 42 UU ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam Undang-Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana ("KUHAP") dan ketentuan dalam UU ITE. Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain:

1. Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Kementerian Komunikasi dan Informatika;
2. Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data;
3. Penggeledahan dan atan penyitaan terhadap Sistem Elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat;
4. Dalam melakukan penggeledahan dan/atau penyitaan Sistem Elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Adapun salah satu pasal UU ITE di Bab VII tentang Perbuatan Yang Dilarang, Pasal 31 ayat (1) dan (2) menyebutkan, "*mereka yang secara sengaja dan tanpa hak melakukan penyadapan atas informasi dan/atau dokumen elektronik pada computer atau alat elektronik milik orang lain akan*

[22]Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, (Jakarta: PT. Tatanusa, 2012).

dikenakan hukuman berupa penjara dan/atau denda." Kecurangan fraud sama halnya dengan pemalsuan, penipuan atau pemberian gambaran atau keterangan yang tidak sebenarnya dengan tujuan memperoleh keuntungan dengan menimbulkan kerugian materil bagi pihak lain. Contohnya dari bentuk kecurangan dalam perkreditan yaitu tindakan *mark up* (penggelembungan jumlah kebutuhan investasi suatu proyek untuk mendapatkan kredit yang lebih besar dari semestinya). Bentuk tindakan lain yang dapat digolongkan pada penipuan dan kecurangan dalam bidang perkreditan (*credit fraud*) yaitu tindak pidana yang diatur dalam Pasal 35 UU Nomor 42 Tahun 1999 tentang *Jaminan Fidusia*, yaitu tindakan debitor yang memberikan keterangan secara menyesatkan, sebagaimana diatur dalam Pasal tersebut, yang intinya mengatur sebagai berikut:

"Setiap orang yang sengaja memalsukan, mengubah, menghilangkan, atau dengan cara apapun memberikan keterangan secara menyesatkan sehingga terjadinya perjanjian fidusia maka dapat dipidana dengan pidana penjara paling singkat satu tahun dan paling banyak Rp. 100.000.000,00."

Ketentuan penyidikan dalam UU ITE berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan. Selain UU ITE, peraturan yang landasan dalam penanganan kasus *cybercrime* di Indonesia ialah peraturan pelaksana UU ITE dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.

Pencegahan dan penanggulangan kejahatan bukan sekadar terbatas pada upaya penal yang seringkali bersifat represif, akan tetapi akan lebih efektif jika dikaitkan langsung dengan karakteristik yang khas dari tindak pidana tersebut. Misalnya, pada tindak pidana perbankan, ciri yang khas adalah pada perhitungan alur masuk dan keluar uang dari nasabah, dan ilmu yang tepat untuk mengetahui kewajaran atau ketidakwajaran atas alur ini adalah akuntansi. Penilaian yang tepat dari ilmu ini akan mencegah secara lebih dini terjadinya tindak pidana perbankan.

Secara spesifik, menyebutkan bahwa dalam rangka penegakan hukum dan pencegahan kejahatan perbankan, maka langkah-langkah yang harus ditempuh adalah:

1. Perlunya peningkatan kemampuan penyidik dalam bidang akunting dan keuangan;
2. Sistem pengawasan dari pihak bank yang efektif dan ini bisa dilakukan kalau rekruitmen pegawai lebih menekankan kepada mental idiologi;
3. Perlunya kewenangan penyidik dalam rangka menjalankan tugasnya, bukan hanya sekadar menyangkut rahasia bank;
4. Perlunya pembaharuan perundang-undangan dalam bidang ekonomi, in casu undang-undang perbankan.[23]

Sedangkan terdapat beberapa upaya pencegahan tindak pidana, ataupun penanganan tindak pidana dimana UU ITE yang menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan computer (cybercrime),

[23]Edi Setiadi dan Rena Yulia, Op.cit, hal.145-146.

termasuk kejahatan pencurian data kartu kredit, pencucian uang dan kejahatan terorisme, yaitu antara lain:

1. *Pertama,* terkait tanggung jawab penyelenggara sistem elektronik, perlu dilakukan pembatasan atau limitasi atas tanggungjawab sehingga tanggungjawab penyelenggara tidak melampaui kewajaran.
2. *Kedua,* seluruh informasi elektronik dan tanda tangan elektronik yang dihasilkan oleh suatu system informasi, termasuk *print out*-nya harus dapat menjadi alat bukti di pengadilan.
3. *Ketiga,* perlunya aspek perlindungan hukum terhadap Bank Sentral, dan lembaga perbankan/keuangan, penerbit kartu kredit/kartu pembayaran dan lembaga keuangan lainnya dari kemungkinan adanya gangguan dan ancaman kejahatanelektronik. Dalam UU ITE ini, perlindungan tersebut dapat dilakukan dengan mengkriminalisasi setiap penggunaan dan akses yang dilakukan secara *illegal* terhadap komputer institusi/lembaga tersebut, mengingat peranan yang sangat vital dari lembaga-lembaga keuangan dalam perekonomian dan dalam rangka menjaga tingkat kepercayaan masyarakat terhadap lembaga keuangan.
4. *Keempat,* perlunya 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. [24]

[24] *Urgensi Cyberlaw Di Indonesia Dalam Rangka Penanganan Cybercrime Di Sektor Perbankan*, (Tim Perundang-undangan dan Pengkajian Hukum Direktorat Hukum Bank Indonesia, Buletin Hukum Perbankan Dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006), hal. 23.

KESIMPULAN

Kejahatan pencurian data kartu kredit yang terjadi selama ini dilakukan oleh oknum-oknum yang mengerti dan paham tentang mekanisme transaksi dan teknis jaringan dalam bank yang dituju sebagai objek pembobolan, hal ini memungkinkan adanya pihak terafiliasi (pihak dalam bank) yang turut andil melakukan pencurian data kartu kredit. Pihak-pihak yang melakukan pencurian data kartu kredit tersebut menggunakan modus porandi mulai dari pembelian data nasabah, pemalsuan dokumen, pembukuan ganda hingga menyiapkan situs online palsu. Kejahatan perbankan merupakan ancaman serius terhadap tingkat kesehatan bank dan sekaligus tingkat kepercayaan masyarakat, oleh karena itu upaya untuk mencegah dan menanggulanginya perlu dilakukan secara dini. Kerjasama dari semua pihak yang terlibat dalam kegiatan perbankan perlu dilakukan, mengingat karakteristik yang khas pada kegiatan perbankan.

Pencegahan dan penanggulangan kejahatan perbankan tak dapat diserahkan hanya kepada salah satu pihak saja dalam penegakan hukum, sehingga bukan hanya penyebab kausatif atau simptomatik yang terselesaikan, akan tetapi penyebab yang bersifat komprehensif dan dapat di atasi secara bersama-sama. Pemerintah dalam hal ini aparat hukum yang berwenang harus dapat memberi tindakan yang tegas dan hukuman yang berat serta kewajiban bagi pelaku untuk mengganti semua kerugian yang dialami bank maupun nasabah bank yang bersangkutan dengan demikian bagi pelaku yang terbukti bersalah melakukan pembobolan bank akan menyadari kesalahannya dan akan berdampak bagi pihak-pihak lain untuk tidak akan melakukan kejahatan serupa.

DAFTAR PUSTAKA

Arief, Barda Nawawi. *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan*. Bandung: Citra Aditya Bakti, 2001.

_____, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, Jakarta:* PT Raja Grafindo Persada, 2007.

Mansur, Dikdik M Arief dan Gultom, Elisatris. *Cyber Law Aspek Hukum Teknologi Informasi,* Bandung: Refika Aditama, 2009.

Nitibaskara, Tb. Ronny Rahman. *Ketika Kejahatan Berdaulat*. Jakarta: Peradaban, 2001.

Raharjo, Agus. *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya Bahkti, 2002.

Reksodiputro, Marjono. *Kemajuan Pembangunan Ekonomi dan Kejahatan*, Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum, 1994.

Setiadi, Edi dan Rena Yulia. *Hukum Pidana Ekonomi*. Yogyakarta: Graha Ilmu,2010.

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

Sjahdeini, Sutan Remy. *Himpunan Tulisan Kapita Selekta HukumPerbankan, jilid 1*. Jakarta: UI Press, 2006.

Widodo. *Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana kerja sosial dan Pidana Pengawasan Bagi Pelak Cybercrime*. Yogyakarta: Laksbang Mediatama, 2009.

Haryanto, Toto. *Modus Baru Pencurian Kartu Kredit Terungkap*, www.totoharyato.com. Jakarta: Senin 15 Juni 2015.

Kuwado, Fabian Januarius. *Waspada, Rekening Nasabah di Indonesia Rentan Dibobol*. www.kompas.com. Jakarta: Selasa, 21 April 2015.

Novita Intan Sari, *Kasus-kasus pembobolan kartu kredit yang menggemparkan*, www.merdeka.com, (Jakarta: Sabtu, 5 Desember 2015)

Petriella, Yanita. *Ini Modus Kejahatan Perbankan Yang Berbasis Cyber Crime*. www.bisnis.com. Jakarta: Rabu, 3 Juni 2015.

Raiza Andini, *Bandit Kartu Kredit Ditangkap, Dua Orang Diburu*, www.news.com, (Jakarta: Minggu, 7 Juni 2015)

Sutianto, Feby Dwi. *Cyber Crime Perbankan Makin Lihai, Kerugian Capai Rp 33 Miliar*, www.detikinet.com. Jakarta: Selasa, 28 April 2015.

Waspadai 4 Modus Pencurian Data Kartu Kredit! www.helomoney.com, (April 6, 2015