TINDAK PIDANA CYBER CRIME DALAM KEGIATAN PERBANKAN[1]

Oleh: Christian Henry Ratulangi[2]
Dr. Anna S. Wahongan[3]
Franky R. Mewengkang[4]

ABSTRAK

Tujuan dilakukannya penelitian ini adalah untuk mengetahui bagaimana bentuk-bentuk kejahatan yang termasuk sebagai kejahatan di bidang siber dan bagaimana Penerapan Hukum Pidana Terhadap Pelaku Kejahatan Siber di Sektor Jasa Keuangan dan Perbankan. Dengan menggunakan metode penelitian yuridis normatif, disimpulkan: 1. Kejahatan siber (*cyber crime)* dilakukan oleh orang baik secara sendiri maupun berkelompok yang benar-benar ahli dalam peretasan, alili dalam menggunakan komputer sebagai sarana/alat untuk melakukan kejahatan, sehingga menurut para ahli bentuk-bentuk kejahatan siber (*cyber crime*) itu secara umum adalah berupa pencurian identitas, *spionage cyber,* pemerasan *cyber,* pencurian data perusahaan, dan *carding.* Sedangkan menurut UU No. 11 Tahun 2008 yang dirobah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, bentuk-bentuk kejahatan siber (*cyber crime*) adalah tindak pidana yang berhubungan dengan aktivitas *illegal*, tindak pidana yang berhubungan dengan gangguan (interferens), tindak pidana memfasilitasi perbuatan yang dilarang, dan tindak pidana pemalsuan informasi atau dokumen elektronik. 2. Tindak kejahatan siber *(cyber crime)* di sektor jasa keuangan dan perbankan adalah *social engineering* dan *skimming.* Kedua bentuk kejahatan siber ini dilakukan dengan teknik menipu atau penipuan, penggelapan dan pencurian. Oleh karena itu penerapan hukum pidana terhadap para pelaku kejahatan siber di sektor jasa keuangan dan perbankan itu oleh para hakim banyak menggunakan pasal-pasal yang ada dalam KUHP yaitu Pasal 64 tentang perbuatan berlanjut, karena pelaku melakukannya berkali-kali, Pasal 362 tentang Pencurian, Pasal 363, pencurian yang dilakukan oleh lebih dari satu orang dan Pasal 378 tentang penggelapan.

Kata kunci: Tindak Pidana, Cyber Crime, Kegiatan Perbankan

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi yang terjadi dewasa ini telah mencapai pada titik puncak-nya. Hal ini dapat dilihat dengan semakin berkembang pesatnya fitur-fitur yang terdapat dalam tekhnologi digital, terutama teknologi komputer berbasis internet yang mengakibatkan membuat "dunia" semakin mengecil. Jarak dan waktu lebih dapat dihemat dengan perkembangan tekhnologi informasi yang ada saat ini.

Semua aktivitas yang seharusnya memerlukan waktu yang lama serta harus ditempuh dengan jarak yang jauh, untuk saat ini lebih dimungkinkan untuk dikerjakan/diakses dimana-pun hanya hitungan menit atau bahkan hitungan detik saja. Sebagaimana halnya dengan teknologi digital yang terdapat dalam fitur-fitur komputer yang berbasis internet, memungkinkan pengoperasiannya serba otomatis dan canggih, dengan sistem komputerisasi/ format yang dapat dibaca oleh komputer.

Pasal 4 UU No. 11 Tahun 2008 yang dirobah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menyebutkan bahwa pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan dengan tujuan untuk:[5]

a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
c. meningkatkan efektivitas dan efisiensi pelayanan publik;
d. membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan teknologi

[1] Artikel Skripsi
[2] Mahasiswa pada Fakultas Hukum Unsrat, NIM. 16071101361
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] *UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang dirobah dengan UU No. 19 Tahun 2016.*

informasi se-optimal mungkin dan bertanggung jawab; dan

e. memberikan rasa aman, keadilan dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi.

Melihat rumusan dari Pasal 4 di atas, pemanfaatan teknologi informasi dan transaksi elektronik yang dilakukan oleh orang-orang yang menguasai teknologi sudali tidak sesuai lagi dengan apa yang menjadi harapan dari UU Informasi dan Transaksi Elektronik sebagaimana yang tercantum dalam tujuannya. Kejahatan siber (*cyber crime*) sudah merambah ke seluruh aspek kehidupan masyarakat. Teknologi informasi saat ini menjadi pedang bennata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus juga menjadi sarana efektif perbuatan melawan hukum.

Bank adalah bagian clan sistem keuangan dari sistem pembayaran suatu negara, bahkan pada era globalisasi sekarang ini, bank juga telah menjadi bagian dari sistem keuangan dan sistem pembayaran dunia. Mengingat hai yang demikian itu, maka begitu suatu bank telah memperoleh izin berdiri dan beroperasi dari otoritas moneter negara yang bersangkutan, bank tersebut telah menjadi milik masyarakat. Oleh karena itu, eksistensinya bukan saja harus dijaga oleh para pemilik bank itu sendiri, tetapi juga oleh masyarakat nasional dan global.

Bank sebagai bagian dari sistem keuangan dari sistem pembayaran suatu negara tidak terlepas dari tindakan kejahatan. Sudah banyak korban berjatuhan akibat kurang memahami resiko yang mengancam. Tindak kejahatan di sektor jasa keuangan secara umum terbagi atas 2 jenis yaitu *skimming* dan *social engineering. Skimming* merupakan salali satu bentuk yang banyak teijadi dimana merupakan suatu tindakan pencurian informasi dengan cara menyalin informasi yang terdapat pada strip magnetik kartu debit atau kartu kredit secara illegai.

Disadari bahwa perkembangan internet yang begitu cepat berbanding lurus dengan modus kejahatan yang muncul. Beberapa tahun yang lalu, puluhan ribu pemakai internet terkena virus e-mail '*melissa*' dan '*explore.zip.worm*' yang menyebar dengan cepat, menghapuskan arsip-arsip, menghapuskan sistem-sistem, dan menyebabkan perusahaan-perusaliaan harus mengeluarkan jutaan dolar untuk mendapatkan bantuan dan batas waktu.[11]

Banyak aksi kejahatan siber yang masih terjadi, bahkan pemah menimpa salah satu *e-commerce* terbesar di Indonesia, dimana pelaku meretas server [6 7] perusahaan tersebut, dan berhasil mencatat jutaan data pelanggan. Mulai nama, nomor handphone, hingga alamat. Semua data tersebut bisa saja diperjualbelikan demi keuntungan pelaku. " Kasus yang lain, tiga pelaku *cyber crime* jaringan intemasional, asai Nigeria yakni Igue Chuku Augustin, Ohak Guherbert dan mahasiswa Universitas Paramita, Karawaci, Devi Imasari tertangkap di Kompleks Villa Serpong Blok D No. 10, RT 50/10, Jalan Purimoro III, Jelupang, Kota Tangerang Selatan. Dalam melakukan aksinya, mereka melakukan penipuan melalui internet dengan menawarkan macam-macam barang dan jasa, seperti handphone, laptop dan barang yang lebih besar seperti kamera, barang sudah dibayar oleh pembeli namun barang tidak pemah sampai ke tangan konsumen. Dalam melakukan aksinya mereka menggunakan akun sosial Facebook dan jejaring sosial lainnya yang tersedia di internet.[1^] Berdasarkan hal-hal yang disebutkan di atas, penulis tertarik untuk melakukan penelitian kepustakaan tentang kejahatan siber dan membahasnya kemudian menuangkannya dalam suatu bentuk penulisan hukum untuk akademisi yaitu skripsi dengan judul "Tindak Pidana Cyber Crime dalam Kegiatan Perbankan".

B. Rumusan Masalah

1. Bagaimana bentuk-bentuk kejahatan yang termasuk sebagai kejahatan di bidang siber?
2. Bagaimana Penerapan Hukum Pidana Terhadap Pelaku Kejahatan Siber di Sektor Jasa Keuangan dan Perbankan?

C. Metode Penelitian

Jenis penelitian ini adalah penelitian deskriptif. Adapun metode pendekatan yang digunakan adalah yuridis normatif, artinya

[11] William Wiebe, *Tindak Kejahatan Melalui Komputer,* Seminar, Makassar, 2000, hlm. 13

pembahasan terhadap masalah yang ada, peneliti akan melihat pada ketentuan peraturan perundang- undangan yang ada kaitannya.

PEMBAHASAN

A. Bentuk-Bentuk Kejahatan Cyber Dikaikan Dengan Bank

Kejahatan siber atau *cyber crime* adalah tindak kejahatan yang dilakukan secara *online.* Kejahatan ini tidak mengenal waktu dan tidak pilih-pilih target. Bisa terjadi pada individu atau perusahaan dimanapun berada. Tujuan kejahatan siber sendiri beragam. Bisa sekedar iseng, sampai kejahatan serius yang merugikan korbannya secara finansial. Pada praktiknya, kejahatan dunia maya bisa dilakukan seorang diri atau sekelompok orang. Para pelaku kejahatan dunia maya tentu adalah orang yang sudah ahli dalam berbagai teknik peretasan. Bahkan tidak jarang sebuah aksi kejahatan siber *{cyber crime*) dilakukan dari berbagai tempat berbeda di waktu bersamaan.

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan Teknologi Informasi yang berbasis utama komputer dan jaringan telekomunikasi ini, dalam beberapa literatur dan praktiknya dikelompokan dalam beberapa bentuk, antara lain ;

1. *Unauthorized Acces to Computer System and Service*
   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.
2. *Illegal Contents*
   Merupakan kejahatan dengan memasukan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat diaangapmelanggar hukum atau mengganggu ketertiban umum.
3. *Data Forgery*
   Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless 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 Extotion*
   Kejahatan ini dilakukan dengan membuat gangguan, perusakan aytau penghancuran terhadap suatu data, program komputer atau sistemjaringan komputer yang terhubung dengan Internet.
6. *Offense Against Intellectual Property*
   Kejahatan ini ditujukan terhadap hak atas kekayaan intelekutal yang dimiliki oleh pihak lain di Internet. Sebagai contoh adalah penipuan 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. *Ingrigements of Privacy*
   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara *computerized* , yang apabila diketahui oleh orang lain akan dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor pin atm, cacat atau penyakit tersembunyi dan sebagainya.[8]

Bentuk-bentuk kejahatan cyber seperti di atas tentu berhubungan atau memiliki kaitan dengan perbankan dimana hampir semua perusahaan ataupun badan hukum perdata di dunia ini menerapkan sistem komputerisasi untuk memp[ermudah pekerjaan dan juga membantu pada sisytem penyimpanan data.

UU No. 11 Tahun 2008 yang dirubah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, tidak memberikan defmisi tentang kejahatan siber *(cybercrime),* tetapi membaginya menjadi beberapa pengelompokkan yang mengacu pada

[8] *Op.Cit*, Dikdik Arief Mansur dan Elisatris Gultom, Hlm 10.

Convention on Cybercrime sebagai berikut:[9]

1. Tindak Pidana yang berhubungan dengan aktivitas *illegal,* yaitu:
   a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten *illegal*, yang terdiri dari:
      - kesusilaan {Pasal 27 ayat (1)};
      - perjudian {Pasal 27 ayat (2)};
      - penghinaan dan/atau pencemaran nama baik {Pasal 27 ayat (3)};
      - pemerasan dan/atau pengancaman {Pasal 27 ayat (4)};
      - berita bohong yang menyesatkan dan merugikan konsumen {Pasal 28 ayat(1)};
        menimbulkan rasa kebencian berdasarkan SARA {Pasal 28 ayat (2)}; mengirimkan informasi yang berisi ancaman kekerasan atau menakut- nakuti yang ditujukan secara pribadi {Pasal 29}.

   b. Dengan cara apapun melakukan akses *illegai* {Pasal 30}.
   c. Intersepsi atau penyadapan *illegal* terhadap informasi atau dokumen elektronik dan sistem elektronik {Pasal 31}.
2. Tindak pidana yang berhubungan dengan gangguan (*interferensi*), yaitu:
   a. Gangguan terhadap informasi atau dokumen elektronik *{data interference*
      - Pasal 32)

   b. Gangguan terhadap sistem elektronik *(system interference* - Pasal 33).
3. Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34).
4. Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35).
5. Tindak pidana tambahan *{accessoir* Pasal 36).

[9] Josua Sitompul, *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*, PT Tatanusa, 2012.

6. Pemberatan-pemberatan terhadap ancaman pidana (Pasal 52).

B. Penerapan Hukum Pidana Terhadap Pelaku Kejahatan Siber di Sektor Jasa Keuangan dan Perbankan

Bentuk-bentuk kejahatan siber (*cybercrime*) di Indonesia dapat dikaitkan dengan ketentuan hukum pidana Indonesia, baik ketentuan KUHP maupun ketentuan pidana dalam peraturan perundang-undangan di luar KUHP yaitu UU No. 11 Tahun 2008 Jo UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Meskipun demikian, ada perbedaan konsepsi antara hukum pidana Indonesia dengan karakteristik kejahatan siber (*cybercrime*). Beberapa tekninologi KUHP sulit digunakan sebagai dasar hukum untuk mengadili kejahatan siber *{cybercrime),* misalnya pengertian 'di depan umum yang disamakan dengan pengertian 'di dalam internet', pengertian 'memasuki pekarangan tertutup' sebagaimana diatur dalam KUHP untuk mengadili kasus 'memasuki ruang *{spacey* milik pihak lain di internet *{illegal access).*

Tindak kejahatan siber *(cybercrime)* di sektor jasa keuangan dan perbankan secara umum terbagi atas dua (2) jenis yakni[10]:

1. *Sosial engineering,* adalah manipulasi psikologis seseorang dengan tujuan untuk mendapatkan informasi tertentu dengan cara menipu secara halus, baik disadari atau tidak melalui telepon atau berbicara langsung.
2. *Skimming,* adalah tindakan pencurian informasi dengan cara menyalin informasi yang terdapat pada strip magnetik kartu debit atau kredit secara *illegal.* Metode *skimming* merupakan metode yang digunakan untuk mencuri informasi nasabali pada saat bertransaksi menggunakan ATM. " Dalam menjalankan tindak kejahatan ini terdapat tiga (3) alat utama yang digunakan yaitu: *skimmer, hidden camera* dan *keypad.* Alat *skimmer* berfungsi untuk merekam aktivitas nasabah dalam menggunakan mesin ATM, alat ini mampu merekam strip elektromagnetik yang ada pada kartu korban pada saat kartu dimasukkan ke mesin ATM. *Hidden camera* dan *keypad* digunakan untuk merekam aktivitas korban pada saat melakukan penginputan PIN pada mesin ATM.

Adapun teknik dasar memperoleh informasi dengan modus *social engineering* bermacam-macam, ada tiga (3) yang paling lumrah yakni:

1. *Phishing,* teknik *phising* digunakan para pelaku dengan mengelabui atau memanipulasi para pemilik rekening bank sehingga mereka memberikan data dan informasi yang bisa digunakan untuk mengakses akun perbankan milik nasabah.[11] Pengelabuan yang dilakukan untuk mendapatkan informasi rahasia seperti *password* dengan menyamar sebagai orang atau bisnis terpercaya dalam sebuah komunikasi elektronik. Saluran yang digunakan sebagai *email*, layanan pesan instan (SMS), atau penyebaran link palsu di internet untuk mengarahkan korban ke *website* yang telah dirancang untuk menipu.[12]
2. *Vishing,* yakni upaya penipu melakukan pendekatan terhadap korban untuk mendapatkan informai atau mempengaruhi korban untuk melakukan tindakan. Biasanya komunikasi dilakukan melalui telepon.
3. *Impersonation,* yakni upaya penipu berpura-pura menjadi orang lain dengan tujuan untuk mendapatkan informasi rahasia.

Adapun modus *social engineering* yang sering dilakukan penipu di antaranya:

1. *Fraud internet banking* dan transaksi *online* menggunakan kartu kredit/kartu debit, yakni pelaku mengaku sebagai pegawai bank yang menginformasikan adanya perubahan biaya layanan SMS/intemet banking, pemberian bonus

[10] Farodilah Muqoddam, *Mengenal Modus Kejahatan Keuangan, Definisi Skimming, Phishing dan Vishing,* 2019. diakses darim.bisnis.com pada tanggal 2 Oktober 2020.

[11] *Wasapadaì Modus Operandi Kejahatan Siber Perbankan*, 2019, diakses dari dialogpublik.com pada tanggal 31 Oktober 2020

[12] Farodilah Muqoddam, *Loc-Cit.*

pulsa, pembagian hadiah undangan, dan lain- lain. Pelaku juga melakukan penipuan penawaran pinjaman *online* dengan bunga murah.

2. *Contact center bank,* yakni penipu memanipulasi mesin ATM agar korban gagal bertransaksi dan kartu tertelan di mesin. Pada saat bersamaan, anggota tim penipu *standby* disekitar ATM untuk mengarahkan korban menghubungi nomor *cali center* palsu. Tim yang berpura-pura menjadi *cali centre* palsu memberitahukan bahwa ATM telah diblokir, kemudian meminta korban memberikan identitas pribadi termasuk nomor PIN ATM. Pelaku yang berada disekitar korban kemudian mengambil kartu ATM milik korban yang tertelan di mesin.
3. *Fraud* SMS penipuan, korban menerima konten SMS yang berisi iming-iming hadiah, diskon, bonus pulsa, paket tour wisata, pinjaman *online* dan lainnya. Dengan dalih mencairkan hadiah, korban akan dipancing ke mesin ATM dan diarahkan untuk mengikuti instruksi yang diberikan pelaku seperti melakukan transfer dana atau *top-up* saldo *e-commerce.*

Selain apa yang sudah disebutkan di atas, bentuk-bentuk kejahatan siber di sektor jasa keuangan dan perbankan, masih ada bentuk yang lain yakni:

1. Pencurian identitas nasabah, bisa dilakukan melalui aplikasi apa saja. Salali satu sasaran pencurian adalah melalui *open banking. Open banking* adalah sistem penyedia jasa interaksi antara nasabah dengan lembaga keuangan.

   Sistem ini bisa dibaca oleh pelaku pencurian dengan *'Jamming'* atau menyadap data profil nasabah.
2. *Skimming,* teknik ini dilakukan pelaku dengan cara mengkloning kartu ATM milik nasabah ke dalam kartu ATM kosong. Caranya, para pelaku memasang *wifi pocket oruter* disertai kamera yang dimodifikasi menyerupai penutup PESI pada mesin-mesin ATM untuk mencuri PIN nasabah sebelum kemudian diduplikasi.
3. *Malware,* merupakan singkatan dari *malicious software,* yang artinya *software* yang tidak diinginkan dalam sistem komputer.[13] *Malware* dapat mencakup dari semua perangkat lunak yang digunakan untuk mengukur, memanipulasi atau bahkan memata-matai sebuah sistem. *Malware* merupakan istilah yang digunakan untuk mendeskripsikan perangkat lunak berbahaya. *Malware* dapat disebarkan melalui beberapa metode. Sebagian besar adalah melalui jaringan internet, *email*, pesan pribadi, atau halaman situs *web Malware* sangat sulit untuk dideteksi oleh sistem komputer. Karena ada dua (2) jalur yang menyebabkan sistem komputer terkena oleh *malware* yaitu melalui *USB Drive* dan melalui jaringan internet. Sampai sekarang ini malware masih menjadi ancaman serius bagi dunia maya secara global.
4. *Hacking,* adalah istilah kejahatan siber yang cukup umum. Aksi ini dilakukan dengan cara mengakses sistem komputer korban tanpa hak. Para *hacker* akan menggunakan keterampilan yang dimiliki untuk melakukan berbagai aksi kejahatan publik. Aksi *hacking* tidak selamanya bertujuan mendapatkan Keuntungan finansial. Banyak juga *hacker* yang hanya sekedar untuk memamerkan keahlian yang dimiliki. Contohnya, aksi *hacking* yang kerap teijadi adalah pembobolan kata sandi. Langkah inilah yang menjadi titik awal *hacker* melakukan kejahatan selanjutnya. Beberapa waktu yang lalu, dua media besar di Indonesia pemah menjadi korban *hacking.* Para *hacker* berhasil menembus sistem keamanan situs *web* media tersebut dan berhasil membuat beberapa berita yang pemah dimuat.

Melihat pada bentuk-bentuk kejahatan siber di sektor jasa keuangan dan perbankan di atas, maka ada 3 bentuk kejahatan siber yang penerapan hukumnya dilakukan dengan Kitab Undang-Undang Hukum Pidana, yaitu: [14] 1. Kasus *Unauthorized Transfer Payment* di Bank Negara Indonesia (BNI) cabang New York *Agency* (Tahun 1986).

---

[13] Kumiawan A and Prayudi. Y, *Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics, Hadfex (Hacking and Digital Forensics Exposed),* 2014, hlm. 4-5.

[14] Widodo, *Op-Cit,* hlm. 95 - 96.

Dalam kasus ini, Pengadilan Jakarta menjatuhkan pidana terhadap terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 ayat (1) huruf d KUHP, yaitu pencurian yang dilakukan oleh lebih dari dua (2) orang secara bersama-sama. Putusan tersebut dikuatkan oleh Putusan

Pengadilan Tinggi Jakarta dan Putusan Mahkamah Agung Republik Indonesia.

Ketentuan Pasal 363 ayat (1) KUHP berbunyi sebagai berikut:

Diancam dengan pidana penjara paling lama tujuh tahun: huruf d. pencurian yang dilakukan oleh dua orang atau lebih.

Dalam kasus ini, memindahkan data komputer ke tempat lain dapat dikategorikan dalam pengertian 'mengambik sebagaimana dimaksud KUHP, meskipun data komputer yang dipindahkan tidak mengakibatkan hilangnya data asli.

Dalam kasus-kasus lain, juga teijadi penafisran ekstensif, penafsiran yang memperluas arti, yaitu terhadap penegrtian 'rumah, ruangan, pekarangan tertutup', sehingga perbuatan seseorang dalam memasuki program komputer yang dioperasikan dalam suatu jaringan dapat dikategorikan sebagai perbuatan memaksa memasuki rumah atau ruangan, atau pekarangan tertutup secara melawan hukum sebagaimana diatur dalam KUHP.

2. Kasus Penarikan Hasil Setoran Warkat Fiktif di PT Bak Vali Jakarta (Tahun 1989)

Dalam kasus ini, Pengadilan Negeri Jakarta Barat menjatuhkan pidana penjara kepada terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 362 KUHP, yaitu pencurian biasa.Ketentuan Pasal 362 KUHP berbunyi sebagai berikut:

Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah.

Dalam mengadili perkara ini, hakim melakukan penafsiran ekstensif terhadap penegertian 'mengambil' dan 'barang'.

3. Kasus Manipulasi Data Saldo pada *Master File* Bank Danamon Cabang Glodog Plaza (Tahun 1990)

Pengadilan Negeri Jakarta Barat menjatuhkan pidana penjara kepada terdakwa karea terdakwa secara sah dan meyakinkan melanggar Pasal 363 ayat (1) huruf e KUHP, *juncto* Pasal 64 ayat (1) KUHP, yaitu melakukan pencurian dalam keadaan memberatkan yang dilakukan berulang kali sebagai perbuatan berlanjut. Putusan tersebut dikuatkan oleh putusan Pengadilan

Tinggi dan Putusan Mahkamah Agung.

Dalam kasus ini, pengertian 'kunci palsu' ditafsirkan secara ekstensif, sehingga kode akses *{password)* dapat dikategorikan dalam pengertian kunci palsu sebagaimana diatur dalam KUHP.

Selain pasal-pasal dalam KUHP yang disebutkan di atas, maka penerapan hukum terhadap pelaku kejahatan siber di sektor jasa keuangan dan perbankan adalah juga sebagaimana yang diatur dalam Pasal 378 dan Pasal 362 (tentang kasus *Carding* karena pelaku melakukan penipuan seolah-olah ingin membayar, dengan kartu kredit hasil curian[15]). *Carding* menurut versi POLRI meliputi:

1. mendapatkan nomor kartu kredit (CC) dari tamu hotel, khususnya orang asing.
2. mendapatkan nomor kartu kredit melalui kegiatan chatting di internet.
3. melakukan pemesanan barang ke perusahaan di luar negeri dengan menggunakan jasa internet.
4. mengambil dan memanipulasi data di internet.
5. memberikan keterangan palsu, baik pada waktu pemesanan maupun pada saat pengambilan barang di Jasa Pengiriman.

Carding (pelakunya biasa disebut *carder*) adalah kegiatan melakukan transaksi *e-commerce* dengan nomor kartu kredit palsu atau curian.

PENUTUP

A. Kesimpulan

1. Kejahatan siber (*cyber crime)* dilakukan oleh orang baik secara sendiri maupun berkelompok yang benar-benar ahli dalam peretasan, alili dalam menggunakan komputer sebagai sarana/alat untuk melakukan kejahatan,

[15] Widyopramono, *Kejhatan di Bidang 1Computer*, Pustaka Sinar Harapan,1994, hlm. 67.

sehingga menurut para ahli bentuk-bentuk kejahatan siber (*cyber crime*) itu secara umum adalah berupa pencurian identitas, *spionage cyber,* pemerasan *cyber,* pencurian data perusahaan, dan *carding.* Sedangkan menurut UU No. 11 Tahun 2008 yang dirobah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, bentuk-bentuk kejahatan siber (*cyber crime*) adalah tindak pidana yang berhubungan dengan aktivitas *illegal*, tindak pidana yang berhubungan dengan gangguan (interferens), tindak pidana memfasilitasi perbuatan yang dilarang, dan tindak pidana pemalsuan informasi atau dokumen elektronik.

2. Tindak kejahatan siber *(cyber crime)* di sektor jasa keuangan dan perbankan adalah *social engineering* dan *skimming.* Kedua bentuk kejahatan siber ini dilakukan dengan teknik menipu atau penipuan, penggelapan dan pencurian. Oleh karena itu penerapan hukum pidana terhadap para pelaku kejahatan siber di sektor jasa keuangan dan perbankan itu oleh para hakim banyak menggunakan pasal-pasal yang ada dalam KUHP yaitu Pasal 64 tentang perbuatan berlanjut, karena pelaku melakukannya berkali-kali, Pasal 362 tentang Pencurian, Pasal 363, pencurian yang dilakukan oleh lebih dari satu orang dan Pasal 378 tentang penggelapan.

B. Saran

1. *Cybercrime* merupakan suatu kejahatan modern dimana perbuatan ini merupakan hasil dari lemajuan di bidang teknologi sehingga seluruh dunia menggunakan prinsip serba komputerisasi dan disitulah celah kejahatan yang bisa muncul kapan saja hampir tanpa terdeteksi. Untuk mencegah bahkan melakukan penanganan apabila kejahatan cyber terus terjadi maka disini peran pemerintah untuk membendung dan melakukan penegakan hukum lewat alat-alat negara seperti kepolisian, kejaksaan, bahkan badan intelejen pada institusi pemerintah baik itu Badan Intelejen Negara (BIN) maupun yang ada pada TNI-POLRI berkolaborasi dengan Kementerian Komunikasi dan Informasi untuk membatasi dan memantau perkembangan teknologi yang dalam hal ini adalah informatika dengan menutup akses-akses yang dicurigai dapat menimbulkan suatu tindak pidana. Tentunya pekerjaan ini tidaklah mudah dibutuhkan tenaga yang ahli yang mampu melakukan hal ini yang pada intinya Sumber Daya Manusia (SDM) yang bertanggungjawab memantau bahkan melakukan penegakan hukum pada *cybercrime* diberikan pelatihan serta menyiapkan komponen-komponen tercanggih dan mutakhir sehingga dapat dengan mudah memantau *network and netsocial*.
2. Tindak kejahatan siber disektor jasa keuangan dan perbankan semakin sering terjadi dan sangat merugikan nasabah, oleh karenanya para pelaku kejahatan siber harus mendapat hukuman yang berat agar mereka menjadi jera untuk melakukannya lagi. Dalam peraturan perundang-undangan harus dengan tegas untuk mengatur ancaman hukuman yang berat.

DAFTAR PUSTAKA

Arief Barda Nawawi , *Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2002

A Kumiawan and Prayudi. Y, *Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics, Hadfex (Hacking and Digital Forensics Exposed),* 2014.

Didik Arief Mansur dan Elisatris Gultom, *Cyber* Law, Refika Aditama, Bandung, 2005

I Wayan Parthiana, *Ekstradisi dalam Hukum Internasional dan Hukum Nasional Indonesia*, Mandar Maju, Bandung, 1990,

Judhariksawan, *Pengantar Hukum Telekomunikasi,* Rajawali Press, Jakarta, 2005.

Kartanagara, Satochid*Hukum Pidana II, Delik-Delik Khusus,* Baiai Lektur Mahasiswa, Jakarta, Tanpa Thn.

Kusumah Mulyana. W, *Kejahatan, Penjahat dan Reaksi Sosial,* Akumni, Bandung, 1983

Maskun, *Kejahatan Siber (Cyber crime) Suatu Pengantar,* Kencana, Prenata Media Group, Jakarta, 2013

Prodjodikoro Wiijono, *Tindak-Tindak Pidana Tertentu di Indonesia*, RefikaAditama, Bandung

Rahaijo Agus, *Cyber Crime; Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* Citra aditya Bakti, Jakarta, 2006.

Safitri Indra, *Tindak Pidana di Dunia Cyber, Insider, Legai Journal From Indonesian Capital and Investment Market*, diakses hhtp://business.fortunecity.com pada tanggal 27 Oktober 2020.

Sitompul Josua, *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*, PT. Tatanusa

Soekanto Soeijono dan Sri Mamudji, *Penelitian Hukum Normatif; Suatu Tinjauan Singkat,* PT Raja Grafindo Persada, Jakarta, 2003.

T Arifianto, *Penerapan Fingerprint Recognition Dengan Metode Learning Vector Quantization (LVO) dalam Automatic Teller Machine (ATM),* Jumal SPIRIT, 2018

Wahid Abdul dan Moh, Labib, *Kejahatan Mayantara (Cyber Crime),* Refika Aditama, Jakarta, 2005.

Widyopramono Hadi Widjojo, *Cybercrimes dan Pencegahannnya,* Jumal Hukum Teknologi, Fakultas Hukum Universitas Indonesia, Jakarta, 2005

William Wiebe, *Tindak Kejahatan Melalui Komputer,* Seminar, Makassar, 2000.

Widodo, *Hukum Pidana di Bidang Teknologi Informasi; Cybercrime Law: Telaah Teoritik dan Bedah Kasus,* Aswaja Pressindo, Yogyakarta, 2011

Wisnubroto Aloysius, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Universitas Atmajaya, Yogaykarta, 1999

Widyopramono, *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan,1994.

Peraturan Perundang-Undangan

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang dirobah dengan UU No. 19 Tahun 2016.

Sumber Internet

Azizah Reftika Wulandari, *Mengulik Kiat Bank Atasi Kejahatan Siber,* diakses dari lokadata.id pada tanggal 31 Oktober 2020.

Ferdinand Wisnu, *Pengertian, Jenis dan Fungsi Bank*, diakses pada tanggal 20 Oktober 2020.

Farodilah Muqoddam, *Mengenal Modus Kejahatan Keuangan, Definisi Skimming, Phishing dan Vishing,* 2019, diakses darim.bisnis.com pada tanggal 2 Oktober 2020.

Gema Ari Juliano, *Cyber crime: Sebuah Fenomena di Dunia Maya*, diakses dari www.theceli.com pada tanggal 27 Oktober 2020.

Teguh Arifiyadi, *Menjerat Pelaku Cyber Crime dengan KUHP*, Pusat DataDepartemen Komunikasi dan Informatika, 2008, diakses dari depkominfo.go.id pada tanggal 2 November 2020.

Apa itu malware? Pengertian dan Cara Mengatasinya, diakses dari www.niagalioster.co.id pada tanggal 2 Oktober 2020.*Kompas,* 11 Agustus 1999.

Mengenal Cyber Crime, Kejahatan Online Yang Wajib Diwaspadai, diakses dari www.niagahoster.com pada tanggal 24 Oktober 2020

Mengenal Lembaga Keuangan Non Bank Yang Ada di Indonesia, diakses dari accurate.id pada tanggal 25 Oktober 2020.

SK Mentori Keuangan No. 38/MKJIV/1972 tentang Lembaga Keuangan Bukan Bank.

Waspadai Modus Operandi Kejahatan Siber Perbankan, 2019, diakses dari dialogpublik.com pada tanggal 31 Oktober 202