BAB III

PENCURIAN DANA NASABAH BANK MELALUI MEDIA INTERNET

A. Pihak-Pihak yang Terkait dalam Kasus Pencurian Dana Nasabah Bank melalui Internet

Kecanggihan teknologi komputer telah memberikan kemudahan-kemudahan, terutama dalam membantu pekerjaan manusia. Perkembangan teknologi komputer menyebabkan munculnya jenis kejahatan-kejahatan baru, yaitu dengan memanfaatkan komputer sebagai modus operandi. Penyalahgunaan komputer dalam perkembangannya menimbulkan permasalahan yang sangat rumit, diantaranya proses pembuktian atas suatu tindak pidana (faktor yuridis). Terlebih lagi penggunaan komputer untuk tindak pidana ini memiliki karakter tersendiri atau berbeda dengan tindak pidana yang dilakukan tanpa menggunakan komputer. Perbuatan atau tindakan, pelaku, alat bukti dalam tindak pidana biasa dapat dengan mudah diidentifikasi namun tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer[34].

Banyaknya penyedia internet dan semakin terjangkaunya biaya akses internet membuat semakin banyak orang mulai mengenal internet dan menggunakannya. Hal tersebut membuat para pencuri melakukan aksi *carding database* dengan memanfaatkan kesadaran masyarakat dalam hal ini nasabah bank yang masih kurang mengerti akan dampak negatif dari internet serta ke

[34] M Ahmad , Ramli , *Cyber Law dan Haki dalam Sistem Hukum Indonesia*, Refika Aditama , Bandung , 2006, Hlm 19.

tidak sempurnaan kebijakan-kebijakan pemerintah dalam hal tersebut. *Carding database* adalah pencurian data nasabah berupa nomor rekening dan identitas nasabah melalui *database* bank tersebut, sehingga pelaku akan mendapatkan informasi tentang nasabah yang terkait untuk dijadikan target pencurian, sedangkan pelakunya disebut *carder*. Contoh *carding database* yang sering kita jumpai adalah surat konfirmasi *situs* bank kepada nasabah melalui *email*, konfirmasi hadiah undian dari bank bersangkutan dengan menggunakan telepon, dan lain lain.

Pihak-pihak yang terkait dalam kasus pencurian dana nasabah bank melalui internet yaitu :

1. *Carder*

   Carder adalah pelaku dari *carding database*. *Carder* menggunakan *e-mail*, *banner* atau *pop-up window* untuk menipu *netter* ke suatu situs *web* palsu, dimana *netter* diminta untuk memberikan informasi pribadinya[35]. Teknik umum yang sering digunakan oleh para *carder* dalam aksi pencurian adalah membuat situs atau *e-mail* palsu atau disebut juga *phising* dengan tujuan memperoleh informasi nasabah seperti nomor rekening, PIN (*Personal Identification Number)*, atau *password*. Pelaku kemudian melakukan konfigurasi PIN atau *password* setelah memperoleh informasi dari nasabah, sehingga dapat mengambil dana dari nasabah tersebut[36].

[35] *Ibid*.
[36] Iwan Aditama, *Mengenal Istilah Carding*, http://iwan.or.id, Diakses Pada Tanggal 15 Maret 2010, Pukul 15:30 WIB

Target *carder* yaitu pengguna layanan *internet banking atau* situs-situs iklan, jejaring sosial, *online shopping* dan sejenisnya yang ceroboh dan tidak teliti dalam melakukan transaksi secara *online* melalui situs internet. *Carder* mengirimkan sejumlah *email* ke target sasaran dengan tujuan untuk meng *up-date* atau mengubah *user ID* dan PIN nasabah melalui internet. *E-mail* tersebut terlihat seperti dikirim dari pihak resmi, sehingga nasabah seringkali tidak menyadari kalau sebenarnya sedang ditipu.

Pelaku *carding database* mempergunakan fasilitas internet dalam mengembangkan teknologi informasi tersebut dengan tujuan yaitu menimbulkan rusaknya lalulintas mayantara (*cyberspace*) demi terwujudnya tujuan tertentu antara lain keuntungan pelaku dengan merugikan orang lain disamping yang membuat, atau pun menerima informasi tersebut.

2. *Netter*

   Netter adalah pengguna internet, dalam hal ini adalah penerima *e-mail* (nasabah sebuah bank) yang dikirimkan oleh para *carder*.

3. *Cracker*

   Cracker adalah sebutan untuk orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang dimasuki seperti pencurian data, penghapusan, penipuan, dan banyak yang lainnya.

4. Bank

   Bank adalah badan hukum yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkan kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak[37].

   Bank juga merupakan pihak yang menerbitkan kartu kredit/debit, dan sebagai pihak penyelenggara mengenai transaksi *online*, *e-commerce*, *internet banking*, dan lain-lain.

Banyak cara yang ditempuh oleh para pelaku *carding database* untuk menjerat korbannya, antara lain melalui[38]:

a. Faktor Pendekatan Sosial

   Kebanyakan para korban diberikan suatu *e-mail* palsu dan dituntun ke dalam jebakan dengan tujuan agar korban mau melakukan beberapa tindak lanjut dari *e-mail* palsu tersebut sehingga korban mau memberikan informasi data pribadi, *user ID* atau PIN kepada *carder*.

b. Pengiriman Pesan

   Carder mengirimkan pesan melalui *e-mail spam*, *web-based delivery*, iklan jebakan dalam *web*, IRC dan *Instant Messaging* (*Yahoo Messenger*, MSN *Messenger*, AOL, ICQ dan lain-lain), dapat pula calon korban diajak untuk menuju situs buatan para *carder* yang mengandung trojan, jadi saat korban membuka

[37] Malayu Hasibuan, *Pengertian Bank,* hizkiarahwikoadi.blogspot.com, Di Akses Pada Tanggal 20 Mei 2010, Jam 15.00 WIB

[38] N.N, *Modus Carder*, http://buletin.melsa.net , Diakses Pada Tanggal 11 Mei 2010, Pukul 16:55 WIB

situs jebakan, secara tidak sadar terjadi proses infeksi sistem oleh trojan.

B. Kasus Pencurian Dana Nasabah Bank melalui Internet.

1. Kasus Nasabah Bank Mandiri

Pencurian dana nasabah bank melalui internet terjadi pada bulan Desember 2008 di Purwokerto. Seorang nasabah bank Mandiri pengguna fasilitas *internet banking*, kehilangan uang sebesar Rp. 38 Juta yang dicuri oleh seseorang yang menggunakan teknologi internet. Korban yang bernama Johannes mengatakan telah kehilangan uang Rp 38 Juta yang diambil hampir tiap hari oleh pencuri tersebut. Johannes sebelumnya menerima sebuah *e-mail* dari situs internet banking mandiri yang isinya diharuskan mengaktifkan kembali *user ID* dan PIN yang sebelumnya telah dinonaktifkan. Hasil rekening koran yang dikeluarkan oleh pihak bank, *carder mentransfer* uang hasil curiannya sebesar Rp. 21 Juta ke rekening tabungannya, selain itu *carder* juga memakai uang hasil curiannya untuk berbelanja pulsa telepon seluler Pro XL, sebanyak Rp 17 Juta. Pembelian pulsa dilakukan melalui internet, dan *carder* kemudian mengambil nomor-nomor seri hasil pembelian untuk selanjutnya diisikan ke *handphone*nya.

Isi *e-mail* yang diterima oleh Johannes pada saat itu :

From internet banking
To : berxxxxxxx@telkom.net
Sent : Tuesday, Desember 23, 2008 5:27 AM
Subject: confirmation your identity

The user of Internet Banking Mandiri, please re-confirm your identity. Because your account was not actived with our system. some body has try login to your account but not successed. But our Auto-boot responbility as crime cyber. please re-confirm your account with current identity.
click here (http://searex.no/includes/javaboot/mandiri/online/Login.do.html) to confirm
Hopefully this information help you.
Thank you.

Best Regards,

Bank Mandiri

Berdasarkan *e-mail* di atas dapat dijelaskan bahwa *carder* mengirimkan *e-mail* kepada nasabah untuk mengaktifkan kembali *user ID* dan PIN yang sebelumnya telah dinonaktifkan, kemudian menyertakan *link* untuk membuka halaman perubahan yang seolah-olah halaman *web internet banking* Mandiri sebenarnya. Penggunaan link tersebut sebenarnya tidak ada kaitannya dengan link *internet banking* yang asli[39].

2. Kasus Nasabah Bank BNI

Pencurian dana nasabah bank melalui internet juga terjadi pada bulan November 2006 di Jakarta. Nasabah *Internet banking* Bank Negara Indonesia (BNI) bernama Rony Hermansyah kehilangan uangnya sebesar Rp. 9 juta oleh seseorang dengan menggunakan fasilitas internet. Rony sebelumnya mendapatkan *e-mail* yang mengatasnamakan BNI. *E-mail*

[39] N.N, http://web.bisnis.com, edisicetakharianteknologiinformasi655687.html, Diakses Pada Tanggal 10 April 2010 pukul 23:00 WIB

tersebut di dalamnya terdapat sebuah *link* dengan alamat https://ibank.bni.co.id/directRetail/ibank, untuk konfirmasi identitas pelanggan BNI Internet Banking. *Link* tersebut membawa Ivo ke sebuah halaman situs *verifikasi login* ke BNI *Internet Banking* yang sama persis dengan halaman *login* milik BNI. Carder memakai uang hasil curiannya untuk berbelanja melalui *shopping online* dan sebagian uangnya lagi di *transfer* ke rekening tabungannya[40].

Berdasarkan kasus-kasus di atas, dapat dijelaskan kronologis mengenai pencurian dana nasabah melalui internet dengan *modus carding database* yaitu sebagai berikut :

a. *E-mail* biasanya dikirim secara acak ke beberapa orang sekaligus, jadi biasanya tidak mencantumkan nama nasabah secara spesifik.
b. *E-mail* tersebut biasanya meminta nasabah untuk memperbaharui informasi pribadi atau mengkonfirmasi status rekening nasabah.
c. *E-mail* tersebut dapat juga memperingatkan bahwa rekening nasabah akan ditutup bila tidak segera melakukan hal yang diminta.
d. Umumnya tercantum alamat URL ke *website* palsu

Carder mengaku sebagai pihak bank, sehingga *carder* dapat meyakinkan korbannya sampai 5% dari penerima *e-mail* untuk mengikuti perintahnya. Pada isi *e-mail*, *carder* memberitahukan tentang perlunya

[40]N.N, http://buletin.melsa.net.idjan1001phishing7.html, Diakses Pada Tanggal 16 Juli 2010, Pukul 21:35 WIB

verifikasi *user ID dan PIN* dengan cara mengklik *link* URL pada *e-mail* dan mengirimkannya dengan alasan agar *account*-nya dapat dipergunakan kembali dan ter-*update*, setelah *carder* berhasil mendapatkan *user ID dan PIN*, lalu *carder* dapat menggunakannya untuk berbelanja atau meminjam identitas kita[41].

C. Akibat yang Timbul dari Tindak Pidana Pencurian Dana Nasabah melalui Internet.

Kejahatan mayantara (*cyber crime*) merupakan salah satu bentuk kejahatan modern yang muncul seiring dengan berkembangnya ilmu pengetahuan dan teknologi. Kejahatan di dunia maya mempunyai karakteristik yang berbeda dengan kejahatan-kejahatan konvensional yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP).

Kejahatan mayantara (*cyber crime*) merupakan kejahatan yang mendapat perhatian luas dunia internasional. Tidaklah mudah untuk menanggulangi permasalahan *cyber crime* diantaranya karena kejahatan tersebut dilakukan dalam ruang lingkup elektronik sehingga untuk penanggulangannya diperlukan keahlian khusus, prosedur investigasi dan kekuatan atau dasar hukum.

Faktor-faktor penyebab laju perkembangan *cybercrime* cenderung mengalami peningkatan dari tahun ke tahun yaitu[42] :

---

[41] Hasil Wawancara dengan Yulianty Pratiwi, *Hasil Tinjauan Aksi Carding mengenai Pencurian Dana Nasabah Bank*, bagian HRD (*Human resorce development)* Bank Mandiri, Bandung, Selasa 16 April 2010, Pukul 14.30 WIB

[42] Dikdik M Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama , Bandung, 2005, hlm 89-95

a. Kesadaran Hukum Masyarakat

Kesadaran hukum masyarakat sampai saat ini dalam menanggapi aktivitas *cyber crime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahatan *cyber crime*. Kurangnya pemahaman dan pengetahuan ini menyebabkan upaya penanggulangan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cyber crime.*

b. Faktor Keamanan

Rasa aman akan dirasakan oleh pelaku kejahatan pada saat sedang menjalankan aksinya. Hal ini karena internet umumnya digunakan di tempat-tempat yang relatif tertutup. Akibatnya pada saat pelaku sedang malakukan kejahatan sangat jarang orang mengetahuinya. Apabila pelaku telah melakukan kejahatan maka dengan mudah pelaku dapat menghapus semua jejak kejahatan yang telah dilakukan. Pada saat pelaku tertangkap sulit bagi aparat penegak hukum untuk menemukan bukti-bukti kejahatan.

c. Faktor Penegak Hukum

Faktor penegak hukum sering menjadi penyebab maraknya kejahatan *cyber*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi, sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak

hukum kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku terlebih apabila kejahatan yang dilakukan memiliki sistem pengoperasian yang sangat rumit.

Banyaknya penyedia internet dan semakin terjangkaunya biaya akses internet membuat semakin banyak orang mulai mengenal internet dan menggunakannya. Hal tersebut membuat para pencuri melakukan aksi *carding database* dengan memanfaatkan kesadaran masyarakat dalam hal ini nasabah bank yang masih kurang mengerti akan dampak negatif dari internet serta ke tidak sempurnaan kebijakan-kebijakan pemerintah dalam hal tersebut.

Dampak negatif yang timbul dari tindak pidana pencurian dana nasabah melalui internet untuk memperoleh informasi personal (*carding database*) melalui pengiriman *e-mail* melahirkan akibat hukum karena hal tersebut mengakibatkan kerusakan pada kehidupan manusia, baik kehidupan manusia secara fisik maupun kehidupan mentalnya.[43]

Kejahatan dengan menggunakan teknologi komputer termasuk pencurian dengan modus *carding database* telah menyebabkan kerugian bagi para pihak , dalam hal ini yaitu :

a. Nasabah
    1) Hilangnya sebagian uang atau seluruhnya milik nasabah yang dicuri oleh pelaku *carding database*.
    2) Kesulitan nasabah dalam melaporkan kejahatan ini kepada pihak yang berwenang dikarenakan prosesnya memakan waktu yang cukup lama dan terlalu banyak biaya.

[43]Aziz Dedy Surohmat, *Aksi Carding*, http://www.raharja.ac.id, Diakses Pada Tanggal 12 Juli 2010, Pukul. 18.32 WIB

b. Pihak Bank.

1) Rusaknya citra bank di mata masyarakat

2) Kepercayaan nasabah dan dunia usaha akan berkurang serta berusaha mencari bank penerbit kartu kredit lain yang terjamin keamanannya.

c. Negara.

1) Penilaian terhadap Indonesia menjadi negatif karena dari hasil riset tahun 2001 dan 2003, Indonesia menempati peringkat ke-2 dalam kejahatan *cybercrime,* sehingga secara tidak langsung akan mempengaruhi perekonomian negara serta merusak citra bangsa di mata dunia[44].

Dilihat dari aspek hukum, akibat yang timbul dari pencurian dana nasabah bank melalui internet dapat dijerat Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) yang menyatakan bahwa :

> ”Barangsiapa mengambil barang sesuatu yang seluruhnya atau sebagian kepunyaan orang lain dengan maksud untuk dimiliki secara melawan hukum diancam karena pencurian dengan pidana penjara paling lama lima tahun atau denda paling banyak enam puluh rupiah.”

Pasal 362 KUHP hanya mengatur pencurian secara umum, sedangkan mengenai pencurian melalui internet KUHP tidak mengatur undang-undang tersebut. Setelah disahkannya Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pelaku pencurian dana nasabah bank

[44] Brian Ami Prastyo, *Kejahatan Cyber*, http://www.clearcommerce.com, Diakses Pada Tanggal 13 Juli 2010, Pukul 15.00 WIB

menurut Pasal 32 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa :

> ”Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak dapat dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).”

Pasal 362 KUHP hanya mengatur pencurian secara umum, sedangkan mengenai pencurian melalui internet KUHP tidak mengatur undang-undang tersebut. Setelah disahkannya Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pelaku pencurian dana nasabah bank melalui internet dapat dikenakan atau dijerat Pasal 32 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.