SKRIPSI

TINDAK PIDANA PERBANKAN DENGAN MEDIA INTERNET

ENDAH SUGIARTI
NIM. 030015134

FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
SURABAYA
2004

TINDAK PIDANA PERBANKAN DENGAN MEDIA INTERNET

SKRIPSI

Diajukan Untuk Melengkapi dan Memenuhi Syarat
Untuk Memperoleh Gelar Sarjana Hukum

Dosen Pembimbing

Bambang Suheryadi, SH, M.H
NIP. 123 162 028

Penyusun

Endah Sugiarti
NIM. 030015134

Skripsi ini akan diuji dan dipertahankan di hadapan Panitia Penguji
Pada tanggal 27 Juli 2004, Pukul 08.30 WIB.

Panitia Penguji Skripsi :

Ketua : Didik Endro Purwoleksono, SH, M.H.

Anggota : 1. Bambang Suheryadi, SH, M.H.

2. Toetik Rahayuningsih, SH, M.Hum

3. Astutik, SH, M.H.

Cara satu-satunya untuk menghindari kesalahan ialah dengan pengalaman. Dan, satu-satunya cara untuk memperoleh pengalaman ialah dengan beberapa kali melakukan kesalahan

Memang baik sekali menjadi orang penting, tetapi yang sangat penting ialah menjadi orang yang baik

KATA PENGANTAR

Dengan menyebut nama Allah yang Maha Pengasih dan Maha Penyayang

Alhamdulillah, segala puji bagi Allah SWT, yang telah memberikan rahmat, kasih sayang dan hidayahNya. Sholawat dan salam, kita haturkan kepada junjungan Nabi Besar Muhammad SAW. Berkat bimbingan dan anugerahNya, akhirnya skripsi dengan judul "TINDAK PIDANA PERBANKAN DENGAN MEDIA INTERNET" dapat selesai dengan baik sebagai tugas dan syarat memperoleh gelar sarjana hukum di Universitas Airlangga.

Ucapan terima kasih dan penghargaan yang sebasar-besarnya penulis sampaikan kepada:

1. Ibu (Sumirah) dan Bapak (Sunarto) yang telah memberikan kasih sayang, bimbingan, semangat, do'a dan perhatian kepada penulis.
2. Bapak H. Machsoen Ali, S.H., M.S., selaku dekan Fakultas Hukum Universitas Airlangga.
3. Bapak Bambang Suheryadi, S.H., M.H.,selaku dosen pembimbing yang telah meluangkan waktu.
4. Bapak Didik Endro Purwoleksono, SH, M.H., Ibu Toetik Rahayuningsih, SH, M. Hum dan Ibu Astutik, SH, M. H., selaku dosen penguji yang baik.

5. Bapak I Wayan Titib Sulaksana, S.H., M.H., yang telah memberikan kesempatan sebagai mahasiswa magang di UPKBH Fakultas Hukum.
6. Temen^2 UPKBH, mas Anjar, mas Yudho, mas Dito, mas Ali, mb Fufah, mb Esti' 4 pengalaman slama di UPKBH.
7. Mb. Lintang, Riesa, Ika, Anis, Sumar, Nurul, mas Joko and temen UPKBH yang lain, thanks 4 smuanya. Trus berjuang..:>..
8. Mbak Laily, Mbak Winny and Mbak Areese, Thanks 4 persahabatan, perhatian dan semangatnya. Jangan bosan untuk trus ngingetin End.
9. Aa' Mif yang sudah memberi semangat and nemenin End ngerjain skripsi. Moga Allah ridho...
10. Mb Gita, Mb Kristin, Wulan, Sunu and temen^2 di Gubair 3.14, thanks untuk kebersamaannya.
11. Buat smua yang telah beri warna dalam kehidupan End.

Semago tulisan, yang masih banyak kekurangan ini, dapat bermanfaat untuk semua. Atas perhatian, penulis ucapkan terima kasih.

Hormat Saya

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

1. Latar Belakang dan Rumusan Masalah

Perkembangan internet dipicu oleh peluncuran pesawat *Sputnik* milik Uni Soviet yang ditanggapi oleh Amerika Serikat dengan membuat proyek peluncuran pesawat luar angkasa dan pengembangan pada tahun 1960-an. Internet pada awal perkembangannya digunakan untuk kepentingan kekuasaan, khususnya kepentingan militer Amerika Serikat.[1] Perkembangan internet ini bertolak belakang dengan penggunaan internet pada saat ini, internet telah digunakan dalam berbagai bidang. Kemajuan penggunaan internet telah dimanfaatkan untuk berbagai kepentingan di berbagai negara.

Perkembangan teknologi pada umumnya dan internet pada khususnya, awalnya tidak dapat dinikmati oleh orang-orang seperti sekarang ini, tetapi bermain dalam tingkat elit. Pengabdian total dunia teknologi terhadap kekuasaan negara adalah inovasi perangkat perang. Penaklukan antar negara bukan sekedar memperluas wilayah untuk kepentingan kaum feodal, melainkan penguasaan sumber-sumber bagi mesin industri.[2] Pemanfaatan teknologi pada saat itu sangat membantu tercapainya tujuan suatu negara.

---

[1]Agus Raharjo, ***Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi***, Cet.I, Citra Aditya Bakti, Bandung, 2002, h.3.

[2]Ashadi Siregar, "Membaca Surat Kabar Digital, Membaca Wajah Populis Teknologi Media", ***Kompas***, 28 Juni 2000, h.70.

Setelah perang dingin berakhir, internet tidak lagi digunakan untuk kepentingan militer, tetapi beralih fungsi menjadi sebuah media yang mampu membawa perubahan dan membuka cakrawala baru dalam kehidupan manusia. Internet merupakan sebuah ruang informasi dan komunikasi yang menjanjikan menembus batas-batas antar negara, mempercepat penyebaran dan pertukaran ilmu dan gagasan di kalangan ilmuwan di seluruh dunia. Internet membawa kita kepada ruang atau dunia baru yang dinamakan *cyber space*.[3] Internet dapat digunakan oleh semua orang dan digunakan untuk berbagai kepentingan.

Teknologi Informasi berkembang sangat pesat dan tidak dapat dipungkiri lagi, internet telah memasuki setiap sendi kehidupan manusia modern. Internet digunakan bukan hanya terbatas pada pemanfaatan informasi yang dapat diakses melalui media ini, melainkan juga dapat digunakan sebagai sarana untuk melakukan transaksi perdagangan yaitu *Electronic Commerce* atau *E-Commerce*, yang merupakan bentuk perdagangan secara elektronik melalui media internet.[4]

Perkembangan juga terjadi dalam dunia perbankan yang dituntut dapat mengikuti perkembangan saat ini. Satu hal yang menjadi tren saat ini di dunia perbankan berkaitan dengan dunia internet adalah adanya *Internet Banking* yaitu fasilitas yang diberikan oleh bank untuk kemudahan nasabahnya dengan melakukan transaksi perbankan melalui internet. Nasabah dapat mengajukan aplikasi dan melakukan transaksi setiap waktu, 24 jam sehari, 7 hari dalam seminggu.

---

[3]Agus Raharjo, ***op. cit.***, h.4

[4]Asril Sitompul, ***Hukum Internet (Pengenalan Mengenai Masalah Hukum di Cyberspace)***, Cet. I, Citra Aditya Bakti, Bandung, 2001, h.2.

Internet Banking telah memberikan kemudahan bagi para nasabah untuk melakukan transaksi perbankan. *Internet banking* juga dilengkapi sistem pengamanan yang terbaru untuk kenyamanan para penggunanya, sehingga para pengguna jasa ini merasa aman untuk bertransaksi melalui internet. Sistem pengamanan yang diklaim sebagian besar penyelenggara *Internet Banking* di Indonesia adalah:

1. Program *International Internet Standard Security SSL* 3.0 dengan metode 128-bit enkripsi, yaitu seluruh data yang masuk sejak *log in* di *Internet Banking* akan dikirimkan melalui *Secure Socket Layer* (SSL). SSL akan mengacak data yang dikirim menjadi kode-kode rahasia dengan menggunakan 128-bit *encryption*, yang artinya terdapat 2 pangkat 128 kombinasi angka kunci tetapi hanya satu kombinasi yang dapat membuka kode-kode tersebut.
2. *Security Plugins* yang dipasang secara otomatis saat nasabah mengakses Internet Banking pertama kali. User ID dan Personal Identification Number (PIN) Internet Banking yang harus dimasukkan setiap kali melakukan log in ke Internet Banking dan di cek oleh sistem.
3. *Firewall* berfungsi untuk membatasi dan mencegah akses ilegal ke sistem Internet Banking.
4. *Automatic Log Out* yaitu jika tidak terdapat aktifitas atau transaksi selama 5 sampai 10 menit sistem Internet Banking secara otomatis akan mengakhiri (log out) akses untuk mencegah penyalahgunaan yang tidak berwenang dan kembali ke menu utama.

Fasilitas *internet banking* ini memberikan banyak kemudahan bagi nasabah, mulai dari pengecekan saldo, pemindahbukuan pihak III sampai membayar berbagai macam tagihan, tanpa harus datang langsung ke bank. Transaksi tersebut dapat dilakukan setiap saat hanya dengan mengakses situs bank yang bersangkutan. Contoh penerapan *internet banking* di bank-bank Indonesia antara lain: www.klikbca.com, www.bii.com, www.lippobank.com, www.bankniaga.com dan masih banyak bank-bank lain yang juga manggunakan *internet banking* untuk kemudahan nasabahnya..

Perkembangan teknologi informasi tidak hanya menghasilkan keuntungan ekonomis atau keuntungan lainnya, tetapi juga melahirkan "lahan" baru bagi para penjahat yang akan menghasilkan kejahatan baru pula. Seorang yang ahli di bidang Teknologi Informasi dapat melakukan "pembobolan" rekening nasabah yang menggunakan fasilitas *internet banking.* Kejahatan di dunia internet atau yang juga dikenal sebagai *cyber crime* ini merupakan dampak negatif yang dialami para pengguna dari *internet banking.*

Kejadian "Klik BCA" semu yang baru saja terjadi menyadarkan para pengguna Internet Banking di Indonesia akan dampak negatif ini.[5] Resiko lain adalah apabila nasabah menggunakan komputer di warung internet (warnet) untuk bertransaksi. Komputer di warnet pada umumnya rentan terhadap virus dan program sederhana yang terdownload. Program yang ada tidak mustahil sengaja dibuat untuk membaca yang nasabah ketik (termasuk *user ID* dan *password*), untuk kemudian dikirimkan kepada pembuat program dan digunakan untuk

---

[5] I Made Wiryana dan Tedi Heriyanto, *"Resiko Internet Banking telah Tampak"*, **http://www.tedi-h.com/papers/i-banking.html.**

mengambil manfaat.[6] Dampak negatif ini menjadikan para pengguna *internet banking* untuk lebih waspada dan berhati-hati dalam melakukan transaksinya.

Kecemasan terhadap *cyber crime* ini telah menjadi perhatian dunia, terbukti dengan dijadikannya masalah *cybercrime* sebagai salah satu topik bahasan pada Kongres PBB mengenai *The Prevention of Crime and The Treatment of Offender* ke-8 tahun 1990 di Havana, Kuba dan Kongres ke-10 di Wina dengan topik bahasan *Crime Related to Computer Network.*[7] Kebijakan penanggulangan *cyber crime* yang dikemukakan dalam Resolusi PBB VII tahun 1990, meliputi penanggulangan melalui kebijakan penal dan juga melalui kebijakan non penal.

Penanggulangan melalui kebijakan penal antara lain adalah himbauan negara anggota untuk melakukan modernisasi hukum pidana materiil dan hukum pidana formil. Selain itu juga adanya himbauan untuk melakukan upaya-upaya pelatihan atau *training* bagi para hakim, pejabat dan aparat penegak hukum lainnya mengenai kejahatan ekonomi dan *cyber crime.*

Penanggulangan melalui kebijakan non penal terdiri dari dua pendekatan. Pertama, pendekatan *technoprevention* yaitu upaya pencegahan atau penanggulangan kejahatan dengan menggunakan teknologi. *Technoprevention* ini dilakukan melalui upaya mengembangkan pengamanan atau perlindungan komputer dan tindakan-tindakan pencegahan. Kedua, pendekatan budaya atau kultural atau etik yaitu membangun atau membangkitkan kepekaan warga

---

[6]FAQ, *"Apakah Aman Bertransaksi Lewat Warnet?"*, http://www.lippobank.co.id/faq.html.

[7]Agus Raharjo, *op. cit.*, h.6.

masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan atau mengajarkan etika penggunaan internet atau komputer malalui media pendidikan.

Penanggulangan melalui kebijakan penal di Indonesia dapat kita lihat dalam upaya pengaturan *cyber crime* dalam Rancangan Undang-undang Pemanfaatan Teknologi Informasi (selanjutnya disebut RUU-PTI). Versi ke-6 RUU-PTI merupakan draft final yang disusun oleh Pusat Studi Hukum Teknologi Informasi Fakultas Hukum Universitas Padjajaran atas prakarsa dari Direktorat Jenderal Pos dan Telekomunikasi.

Model yang digunakan dalam RUU-PTI ini adalah *Umbrella Provision* sehingga ketentuan *cyber crime* tidak dalam perundang-undangan tersendiri, tetapi diatur secara umum dalam RUU-PTI tersebut. ketentuan yang terdapat dalam RUU-PTI terlihat bahwa ruang lingkup yang dikemukakan tidak berbeda jauh dengan yang telah diatur dalam perundang-undangan di negara lain.

Dengan adanya RUU-PTI ini, dapat dilihat bahwa Indonesia telah melakukan langkah awal dalam melakukan pengaturan masalah *cyber crime*, walaupun sampai saat ini belum terselesaikan.

Perkembangan penggunaan internet di Indonesia saat ini cukup pesat, walaupun jika dibandingkan dengan negara lain Indonesia masih tertinggal. Perkembangan penggunaan internet di Indonesia dan meningkatnya jumlah pengguna jasa ini, sayangnya tidak disertai dengan perkembangan hukum di bidang ini. Kajian kriminologi yang ada saat ini merupakan kajian terhadap kejahatan yang terjadi di dunia nyata (*physical world* atau *real life*), sedangkan

penggunaan dan pemanfaatan internet menimbulkan dimensi baru kejahatan yang terjadi di dunia maya (*virtual reality*).[8] Kenyataan ini akan menimbulkan kesulitan bagi kita untuk mencegah ataupun menangani kejahatan yang terjadi di dunia maya.

Yusril Ihza Mahendra, mengakui sendiri bahwa Indonesia sampai saat ini belum memiliki pengaturan khusus mengenai *cyber space* atau *cyber world.* Keadaan ini diakuinya bukan berarti pemerintah kurang peka terhadap perkembangan teknologi informasi, tetapi lebih disebabkan pengaturan mengenai *cyber space* memerlukan kajian-kajian yang cermat dan mendalam, agar benar-benar tepat sasaran sesuai dengan tingkat perkembangan perilaku kehidupan masyarakat, sehingga tidak akan menimbulkan stagnasi di dalam implementasinya.[9]

Pengaturan mengenai kejahatan dalam dunia maya memang belum ada pengaturan secara khusus, tetapi hal ini tidak menyurutkan POLRI sebagai salah satu penegak hukum untuk mengantisipasi adanya kejahatan (*crime*) yang dilakukan di dunia maya (*cyber space*). Antisipasi POLRI ini dapat dilihat dengan tanpa banyak publikasi ternyata dalam tubuh POLRI telah dibentuk satu seksi khusus untuk menangani masalah kejahatan ini. Seksi ini bekerja di bawah Sub Dit Pidana Teknologi Informasi diretorat Tindak Pidana Khusus Koserse

---

[8]Agus Raharjo, ***op. cit.***, h.201.

[9]Yusril Ihza Mahendra, ***Regulasi Cyberspace di Indonesia***, Makalah "Cyber Law", Yayasan Cipta Bangsa, Badung, 29 Juli 2000, h. 3.

POLRI.[10] Tindakan ini menunjukkan adanya upaya dalam menanggulangi atau menangani kasus di bidang perbankan terkait dengan *cyber crime*.

Kesulitan dalam penyusunan perundang-undangan dikaitkan dengan serbuan internet dan pemanfaatannya di bidang perbankan yang tidak bisa dibendung, serta dalam menghadapi kejahatan dalam dunia maya (*cyber crime*) ini dimunculkan pemikiran untuk menggunakan hukum positif yang ada (*The Existing Law*).

Keseluruhan uraian latar belakang di atas mengenai *cyber crime* dalam dunia perbankan, maka permasalahan yang dapat diambil adalah sebagai berikut:

1. Apakah perundang-undangan pidana di Indonesia dapat menjangkau tindak pidana perbankan dengan media internet?
2. Bagaimanakah upaya penegakan hukum terhadap tindak pidana perbankan dengan media internet?

2. Penjelasan Judul

Judul Skripsi ini adalah "TINDAK PIDANA PERBANKAN DENGAN MEDIA INTERNET". Adapun penjelasan dari judul di atas adalah sebagai berikut:

Istilah tindak pidana merupakan salinan dari istilah Belanda yaitu *strafbaar feit*, yang pengertiannya:[11]

> Simons menerangkan, bahwa s*trafbaar feit* adalah kelakuan (*handeling*) yang diancam dengan pidana, yang bersifat melawan hukum, yang

[10]Nur Raihan dan Sigit Widodo, **http://www.detik.com.**

[11]Moeljatno, ***Asas-asas Hukum Pidana***, Cet. 6, Rineka Cipta, Jakarta, 2000, h. 56.

berhubungan dengan kesalahan dan yang dilakukan oleh orang yang mampu bertanggung jawab.
Van Hamel merumuskan, bahwa *strafbaar feit* adalah kelakuan orang (*menselijke gedraging*) yang dirumuskan dalam wet, yang bersifat melawan hukum, yang patut di pidana (*strafwaardig*) dan dilakukan dengan kesalahan.
Perbankan dalam judul penulisan ini adalah sebagaimana perbankan yang dimaksud dalamketentuan pasal 1 angka 1 Undang-undang nomor 10 Tahun 1998 tentang Perbankan, yang uraiannya adalah:

> Pasal 1 angka 1:
>
> Perbankan adalah segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya.

Agus Raharjo berpendapat bahwa Internet dari segi penulisannya memiliki 2 (dua) arti, yaitu:[12]

1. *internet*
   Jaringan internet (huruf "i" kecil sebagai huruf awal) adalah suatu jaringan komputer yang mana komputer-komputer terhubung dapat berkomunikasi walaupun perangkat keras dan perangkat lunaknya berlainan (sering kali disebut juga *internet working*)
2. *Internet*
   Jaringan *Internet* (huruf "I" besar sebagai huruf awal) adalah jaringan dari sekumpulan jaringan (*nerwork of network*) yang terdiri dari jutaan komputer yang dapat berkomunikasi satu sama yang lain dengan menggunakan suatu aturan komunikasi jaringan (protokol) yang sama. Protokol yang digunakan tersebut adalah *Transmission Control Protocol/Internet protocol* (TCP/IP).

Internet sendiri merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik, satelit atau pun gelombang frekuensi yang berukuran super besar berbasis pada *Transmission Control Protocol/Internet Protocol* (TCP/IP).[13]

---

[12] Agus Raharjo, ***op. cit.***, h. 60

[13] ***Ibid.*** , h. 59.

3. Alasan Pemilihan Judul

Alasan pemilihan judul tentang "TINDAK PIDANA PERBANKAN DENGAN MEDIA INTERNET" karena masalah kejahatan dengan media *internet* ini cukup menarik untuk dikaji, khususnya dalam pengembangan ilmu hukum pidana di era *cyber space*.

Tulisan ini juga diharapkan dapat memberikan sumbangan bagi para pengguna layanan internet dan penegak hukum terutama dalam kaitannya dengan pencegahan, penanggulangan dan penanganan kasus-kasus yang terjadi di Indonesia pada masa kini dan utamanya masa yang akan datang.

4. Tujuan Penulisan

Tujuan utama yang ingin dicapai dalam penulisan ini adalah untuk mengetahui pengaturan tentang Tindak Pidana Perbankan dengan media internet dalam perundang-undangan pidana di Indonesia, sehingga dapat diterapkan dalam menangani kasus tindak pidana perbankan khususnya yang terkait dengan media internet

Tujuan khusus yang ingin dicapai dalam penulisan ini adalah pertama, untuk mengetahui perundang-undangan pidana di Indonesia dapat atau tidak menjangkau Tindak Pidana Perbankan dengan media internet. Kedua, untuk mengetahui upaya penegakan hukum terhadap Tindak pidana Perbankan dengan media internet.

5. Metode Penulisan

a. Pendekatan masalah.

Penulisan skripsi ini adalah penulisan hukum normatif. Pendekatan masalah yang digunakan adalah *Statute Approach*, yaitu pendekatan melalui perundang-undangan khususnya dengan melihat berbagai peraturan perundang-undangan yang terkait dengan tindak pidana perbankan dengan media internet atau kejahatan yang dilakukan di dunia maya *(cyber space)*.

b. Bahan hukum.

Bahan hukum yang dipergunakan dalam penulisan skripsi ini terdiri dari dua jenis. Pertama, bahan hukum primer yaitu peraturan perundang-undangan, keputusan-keputusan maupun ketetapan-ketetapan dari lembaga yang berwenang, yang berkaitan dengan tema dalam penulisan skripsi ini. Diantaranya adalah Kitab Undang-undang Hukum Pidana (KUHP), Undang-undang Nomor 7 tahun 1992 jo Undang-undang Nomor 10 tahun 1998 tentang Perbankan, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan peraturan perundang-undangan lainnya yang terkait dengan tema penulisan ini. Kedua, bahan hukum sekunder yaitu bahan hukum yang menunjang pembahasan permasalahan yang ada di kepustakaan,yang berupa buku-buku, tulisan-tulisan dari para sarjana hukum, surat kabar, internet maupun karya-karya lain yang terkait dengan penulisan ini.

c. Analisis bahan hukum.

Metode analisis yang digunakan dalam penulisan ini adalah *Yuridis Interpretatif*, yaitu dengan menginterpretasikan isi dari peraturan perundang-undangan yang terkait dengan media internet dalam Tindak Pidana Perbankan sehingga dapat menjawab pertanyaan-pertanyaan yang timbul dalam penulisan ini. Interpretasi yang dilakukan didukung oleh adanya bahan-bahan sekunder yang mendukung interpretasi tersebut.

6. Pertanggungjawaban Sistimatika

Pertanggungjawaban dari sistematika yang telah tersusun dalam kerangka skripsi ini adalah sebagai barikut:

Bab I tentang Pendahuluan, membahas tentang latar belakang dan rumusan masalahnya, penjelasan judul, alasan pemilihan judul, tujuan dari penulisan skripsi, metode penulisan yang dibagi dalam sub-subbab, yaitu pendekatan masalah, bahan hukum dan analisis bahan hukum, dan subbab terakhir adalah pertanggungjawaban sistematika. Bab ini merupakan dasar pembahasan dalam bab-bab selanjutnya.

Bab II tentang ketentuan-ketentuan hukum pidana yang terkait dengan Tindak Pidana Perbankan dengan media internet. Subbab pertama membahas tentang kejahatan *internet* dalam bidang perbankan di Indonesia. Subbab kedua membahas tentang ketentuan hukum pidana dalam perundang-undangan di Indonesia terkait dengan Tindak Pidana Perbankan dengan media internet.

Bab III tentang upaya penegakan hukum terhadap tindak pidana perbankan dengan media internet. Subbab pertama membahas tentang penyelidikan dan penyidikan dalam kasus Tindak Pidana Perbankan dengan Media Internet. Subbab kedua membahas tentang Kendala-kendala yang dihadapi dalam menangani Kasus Tindak Pidana Perbankan dengan Media Internet.

Bab IV merupakan penutup yang berisi kesimpulan dan saran. Kesimpulan berisi uraian singkat dari pembahasan dua rumusan masalah yang diajukan pada bab-bab sebelumnya. Saran diharapkan dapat berguna dalam pembentukan Undang-Undang tentang kejahatan (*crime*) dunia maya (*cyberspace*).

BAB II

KETENTUAN HUKUM PIDANA TERKAIT DENGAN TINDAK PIDANA PERBANKAN YANG MENGGUNAKAN MEDIA INTERNET

1. Kejahatan Perbankan Dengan Media Internet

Teknologi internet yang telah mengalami perkembangan pesat menawarkan pelbagai macam kemudahan dalam kegiatan transaksi bisnis, termasuk bagi dunia perbankan di Indonesia yang diwujudkan dalam bentuk *internet banking*. Kemudahan itu antara lain dimulai dari penawaran jasa perbankan melalui situs-situs yang dibuat oleh bank sampai pada tawaran untuk melakukan transaksi secara *online* melalui media internet.

Pada dasarnya *internet banking* memiliki 3 (tiga) tahapan pelayanan yang ditawarkan pada nasabahnya yaitu: [14]

a) Layanan Informasi (*Informational*)

Bank dalam layanan ini hanya menyediakan informasi jasa keuangan bagi *website*nya.

b) Layanan Komunikasi (*communicational*)

Nasabah sudah dimungkinkan untuk berkomunikasi dengan bank melalui *website*nya.

---

[14] Syahril Sabirin, ***Urgensi Regulasi dalam Internet banking***, Seminar Sehari "Aspek hukum *internet banking* dalam kerangka Hukum Teknologi Informasi", Universitas Padjajaran, Bandung, 13 Juli 2001, h. 2.

c) Layanan Transaksi (*Transactional/advance*)

Nasabah dalam layanan ini sudah dimungkinkan untuk melakukan transaksi-transaksi keuangan *virtual* seperti transfer dana, pengecekan saldo, ataupun berbagai jenis pembayaran.

Keberadaan *internet banking* telah menyebabkan tingkat efisiensi penyelenggaraan kegiatan usaha bank sangat tinggi. Secara konvensional dulu bank dalam penyelenggaraan kegiatan usahanya membutuhkan biaya yang sangat besar. Namun, dibalik keuntungan yang di dapat dari *internet banking* ada beberapa resiko yang akan dihadapi dari penyelenggara *internet banking*.

Syahril Sabarin berpendapat ada 4 (empat) resiko manajemen yang terkait dengan penggunaan *internet banking*, yaitu:[15]

a) *Technology risk*

Resiko ini berhubungan dengan kehandalan dan keamanan sistem dari berbagai bentuk manipulasi ataupun "pembobolan".

b) *Reputational risk*

Berkaitan erat dengan *corporate image* dari bank sendiri apabila pelayanan *internet banking*nya tidak berjalan dengan baik.

c) *Outsourcing risk*

Resiko yang muncul karena bank kerap menggunakan jasa pihak ketiga sebagai *internet service provider* (ISP) sehingga ada kemungkinan layanan ISP pada suatu waktu dapat mengalami gangguan.

---

[15] ***Ibid.***

d) *Legal risk*

Resiko ini berkaitan dengan hukum *internet banking* yang sampai saat ini belum diatur jelas.

Antisipasi pada kejahatan yang dilakukan di dunia maya (*cyberspace*) perlu dilakukan karena berdasarkan salinan data yang diperoleh dari *hukumonline*, jumlah kasus yang masuk ke Subdit Tindak Pidana Teknologi Informasi (Subdit TPTI) sepanjang 2002 mengalami peningkatan dibandingkan tahun 2001 yang bentuk kejahatannya dibagi menjadi dua kelompok besar, yaitu:[16]

Tabel 1.

KEJAHATAN UMUM YANG DIFASILITASI TEKNOLOGI INFORMASI			
No.	Jenis Kejahatan	Jumlah kasus	
		2001	2002
1.	*credit card fraud*	5	104
2.	*stock exchange fraud*	1	-
3.	*banking fraud*	1	4
4.	*child phornography*	1	-
5.	*drug trafficking*	1	-
6.	*terorism*	-	1

Tabel 2.

KEJAHATAN YANG MENJADIKAN SISTEM DAN FASILITAS TEKNOLOGI INFORMASI SEBAGAI SASARAN			
No.	Jenis Kejahatan	Jumlah kasus	
		2001	2002
1.	*DDoS attack*	4	3
2.	*Defacing*	3	-
3.	*Cracking*	1	3
4.	*Phreaking*	-	1
5.	*lainnya*	1	-

[16] *Modus Operandi Cybercrime di Indonesia Makin Canggih*, **www. hukumonline.com**, 3 Januari 2003.

Kejahatan internet yang berkaitan dengan tindak pidana perbankan dari sumber Subdit TPTI tersebut antara lain: *credit card fraud* dan *banking fraud* yang jumlahnya mengalami banyak peningkatan. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasaran juga dapat terjadi dalam dunia perbankan yaitu melalui layanan *internet banking*nya.

Kejahatan *internet* di bidang perbankan dari sumber Subdit TPTI secara keseluruhan dapat dibagi menjadi 2 (dua) kategori, yaitu:

1. Kejahatan umum di bidang perbankan yang difasilitasi teknologi informasi.

   Teknologi informasi yang dimaksud sebagai fasilitas kejahatan umum di bidang perbankan adalah *internet.* Contohnya adalah adanya *credit card fraud* dan *banking fraud.*

2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasaran.

   Teknologi informasi bidang perbankan tersebut diwujudkan dalam *internet banking.* Contohnya adalah layanan *internet banking* suatu bank yang mengalami *hacking, defacing* atau *cracking.*

Penulisan skripsi ini dikaitkan dengan dua kategori yang tersebut di atas, lebih mengarah pada bentuk-bentuk kejahatan umum dalam bidang perbankan yang difasilitasi dengan teknologi informasi.

Badan Pembinaan Hukum Nasional (BPHN) telah mengidentifikasi bentuk-bentuk kejahatan yang berkaitan dengan aktivitas di *cyberspace* antara lain:

1. *Joycomputing*

   Bentuk kejahatan ini diartikan sebagai perbuatan seseorang yang menggunakan komputer secara tidak sah atau tanpa ijin dan menggunakannya melampaui wewenang yang diberikan.

2. *Hacking*

   Kejahatan ini diartikan sebagai perbuatan penyambungan dengan cara merambah terminal komputer baru pada sistem jaringan komputer tanpa ijin (dengan melawan hukum) dari pemilik sah jaringan komputer tersebut.

3. *The Trojan Horse*

   Suatu prosedur yang menambah, mengurangi atau mengubah instruksi pada sebuah program, sehingga program tersebut selain menjalankan tugas yang sebenarnya juga akan melakukan tugas lain yang tidak sah.

4. *Data Leakage*

   Merupakan pembocoran rahasia yang dilakukan dengan cara menulis data-data rahasia tersebut ke dalam kode-kode tertentu sehingga data dapat dibawa keluar tanpa diketahui oleh pihak yang bertanggung jawab.

5. *Data diddling*

   Suatu perbuatan yang mengubah data *valid* atau sah dengan cara tidak sah yaitu dengan mengubah *input* data atau *output* data.

6. Penyia-nyiaan data komputer.

   Perbuatan yang dilakukan dengan suatu kesengajaan untuk merusak atau menghancurkan media disket atau media penyimpanan sejenis lainnya yang

berisikan data atau program komputer, sehingga data atau progam yang dimaksud menjadi tidak berfungsi dan tidak dapat dijalankan.

Bentuk-bentuk kejahatan hasil dari identifikasi BPHN tersebut dapat terjadi di dunia perbankan melalui layanan *internet banking*-nya, misalnya untuk *joycomputing* dapat terjadi pada kajahatan kartu kredit (*credit card fraud*). Bentuk kejahatan pada angka 1 (satu), 4 (empat) dan 6 (enam) dapat dikategorikan sebagai kejahatan yang menjadikan sistem dan fasilitas teknologi informasi dalam dunia perbankan yang diwujudkan dalam layanan *internet banking* sebagai sarana atau alat.

Masalah hukum dalam praktik *internet banking* dikaitkan dengan bentuk-bentuk kejahatan internet yang telah diuraikan sebelumnya, kita dapat mengacu pada 3 (tiga) pendapat yang berkembang pada penerapan hukum secara umum dalam aktivitas internet.[17]

Pendapat pertama adalah menolak secara total setiap usaha untuk membuat aturan hukum bagi aktivitas-aktivitas di internet yang didasarkan pada sistem hukum konvensional. Pendapat ini beranggapan bahwa internet yang layaknya sebuah surga demokrasi (*democratic paradise*) yang menyajikan wahana bagi adanya lalu lintas ide yang secara bebas dan terbuka tidak boleh dihambat dengan aturan yang didasarkan pada sistem hukum konvensional yang bertumpu pada batas-batas teritorial.

Pendapat kedua adalah penerapan hukum konvensional untuk mengatur aktivitas di internet dapat dilakukan karena sangat mendesak. Penerapan tersebut

---

[17] Budi Agus Riswandi, ***Hukum dan Internet di Indonesia***, Cet. I, UII Press, Yogyakarta, April 2003, h. 77.

tanpa harus menunggu terbentuknya sistem hukum yang paling tepat untuk mengatur aktivitas di internet.

Pendapat ketiga menyatakan bahwa aturan hukum yang akan mengatur aktivitas di internet harus dibentuk secara *evolutif* dengan cara menerapkan prinsip-prinsip *common law* yang dilakukan secara hati-hati dan dengan menitikberatkan pada aspek tertentu dalam aktivitas *cyberspace*.

2. Ketentuan-ketentuan Hukum Pidana yang Terkait dengan Tindak Pidana Perbankan dengan Media Internet

Masalah yang ditimbulkan dengan adanya layanan *internet banking* dalam dunia perbankan telah mendapat perhatian yang serius dari pihak Bank Indonesia sebagai lembaga yang mempunyai tugas mengawasi bank-bank umum.

Keseriusan Bank Indonesia salah satunya diwujudkan dengan diberlakukannya Surat Keputusan Direksi Bank Indonesia Nomor 27/164/Kep/Dir dan Surat Edaran Bank Indonesia Nomor 27/9/UPPB tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank. Surat keputusan Direksi Bank Indonesia ini mengatur adanya kewajiban melapor oleh bank kepada Bank Indonesia apabila bank yang bersangkutan memanfaatkan atau mengembangkan teknologi sistem informasi, yaitu terdapat dalam pasal 5 Surat Keputusan Direksi Bank Indonesia Nomor 27/164/Kep/Dir/1995 yang terdiri dari 6 (enam) macam laporan.

Pelanggaran terhadap ketentuan pasal 5 ini selain dikenakan sanksi administrasi, juga dapat dikenakan sanksi berupa denda. Sanksi administrasi yang

dikenakan dapat berupa pembekuan kegiatan usaha tertentu yang berhubungan dengan teknologi sistem informasi dan atau penurunan tingkat kesehatan bank. Sanksi denda untuk tidak disampaikannya laporan adalah dengan membayar uang setinggi-tingginya Rp 2.000.000,00 (dua juta rupiah) untuk masing-masing laporan dan untuk keterlambatan penyampaian laporan dikenakan denda sebesar Rp 1.000.000,00 (satu juta rupiah) per bulan keterlambatan untuk masing-masing laporan, kecuali untuk jenis laporan dalam huruf b dan c pasal 5 Surat Keputusan Direksi Bank Indonesia Nomor 27/164/Kep/Dir/1995.

Hal-hal yang diatur dalam Surat Keputusan Direksi Bank Indonesia Nomor 27/164/Kep/Dir/1995 tersebut lebih pada langkah preventif dari Bank Indonesia dalam menghadapi meningkatnga pemanfaatan Teknologi Sistem Informatika (TSI) oleh bank-bank yang ada di Indonesia. Langkah preventif ini lebih ditekankan pada pengamanan penggunaan TSI oleh bank. Langkah lain yang dilakukan Bank Indonesia dalam menghadapi penyalahgunaan TSI adalah dengan membentuk Unit Investigasi Tindak Pidana Perbankan.

Permasalahan yang kemudian muncul adalah peraturan yang akan diterapkan jika terjadi tindak pidana perbankan yang terkait dengan TSI. Aturan hukum yang dapat diterapkan untuk para pelaku tindak pidana perbankan dengan media internet yaitu:

a. KUHP

Ketentuan-ketentuan dalam KUHP yang dapat diterapkan untuk pelaku tindak pidana perbankan dengan media *internet* dapat dilihat dalam beberapa pasal dalam KUHP, antara lain:

1.) Pasal 362

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

Unsur-unsur yang terdapat dalam Pasal 362 adalah:

1. unsur mengambil

   Unsur pertama Pasal 362 KUHP ini memiliki pengertian harus adanya perbuatan "mengambil" dari tempat dimana barang tersebut terletak. Kata "mengambil" sudah tersimpul pengertian "sengaja", sehingga pada pasal ini tidak menyebutkan "dengan sengaja mengambil".[18] Perbuatan "mengambil" pada umumnya terjadi karena sentuhan tangan atau dengan sentuhan tangan, tetapi pencurian juga dapat terjadi misalnya dengan "mengambil" nomor kartu kredit orang lain dengan "membobol" *database* dari suatu bank yang juga sebagai penyedia jasa kartu kredit.

2. unsur "barang" yang diambil

   Barang yang diambil harus barang yang berwujud, tetapi berdasarkan Arrest Hoge Raad tanggal 23 Mei 1921 No. W.10728[19] tentang pencurian listrik. Arrest Hoge Raad. ini, tenaga listrik melalui interpretasi/penafsiran *extensif* dapat menjadi obyek pencurian. Berdasarkan Arrest Hoge Raad tersebut maka nomor kartu kredit milik orang lain yang terdapat dalam *database* dari suatu bank juga dapat menjadi obyek pencurian.

---

[18] Hermien Hadiati Koeswadji et al, ***Delik harta kekayaan, asas-asas, kasus dan Permasalahannya***, Cet. I, Sinar Wijaya, Surabaya,1984, h. 20.

[19] ***Ibid***., h. 22.

3. unsur tujuan memiliki barang secara melawan hukum

Wirjono berpendapat bahwa titik berat unsur ini harus diletakkan pada tidak adanya ijin dari pemilik dan juga dapat ditafsirkan menurut pendapat Noyon yaitu bahwa "pemilikkan dengan melawan hukum "diartikan sebagai: "berbuat sesuatu dengan barang seolah-olah pemilik barang tersebut dan dengan perbuatan itu melanggar atau melawan hukum".[20]Uraian unsur tersebut dapat diterapkan pada para pelaku tindak pidana kartu kredit dengan media *internet* yang mengambil dan menggunakan kartu kredit orang lain seolah-olah ia pemilik kartu kredit tersebut.

Kejahatan kartu kredit juga dapat dikenakan ketentuan Pasal 378 KUHP tentang penipuan, berikut uraian pasalnya:

> 2.) Pasal 378
>
> Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat (hoedanigheid) palsu; dengan tipu muslihat,ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam, karena penipuan, dengan pidana penjara paling lama empat tahun.

Unsur-unsur yang terdapat dalam Pasal 378 adalah:

1. Dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum

Unsur ini terdapat adanya kesengajaan dari *carder* untuk menguntungkan diri sendiri dengan melakukan perbuatan-perbuatan yang melawan hukum untuk mendapatkan barang yang dibelinya secara *on-line*.

---

[20] ***Ibid.***, h. 25

2. Dengan menggunakan daya upaya, seperti memakai nama palsu atau martabat (hoedanigheid) palsu; dengan tipu muslihat,ataupun rangkaian kebohongan.

   Seorang pelaku dalam kejahatan kartu kredit tidak secara langsung mengambil barang yang ingin dimilikinya. Seorang *carder* menggunakan identitas palsu dan nomor kartu kredit milik orang lain pada saat bertransaksi secara *on-line* dengan penjual.

3. Menggerakkan orang lain untuk menyerahkan barang/benda atau supaya memberi utang maupun menghapuskan piutang

   Unsur ketiga ini sesuai dengan tindakan *carder* yang membuat Penjual toko *on-line* untuk menyerahkan barang atau jasa yang ia jual kepada *carder*.

Bentuk kejahatan lain yang dapat dikenakan Pasal 362 ini adalah *joycomputing*, karena pelaku "mengambil" dengan cara menggunakan komputer secara tidak sah atau tanpa ijin yang melampaui wewenang (seolah-olah ia pemiliknya).

Pasal lain yang dapat dikenakan pada *joycomputing* adalah Pasal 167 ayat (1) KUHP, yang uraiannya adalah:

> 3.) Pasal 167 ayat (1)
>
> Barang siapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama sembilan bulan atau denda paling banyak tiga ratus rupiah.

Unsur-unsur yang terdapat dalam Pasal 167 KUHP antara lain:

1. unsur memaksa masuk

   Unsur memaksa masuk dalam pasal ini dapat dilakukan dengan cara merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu tanpa sepengetahuan yang berhak.

   Dalam kejahatan di dunia maya, "cara" yang digunakan tidak lagi langsung pada obyeknya yang bersifat fisik. Tindakan ini dapat berupa suatu jejak elektronik *(electronic path)* yang berisikan data atau angka matematis yang mengindikasikan telah berlangsung aktivitas elektronis.

2. rumah, ruangan atau pekarangan tertutup yang dipakai orang lain secara melawan hukum

   Unsur kedua ini termasuk juga suatu sistem jaringan komputer milik orang lain tanpa ijin dari pemilik yang sah (dengan melawan hukum) karena menyangkut *privasi* seseorang..

   Tidak termasuk kejahatan dengan media informasi, jika seseorang masuk dalam suatu sistem informasi situs *website* yang hanya memuat iklan atau hanya digunakan untuk melakukan browsing atas informasi yang disediakan. Situs yang hanya menyediakan informasi saja dikategorikan pasif. Seseorang yang masuk ke dalam situs ini tanpa melakukan hal-hal yang merugikan pemilik *website*, maka tidak temasuk dalam ketentuan Pasal 167 KUHP.

Pasal 167 KUHP ini dapat dikenakan pada bentuk kejahatan di internet yang berupa *hacking*, yaitu memasuki sistem jaringan komputer tanpa ijin dari

pemilik sah (secara melawan hukum) dan adanya kerugian yang dirasakan dari pemilik *website.*

Bentuk kejahatan lain yang dapat dikenakan ketentuan pasal dalam KUHP adalah *The Trojan Horse* yaitu dengan Pasal 372 KUHP, yang uraiannya adalah:

4.) Pasal 372

> Barangsiapa dengan sengaja dan melawan hukum mengaku sebagai milik sendiri (zich toeegenen) barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, tetapi yang ada dalam kekuasaannya bukan karena kejahatan, diancam, karena penggelapan, dengan pidana penjara paling lama empat tahun atau denda paling banyak enam puluh rupiah.

Unsur-unsur yang terdapat dalam Pasal 372 KUHP kaitannya dengan *The Trojan Horse* adalah:

1. Dengan sengaja dan melawan hukum mengaku sebagai milik sendiri

   The Trojan Horse dilakukan dengan kesengajaan menambah, mengubah atau mengurangi instruksi pada sebuah program seolah-olah ia adalah pemiliknya.
2. Barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain.

   Unsur "barang" dalam pasal ini dapat berupa program dalam suatu sistem komputer *dengan* cara menambah, mengurangi atau mengubah instruksi dalam program tersebut.

The Trojan Horse jika berkaitan dengan jabatan atau hubungan kerja maka dapat dikenakan Pasal 374 KUHP, yang pasalnya berbunyi:

5.) Pasal 374

> Penggelapan yang dilakukan oleh orang yang penguasaannya terhadap barang disebabkan karena ada hubungan kerja atau karena pencariannya atau karena mendapat upah untuk itu, diancam dengan pidana penjara paling lama lima tahun.

Unsur-unsur yang terdapat dalam Pasal 263 KUHP antara lain:

1. dengan sengaja dan melawan hukum

   Unsur ini terdapat adanya kesengajaan pelaku dalam melakukan tindakannya yang melawan hukum yang berupa merusak, menghancurkan atau menghilangkan barang milik orang lain sehingga tidak dapat dipakai.

   Kejahatan dengan media internet kebanyakan dilakukan dengan suatu kesengajaan karena untuk masuk ke dalam suatu sistem informasi diperlukan suatu keahlian yang khusus, yaitu keahlian di bidang teknik informasi.

   Kesengajaan menurut doktrin dalam Hukum Pidana kita terbagi atas:[21]

   a. Kesengajaan sebagai maksud atau tujuan, terjadinga suatu maksud atau tindakan atau akibat tertentu (sesuai dengan perumusan undang-undang hukum pidana) adalah betul-betul sebagai perwujudan dari maksud atau tujuan dan pengetahuan dari si pelaku.

   b. Kesengajaan dengan kesadaraan kapastian atau keharusan, yang menjadi sandaran adalah seberapa jauh pengetahuan atau kesadaran pelaku tentang tindakan dan akibat yang merupakan salah satu unsur dari suatu delik. Dalam hal ini tindakan atau akibat tersebut harus pasti terjadi.

   c. Kesengajaan dengan kesadaran kemungkinan, kesengajaan dengan gradasi terendah, bahkan sering sukar untuk membedakan dengan kealpaan. Sandarannya adalah sejauh mana pengetahuan pelaku tentang akibat dan tindakan yang dilarang beserta tindakan lainnya yang mungkin akan terjadi.

---

[21] R. Soesilo, ***KUHP dan Komentar Pasal demi Pasal***, Politea, Bogor, 1996, h. 144

2. unsur menghancurkan, merusakan, membikin tak dapat dipakai atau menghilangkan barang.

   "Menghancurkan" pada kasus penyalahgunaan komputer adalah perbuatan menghancurkan disket dan sejenisnya yang berisikan data atau program komputer sehingga data atau program yang ada di dalamnya menjadi hancur dan tidak dapat dimanfaatkan lagi.

   "Merusakan" pada kasus penyalahgunaan komputer adalah hampir sama dengan "menghancurkan", perbedaannya adalah disket tersebut menjadi cacat data, adanya tambahan data baru, adanya pengacauan data (mengacak-acak data).

   "Membuat tidak dapat dipaki lagi" pada kasus penyalahgunaan komputer adalah perbuatan sedemikian rupa sehingga data atau program komputer yang seharusnya dapa dimanfaatkan sesuai dengan fungsinya menjadi tidak dapat digunakan atau dimanfaatkan karena dihapus, dirusak, diacak ataupun dikacaukan.

   "Menghilangkan barang" dalam penyalahgunaan komputer adalah perbuatan menghilangkan atau menghapuskan data atau program yang tersimpan di dalam disket dan media penyimpanan lainnya sehingga mengakibatkan semua data atau informasi yang disimpan menjadi hapus sama sekali.

3. adanya barang milik orang lain

   Yang dalam hal ini adalah media disket atau media penyimpan sejenis lainnya, yang dihancurkan atau dirusak sehingga barang (data atau program) menjadi tidak berfungsi atau tidak dapat dijalankan.

b. Di Luar KUHP

1.) Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Beberapa pasal dalam Undang-undang Nomor 36 Tahun 1999 dapat digunakan untuk menjerat pelaku tindak pidana perbankan dengan media internet. Rumusan Pasal 22 Undang-undang Nomor 36 Tahun 1999 mengatur tentang adanya larangan untuk memasuki suatu akses tanpa hak, yang uraian pasalnya adalah sebagai berikut:

1.) Pasal 22

Setiap orang dilarang keras untuk melakukan perbuatan tanpa hak, tidak sah atau memanipulasi:
a. akses ke jaringan telekomunikasi; dan atau
b. akses ke jasa telekomunikasi; dan atau
c. akses ke jaringan telekomunikasi khusus.

Sanksi atau hukuman yang dikenakan untuk larangan dalam pasal 22 diatas diatur di pasal 50 Undang-undang Nomor 36 Tahun 1999, yang berbunyi:

2.) Pasal 50

Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)

Ketentuan pasal 1 angka 6 Undang-undang Nomor 36 Tahun 1999 yang menjelaskan tentang arti jaringan telekomunikasi adalah:

Pasal 1 angka 6

Jaringan telekomunikasiadalah rangkaian perangkat telekomunikasi dan kelengkapannya yang digunakan dalam bertele komunikasi.

Dari pasal 1 angka 6 tersebut maka *internet* dalam hal ini adalah *internet banking* termasuk pada kategori jaringan telekomunikasi karena merupakan jaringan yang

terdapat pada komputer yang dari jaringan tersebut dapat dilakukan telekomunikasi melalui komputer.

2.) Undang-undang Nomor 10 Tahun 1998 jo. Undang-undang Nomor 7 Tahun 1992 tentang Perbankan

Ada beberapa ketentuan yang dapat dikenakan dalam kejahatan yang berupa *Data Leakage* yaitu berkaitan dengan "pembocoran" data rahasia. Data rahasia dalam kejahatan ini dapat berupa rahasia yang harus dirahasiakan oleh bank.

Kejahatan mengenai rahasia bank dalam Undang-undang Nomor 10 Tahun 1998 jo. Undang-undang Nomor 7 Tahun 1992 tentang Perbankan diatur dalam Pasal 40 ayat (1), berikut kutipan pasal tersebut:

1.) Pasal 40 ayat (1)

> Bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44 dan Pasal 44A.

Ketentuan Pasal 40 tersebut mewajibkan Bank dan juga pihak terafiliasi (Pasal 40 ayat [2]) untuk merahasiakan keterangan tentang nasabah penyimpan dan simpanannya. Pasal 40 juga menyebutkan adanya pengecualian dalam menyimpan rahasia tersebut. Pengecualian tersebut berkaitan dengan:

1. Untuk kepentingan perpajakan (Pasal 41);
2. Untuk penyelesaian piutang bank yang sudah diserahkan kepada Badan Urusan Piutang dan Lelang Negara atau Panitia Urusan Piutang Negara (Pasal 41A);
3. Untuk kepentingan peradilan dalam perkara pidana (Pasal 42);

4. Dalam perkara perdata antara Bank dengan nasabahnya (Pasal 43);
5. Dalam rangka tukar menukar informasi antar bank (Pasal 44);
6. Atas permintaan, persetujuan atau kuasa dari nasabah penyimpan yang dibuat secara tertulis (Pasal 44A).

Selain untuk ke enam alasan di atas, bank tidak dapat mengungkapkan keterangan yang berupa rahasia bank. Sanksi untuk pelanggaran rahasia bank diatur dalam Pasal 47, yang bunyi pasalnya adalah:

> Pasal 47
>
> Ayat (1). Barang siapa tanpa membawa perintah tertulis atau ijin dari Pimpinan bank Indonesia sebagaimana dimaksud dalam pasal 41, pasal 41A dan pasal 42, dengan sengaja memaksa bank atau pihak terafiliasi untuk memberikan keterangan sebagaimana dimaksud dalam pasal 40, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun dan paling lama 4 (empat)tahun serta denda sekurang-kurangnya Rp 10.000.000.000,00 (Sepuluh Miliar Rupiah) dan paling banyak Rp 200.000.000.000,00 (Dua Ratus Miliar Rupiah).
>
> Ayat (2). Anggota dewan komisaris, direksi, pegawai bank atau pihak terafiliasi lainnya yang dengan sengaja memberikan keterangan yang wajib dirahasiakan menurut pasal 40, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun dan paling lama 4 (empat) tahun serta denda sekuramg-kurangnya Rp 4.000.000.000,00 (Empat Miliar Rupiah) dan paling banyak Rp 8.000.000.000,00 (Delapan Miliar Rupiah).

Ketentuan Pasal 40 dan Pasal 47 diatas dapat digunakan untuk bentuk kejahatan *internet* berupa *data leakage* karena bentuk kejahatan ini berhubungan dengan rahasia bank.

Kejahatan internet lainnya yang dapat dikenakan ketentuan dalam Undang-undang Nomor 10 Tahun 1998 jo. Undang-undang Nomor 7 Tahun 1992 tentang Perbankan adalah *Data Diddling* yaitu mengubah data valid atau sah pada

saat pemasukan data atau informasi (*input*) atau pada saat pengeluaran data (*output*) dalam pengoperasian komputer.

Data Diddling ini dapat dikenakan ketentuan dalam pasal 49 ayat (1) huruf c Undang-undang Nomor 10 Tahun 1998 jo. Undang-undang Nomor 7 Tahun 1992 tentang Perbankan, yang uraiannya sebagai berikut:

> Pasal 49 ayat (1) huruf c
>
> Mengubah, mengaburkan, menyembunyikan, menghapus, atau menghilangkan adanya suatu pencatatan dalam pembukuan atu dalam laporan, maupun dalam dokumen atau laporankegiatan usaha, laporan transaksi atau rekening suatu bank, atau dengan sengaja mengubah, mangaburkan, menghilangkan, menyembunyikan atau merusak catatan pembukuan tersebut,
> diancam dengan pidana penjara sekurang-kurangnya 5 (lima) tahun dan paling lama 15 (lima belas) tahunserta denda sekurang-kurangnya Rp 10.000.000.000,00 (sepuluh miliar rupiah) dan paling banyak Rp 200.000.000.000,00 (dua ratus miliar rupiah).

Pasal 49 ayat (1) huruf c di atas dapat digunakan untuk kejahatan *data diddling* karena dalam kejahatan ini terdapat adanyaupaya untuk mengubah suatu pencatatan (dalam hal ini adalah data valid atau sah) yang dilakukan dengan media komputer atau internet.

Kejahatan dalam bidang perbankan dengan media *internet* tersebut memiliki unsur-unsur yang sama dengan bentuk-bentuk kejahatan yang diatur dalam ketentuan hukum pidana yang sudah ada. Perbedaannya terletak pada media yang digunakan yaitu media *internet* pada kejahatan di dunia maya (*cyber space*), sedangkan ketentuan hukum pidana yang ada lebih pada kejahatan di dunia nyata.

Ketentuan hukum konvensional dari uraian sebelumnya dapat digunakan untuk menyelesaikan kasus-kasus pidana di bidang perbankan yang menggunakan

media internet, dan di lain pihak kita dapat terus mengkaji bentuk hukum yang tepat untuk mengantisipasi munculnya kasus-kasus *internet banking* yang tiap hari terus bertambah di Indonesia.

Belum adanya pengaturan secara khusus tentang kejahatan tersebut tidak menyebabkan para pelaku kejahatan dalam dunia perbankan dengan media *internet* dapat leluasa menjalankan aksinya. Hal ini dikarenakan untuk saat ini, sistem hukum konvensional untuk sementara waktu dapat digunakan untuk menangani kasus-kasus yang ada.

BAB III

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA PERBANKAN DENGAN MEDIA INTERNET

1. Penyelidikan dan Penyidikan dalam Kasus Tindak Pidana Perbankan dengan Media Internet

Penyelidikan dan penyidikan dalam hukum pidana di Indonesia menggunakan Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (yang selanjutnya disebut KUHAP) sebagai hukum acaranya. Penyelidikan menurut ketentuan Pasal 1 butir 5 KUHAP berarti serangkaian tindakan mencari dan menemukan suatu keadaan atau peristiwa yang berhubungan dengan keadaan kejahatan atau pelanggaran tindak pidana atau yang diduga sebagai perbuatan pidana.[22]

Proses penyidikan dilakukan oleh penyidik yang diatur dalam Pasal 1 angka 1 KUHAP yang berbunyi:

> Pasal 1 angka 1
>
> Penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan.

---

[22] Yahya Harahap,***Pembahasan, Permasalahan dan Penerapan KUHAP penyidikan dan penuntutan***, Edisi ke 2, Cet. 5, Sinar Grafika, Jakarta, 2003, h.101

Hal ini diperinci dan di pertegas lagi dalam Pasal 6 ayat (1) KUHAP yang isinya:

Pasal 6 ayat (1)

Penyidik adalah:
a. Pejabat polisi negara Republik Indonesia;
b. Pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang.

Masalah jurisdiksi menjadi sangat penting dalam penyelidikan dan penyidikan kasus kejahatan internet, khususnya dalam bidang perbankan. Hal ini disebabkan karena menyangkut kewenangan kepolisian untuk melakukan penyelidikan dan penyidikan.

Permasalahan jurisdiksi ini dapat kita lihat dari ruang lingkup berlakunya KUHAP, yang hal ini diatur dalam Pasal 2 KUHAP beserta penjelasannya, uraiannya sebagai berikut:

Pasal 2

Undang-undang ini berlaku untuk melaksanakan tata cara peradilan dalam lingkungan peradilan umum pada semua tingkat peradilan.

Penjelasan Pasal 2

a. Ruang lingkup undang-undang ini mengikuti asas-asas yang dianut oleh hukum pidana Indonesia.
b. Yang dimaksud dengan "peradilan umum" termasuk pengkhususannya sebagaimana tercantum dalam penjelasan pasal 10 ayat (1) alinea terakhir Undang-undang Nomor 14 tahun 1970.

Dari uraian di atas, khususnya Penjelasan Pasal 2 huruf a, memiliki pengertian semua hukum pidana Indonesia termasuk hukum pidana khusus, sepanjang hukum pidana khusus itu mengandung asas-asas daya jangkau berlakunya berupa asas khusus di luar KUHP.[23]

---

[23] ***Ibid.***, h.86

Ruang lingkup berlakunya KUHAP tersebut meliputi ruang lingkup yang terdapat dalam Pasal 2 sampai dengan Pasal 9 KUHP, yang deapat dibagi menjadi beberapa asas yaitu asas teritorial, asas personalitas/nasional aktif, asas perlindungan/nasional pasif dan asas universal. [24]

Asas-asas di atas berkaitan dengan jurisdiksi tradisional yang mempunyai "batas-batas" tertentu. Jurisdiksi tradisional ini akan menjadi kendala sehubungan dengan aktifitas *online* di ruang *cyber* yang tidak mengenal batas.

Media internet tidak mengenal batas-batas wilayah. Permasalahan jurisdiksi dalam media internet menjadi sangat rumit daripada masalah jurisdiksi pada peradilan biasa. Penentuan jurisdiksi personal, meskipun belum banyak kasus yang terjadi, di Amerika Serikat telah diperkenalkan suatu test untuk penentuan jurisdiksi personal situs web internet, yaitu dengan menilai aktivitas suatu situs web. Aktivitas ini diukur dengan mempertimbangkan apakah kegiatan di suatu lokasi merupakan kegiatan interaktik atau pasif.

Situs web dikategorikan melakukan kegiatan interaktif apabila melalui situs web tersebut dilakukan komunikasi *on-line* 2 (dua) arah untuk mengadakan transaksi bisnis atau dilakukan pertukaran informasi antar penggunanya untuk kepentingan bisnis. Situs web internet tidak dapat dikategorikan interaktif bila hanya memuat suatu iklan saja atau hanya digunakan untuk melakukan *browsing* atas informasi yang disediakan. Situs web yang hanya menyediakan informasi saja dikategorikan pasif.

---

[24] Moeljatno, *op. cit.* h. 41-44

Barda Nawawi Arief dalam bukunya yang berjudul *"Kapita Selekta Hukum Pidana"* mengusulkan untuk memberlakukan prinsip ubikuitas atau asas universal dalam menghadapi kejahatan di dunia maya *(cyber crime)*. Prinsip ubikuitas adalah prinsip yang menyatakan bahwa delik-delik yang dilakukan atau terjadi di sebagian wilayah teritorial negara dan sebagaian di luar wilayah teritorial suatu negara (ekstrateritorial) harus dapat dibawa ke dalam jurisdiksi setiap negara yang terkait.[25]

Asas universal yang telah dianut dalam KUHP kita lebih menekankan pada jenis kejahatan internasional, sehingga setiap negara yang berkepentingan dapat menerapkannya sepanjang kejahatan tersebut tergolong sebagai kejahatan internasional. Permasalahannya adalah kejahatan internet, khususnya dalam bidang perbankan, belum dikategorikan sebagai kejahatan internasional. Jalan keluar satu-satunya untuk mengatasi masalah jurisdiksi adalah dengan mengadakan perjanjian internasional mengenai kejahatan ini. Masalah jurisdiksi akan semakin sulit ditentukan jika pelaku tidak diketahui.

Kepolisian Republik Indonesia (Polri) sudah melakukan tindakan yang konkret untuk menghadapi kejahatan di dunia maya *(cyber crime)* yang semakin meningkat. Polri telah meluncurkan prototipe komputer forensik untuk mendukung kinerja dari penyidik Polri dalam menangani *cyber crime*.[26]

Pengertian penyidik di atas jika dikaitkan dengan dibentuknya komputer forensik yang khusus menangani kejahatan internet (*cyber crime*) akan

---

[25] Barda Nawawi Arief, ***Kapita Selekta Hukum Pidana***, Rajawali Press, Jakarta, h. 253

[26] *"Polri akan luncurkan Prototipe Komputer Forensik"*, **www.hukumonline.com**, 13 Mei 2002.

menimbulkan kendala. Kewenangan komputer forensik yang digagas oleh Irjendpol Drs Didi Widayati di Kapuspen Polri hingga saat ini belum sampai ke taraf penyidikan.

Mentahnya hasil penyelidikan yang telah diperoleh oleh forensik komputer tersebut disebabkan oleh sistem kerja dari polri yang terfragmentasi oleh satuan kerja. Tidak adanya kewenangan untuk melanjutkan ke taraf penyidikan menjadikan badan ini tidak berfungsi secara optimal. Hal ini disampaikan oleh Kombes Alfons LM, SH pada *hukumonline* di ruang kerjanya. Selama ini, apa yang dilakukan forensik komputer hanya sebatas mengumpulkan dan menginventarisasi bukti awal guna diserahkan kepada dinas reserse atau intel Polri. "Padahal sejak pertama digagas, badan ini juga berkompeten untuk melakukan ke tahap penyidikan," ujar Alfons.[27]

Kepolisian Daerah Jawa Timur (Polda Jatim) saat memiliki unit khusus yang menangani kejahatan internet yaitu Unit Cyber Crime Polda Jatim. Hal ini menjadi salah satu jalan keluar jika dikaitkan dengan tidak berwenangnya Forensik Komputer Polri dalam melakukan penyidikan.

Masalah lain yang menjadi kendala dalam proses penyelidikan dan penuntutan adalah alat bukti yang ada dalam KUHAP dikaitkan dengan alat bukti yang ditemukan dalam kejahatan dengan media internet dalam bidang perbankan. Walaupun perbuatan atau tindakan yang dilakukan itu dapat ditarik dengan mengacu pada KUHP atau ketentuan-ketentuan hukum pidana yang lainnya, tetapi hal ini masih "terbentur" dengan hukum acara pidana kita yang belum mengatur

---

[27] *Forensik Komputer Polri Tidak Punya Kewenangan Menyidik*, http://www.hukumonline.com, Mei 2001.

mengenai alat bukti elektronik sebagai alat bukti yang sah. Alat bukti yang sah dalam KUHAP diatur dalam Pasal 184 ayat (1) KUHAP, yang berbunyi:

> Pasal 184 ayat (1)
>
> Alat bukti yang sah ialah:
> a. Keterangan saksi;
> b. Keterangan ahli;
> c. Surat;
> d. Petunjuk;
> e. Keterangan terdakwa.

Alat bukti berupa keterangan saksi dalam tindak pidana dengan media internet, kemungkinan ditemukannya saksi yang mengetahui pelaku melakukan tindak pidana sangatlah sulit. Hal ini dikaitkan dengan persyaratan bagi seorang saksi yaitu orang yang melihat, mendengar atau mengalami sendiri suatu tindak pidana. Hal ini sesuai dengan ketentuan Pasal 1 butir 26 KUHAP, yang uraiannya sebagai berikut:

> Pasal 1 butir 26
>
> Saksi adalah orang yang dapat memberikan keterangan guna kepentingan penyidikan, penuntutan, dan peradilan tentang suatu perkara pidana yang ia dengar sendiri, ia lihat sendiri dan ia alami sendiri.

Adanya saksi dimungkinkan jika pelaku memiliki kedekatan dengan orang yang memiliki kemampuan yang sama atau dapat juga orang-orang di sekitar pelaku sudah mengetahui (telah menjadi rahasia umum), maka ia dapat diminta keterangannya sebagai saksi.

Pelaku dalam *cyber crime* itu bersifat *virtual*, sehingga keterangan yang diberikan oleh para saksi atas suatu tindakan diperoleh secara tidak langsung. Dalam hukum acara pidana kita dikenal dengan *testimonium de auditu* atau

hearsay evidence yaitu keterangan saksi yang diperoleh atau didapat dari orang lain dan kesaksian yang demikian ini tidak diperkenankan sebagai alat bukti.[28]

Alat bukti berupa keterangan saksi ahli dalam tindak pidana dengan media internet merupakan suatu yang tidak dapat di tawar-tawar lagi, mengingat metode dan cara-cara yang dilakukan memiliki karakter yang berbeda dengan tindak pidana biasa.

Sebelum tiba pada taraf pembuktian atau pencarian alat atau barang bukti, harus dilakukan suatu *due diligent* terhadap sistem komputer. Hasil pemeriksaan awal atas keabsahan suatu sistem komputer ini adalah diperolehnya jaminan bahwa sistem tersebut dapat dikatakan otentik dan dapat dipertanggungjawabkan. Untuk mengambil suatu keputusan atau kesimpulan pembuktian alat bukti elektronik itu agar memiliki kekuatan pembuktian maka masih diperlukan keterangan seorang saksi ahli.

Kedudukan seorang saksi ahli dalam menerangkan atau menjelaskan alat bukti elektronik akan sangat penting dalam memberikan kenyakinan pada hakim dalam memutus perkara. Peran seorang ahli adalah memberikan penjelasan bahwa data elektronik tersebut adalah sah dan dapat dipertanggungjawabkan secara hukum.

Alat bukti surat yang akan mengarahkan suatu peristiwa pidana dalam kejahatan dengan media internet adalah berupa data-data elektronik baik yang berada di dalam komputer itu sendiri (*hard disc* atau *floopy disc*) atau yang

---

[28] Yahya Harahap, ***Hukum Acara Pidana di Indonesia***, CV. Sapta Arta Jaya, Jakarta, h. 273

merupakan hasil *print out* atau dalam bentuk lain yang berupa jejak (*path*) dari suatu aktivitas penggunaan internet.[29]

Tidak adanya pengakuan data elektronik sebagai salah satu alat bukti yang sah tersebut bertolak belakang dengan praktek bisnis di Indonesia. Misalnya dalam transaksi ekspor dan impor (antar negara), Indonesia sudah menggunakan teknologi EDI (*Elektronik Data Interchange*), selain itu juga terdapat EFT (*Electronic Funds Transfer*) yang keduanya diperkenalkan pertama kalinya di akhir tahun 1970-an.[30] Namun anehnya, pengadilan sendiri (dalam hal ini sesuai Hukum Acara Pidana kita) belum menerima bukti elektronik tersebut sebagai alat bukti yang sah di pengadilan.

Alat bukti petunjuk dalam kejahatan dengan media internet diperoleh dengan batasan tiga hal yaitu keterangan saksi, surat dan keterangan terdakwa. Hal ini sesuai dengan ketentuan Pasal 188 ayat (2) KUHAP yang uraiannya sebagai berikut:

> Pasal 188 ayat (2)
>
> Petunjuk sebagaimana yang dimaksud dalam ayat 1 hanya dapat diperoleh dari:
> a. Keterangan saksi;
> b. Surat;
> c. Keterangan terdakwa.

Mewujudkan suatu petunjuk dari bukti-bukti yang ditemukan dalam kejahatan dengan media internet akan sangat sulit jika kita melandasi pada ketiga sumber petunjuk yang ada dalam KUHAP tersebut.

---

[29] Edmon Makarim, ***Kompilasi Hukum Telematika***, Edisi I, Cet. 1, PT. Raja Grafindo Persada, Jakarta, 2003, h. 423

[30] ***Ibid.***, h. 226.

Proses pembuktian merupakan suatu upaya untuk memperoleh kebenaran sejati (materiil) terhadap:[31]

a. Perbuatan-perbuatan manakah yang dianggap terbukti menurut pemeriksaan pemeriksaan persidangan.
b. Apakah telah terbukti bahwa terdakwa bersalah atas perbuatan-perbuatan yang didakwakan kepadanya.
c. Tindak pidana apakah yang dilakukan sehubungan dengan perbuatan-perbuatan itu.
d. Hukuman apakah yang harus dijatuhkan kepada terdakwa.

Kebenaran sejati dalam kejahatan dengan media internet di bidang perbankan khususnya bukanlah pekerjaan yang mudah untuk memperolehnya.

Proses pembuktian dalam konteks hukum pidana merupakan bagian yang essensial untuk membuktikan atau menyatakan bahwa seseorang telah melakukan suatu tindak pidana. Dari hasil pemeriksaan dalam persidangan dapat menimbulkan 3 (tiga) kemungkinan putusan hakim atau majelis hakim.

Kemungkinan pertama, jika pengadilan (dalam hal ini hakim atau majelis hakim) berpendapat bahwa hasil pemeriksaan di sidang, kesalahan terdakwa atas perbuatan yang didakwakan kepadanya tidak terbukti secara sah dan menyakinkan maka terdakwa diputus bebas.

Kemungkinan kedua, jika pengadilan berpendapat bahwa perbuatan yang didakwakan kepada terdakwa terbukti, tetapi perbuatan itu tidak merupakan suatu tindak pidana, maka terdakwa diputus lepas dari segala tuntutan hukum.

---

[31] Martiman Prodjohamidjojo, ***Pembahasan Hukum Acara Pidana dalam Teori dan Praktek***, Cet. 1, Pradnya Paramita, Jakarta, 1989, h. 133

Kemungkinan ketiga, jika hakim atau majelis hakim berpendapat bahwa dari hasil pemeriksaan sidang, kesalahan terdakwa atas perbuatan yang didakwakan kepadanya terbukti secara sah dan menyakinkan maka terdakwa diputus bersalah dan dipidana.

Proses pembuktian di lihat dari uraian di atas, mempunyai kedudukan yang sangat penting untuk menentukan nasib seorang terdakwa. Bersalah atau tidaknya seorang terdakwa ditentukan pada proses pembuktian.

Peran serta aktif hakim sangat diperlukan untuk menangani dan mengatasi masalah pembuktian ini. Peran serta ini dikaitkan dengan ketentuan Pasal 6 Undang-undang Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman, yang masing-masing berbunyi:

> Pasal 6
>
> Tidak seorang pun dapat dihadapkan di depan pengadilan selain daripada yang ditentukan oleh undang-undang.
> Tidak seorang pun dapat dijatuhi pidana, kecuali apabila pengadilan, karena alat pembuktian yang sah menurut undang-undang, mendapat keyakinan bahwa seseorang yang dianggap dapat bertanggung jawab, telah bersalah atas perbuatan yang didakwakan atas dirinya.

Dari ketentuan di atas, seseorang dapat dijatuhi pidana jika pengadilan berdasarkan alat bukti yang sah menurut undang-undang mendapat kenyakinan bahwa ia bersalah atas perbuatan yang didakwakan kepadanya. Tumpuan utama dalam ketentuan Pasal 6 Undang- Undang Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman adalah karena alat pembuktian yang sah menurut undang-undang. Alat bukti elektronik yang terdapat dalam kejahatan di dunia maya bukan merupakan alat bukti yang sah menurut KUHAP yang saat ini digunakan sebagai hukum acara pidana di Indonesia.

Ketentuan Pasal 6 Undang- undang Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman tersebut sejalan dan sesuai dengan ketentuan Pasal 1 ayat (1) KUHP yang mengatur tentang asas legalitas. Hal ini akan menjadi kendala dalam upaya penanganan tindak pidana perbankan dengan media internet khususnya di depan persidangan, karena seperti yang dijelaskan sebelumnya bahwa dalam kejahatan dengan media internet, alat bukti yang ada berupa alat bukti elektronik.

2. Kendala yang Dihadapi dalam Menangani Kasus Tindak Pidana Perbankan dengan Media Internet

Kasus yang saat ini ditangani oleh Kepolisian Daerah Jawa Timur (Polda Jatim) belum sampai pada tingkat penuntutan. Ada tiga perkara yang saat ini ditangani Polda Jatim, antara lain:[32]

Laporan dari Kepolisian Wilayah Malang, yaitu berupa penipuan dengan menggunakan nomor kartu kredit orang lain yang dilakukan melalui internet untuk membeli suatu barang melalui layanan *E-Commerce*. Pihak pelapor dalam kasus ini adalah warga negara asing yaitu warga negara Jerman.

Laporan ke dua adalah perkara yang ditangani oleh Polresta Malang, kasus ini hampir sama dengan yang terjadi di Kepolisian Wilayah Malang. Perbedaan terletak pada pelapor, pelapor dalam perkara yang ditangani Polresta Malang adalah warga negara Indonesia.

---

[32] ***Wawancara dengan Bapak Partoyo***, Kanit II Tindak Pidana Ekonomi Polda Jatim, 19 Juli 2004.

Laporan ke tiga adalah perkara yang ditangani oleh Kepolisian Wilayah Madiun, yaitu penipuan dengan media SMS (*Short Massege Send*). Tindakan ini dilakukan dengan mengirim SMS kepada korban yang menyatakan bahwa dia memenangkan sebuah hadiah dari suatu undian. Hadiah tersebut dapat dikirimkan dengan syarat korban diharuskan untuk mentransfer sejumlah uang. Kasus ini dapat dikategorikan kejahatan dengan media internet, jika korban dalam mentrasfer dana menggunakan layanan *internet banking*.

Kasus-kasus yang ditangani tersebut, sampai saat tulisan ini dibuat, masih dalam tahap pemeriksaan di tingkat penyidikan. Lamanya penanganan kasus tersebut berkaitan dengan kendala-kendala yang dihadapi dalam tingkat penyidikan. Kendala-kendala tersebut antara lain:[33]

1. Jika berkaitan dengan pelapor yang merupakan warga negara asing yang berdomisili di luar negeri.

   Untuk memanggil pihak pelapor untuk diperiksa sebagai saksi oleh penyidik atau dalam pemeriksaan di depan sidang, memerlukan prosedur dan waktu yang lama.

   Kepolisian Malang dalam kasus di atas akan melaporkan ke Kepolisian Daerah Jawa Timur. Laporan ini akan dilanjutkan ke Interpol, dari interpol baru disampaikan kepada yang bersangkutan.

2. Jika pelaku berada di luar negeri dan akibatnya dirasakan Indonesia.

   Pemerintah Indonesia baru dapat menangani kasus ini, jika sudah ada perjanjian ekstradisi antara Indonesia dengan negara tempat tersangka berada.

---

[33] ***Ibid.***

3. Kendala yang berkaitan dengan bukti berupa hasil *print out* suatu sistem informasi.

   Penyidik dalam menggunakan hasil *print out* tersebut sebagai alat bukti, harus memastikan bahwa hasil *print out* tersebut adalah asli. Untuk mendapatkan kenyakinan tentang keaslian hasil *print out*, penyidik akan menanyakan kepada pihak yang mengeluarkan *print out* tersebut apakah hasil *print out* yang diperoleh polisi tersebut isinya masih asli, jika benar maka hasil *print out* tersebut baru digunakan sebagai alat bukti.

4. Informasi yang dibutuhkan akan sulit di dapat jika berhubungan dengan rahasia bank.

   Informasi yang berkaitan dengan rahasia bank harus melalui prosedur yang memerlukan waktu yang lama karena harus atas ijin Bank Indonesia.

BAB IV

PENUTUP

1. Simpulan

a. Ketentuan hukum pidana yang ada di Indonesia dapat digunakan untuk menangani bentuk tindak pidana yang menggunakan media internet. Tindak pidana yang berkaitan dengan media informasi ini memiliki unsur-unsur yang sama dengan bentuk tindak pidana yang diatur dalam ketentuan hukum pidana yang ada. Perbedaannya terletak pada sarana yang digunakan untuk melakukan tindak pidana yaitu dengan media internet yang dalam bidang perbankan diwujudkan dalam layanan *internet banking*.

b. Penegakan hukum dalam tindak pidana perbankan dengan media internet dalam prakteknya, banyak kendala-kendala yang dihadapi oleh aparat penegak hukum. Kendala yang dihadapi menyebabkan proses pemeriksaan menjadi lama dan memerlukan biaya yang banyak. Kendala utama yang dihadapi adalah berkaitan dengan alat bukti yang ditemukan dalam tindak pidana dengan media internet dalam media perbankan dikaitkan dengan alat bukti yang diakui dalam KUHAP.

2. Saran

a. Perlu adanya kriminalisasi terhadap kejahatan komputer (*Computer Related Crime*, baik yang berupa aturan umum (*general rules*) yang berada di dalam KUHP (Buku I) maupun aturan khusus (*special rules*) yang berada di dalam KUHP (Buku II dan Buku III) dan dalam undang-undang khusus di luar KUHP khususnya dalam bidang perbankan.

b. Perlu adanya pengaturan baru tentang hukum acara pidana yang tepat untuk menangani kasus-kasus tindak pidana dengan media internet di dunia *cyber*, agar penegakan hukum dapat dilakukan secara maksimal.

DAFTAR BACAAN

Buku:

Febrian, Jack dan Farida Andayani, *Kamus Komputer dan Istilah Teknologi Informasi*, Informatika, Bandung, 2002.

Hadiati Koeswadji, Hermien et al, *Delik harta kekayaan, asas-asas, kasus dan Permasalahannya*, Cet. I, Sinar Wijaya, Surabaya,1984.

Harahap, Yahya, *Pembahasan Permasalahan dan Penerapan KUHAP*, Penyidikan dan Penuntutan, Edisi Kedua, Cet.5, Sinar Grafika, Jakarta, 2003.

_____, *Hukum Acara Pidana di Indonesia*, CV. Sapta Arta Jaya, Jakarta.

Makarim, Edmon, *Kompilasi Hukum Telematika*, Edisi I, Cet. 1, PT. Raja Grafindo Persada, Jakarta, 2003.

Moeljatno, *Asas-asas Hukum Pidana*, Cet. 6, Rineka Cipta, Jakarta, 2000.

Nawawi Arief, Barda, *Kapita Selekta Hukum Pidana*, Rajawali Press, Jakarta

Prodjohamidjojo, Martiman, *Pembahasan Hukum Acara Pidana dalam Teori dan Praktek*, Cet. 1, Pradnya Paramita, Jakarta, 1989.

Raharjo, Agus, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Cet.I, Citra Aditya Bakti, Bandung, 2002.

Riswandi, Budi Agus, *Hukum dan Internet di Indonesia*, Cet. I, UII Press, Yogyakarta, April 2003.

Siregar, Ashadi, *"Membaca Surat Kabar Digital, Membaca Wajah Populis Teknologi Media"*, Kompas, 28 Juni 2000.

Sitompul, Asrul, *Hukum Internet (Pengenalan Mengenai Masalah Hukum di Cyberspace)*, Cet. I, Citra Aditya Bakti, Bandung, 2001.

Makalah:

Mahendra, Yusril Ihza, "Regulasi Cyberspace di Indonesia", Makalah "Cyber Law", Yayasan Cipta Bangsa, Badung, 29 Juli 2000.

Sabirin, Syahril, "Urgensi Regulasi dalam Internet banking", Seminar Sehari "Aspek hukum internet banking dalam kerangka Hukum Teknologi Informasi", Universitas Padjajaran, Bandung, 13 Juli 2001.

Internet:

FAQ, *"Apakah Aman Bertransaksi Lewat Warnet?"*, **http://www.lippobank.co.id/faq.html.**

Forensik Komputer Polri Tidak Punya Kewenangan Menyidik, **http://www.hukumonline.com, Mei 2001.**

http://www.hukumonline.com/artikel detail.asp?id=7136

I Made Wiryana dan Tedi Heryanto, *"Resiko Internet Banking telah Tampak"*, **http://www.tedi-h.com/papers/i-banking.html.**

Modus Operandi Cybercrime di Indonesia Makin Canggih, **www. hukumonline.com**, 3 Januari 2003.

Nur Raihan dan Sigit Widodo, http://www.detik.com.

Peraturan Perundang-undangan:

Kitab Undang-undang Hukum Pidana (KUHP)

Undang undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana

Undang-undang Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman

Undang-undang Nomor 7 tahun 1992 jo. Undang-undang Nomor 10 tahun 1998 tentang Perbankan

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Surat Keputusan Direksi Bank Indonesia Nomor 27/164/Kep/Dir tanggal 31 Maret 1995

Surat Edaran Bank Indonesia Nomor 27/9/UPPB tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank