BAB III
PROSES PEMBUKTIAN SECARA ELEKTRONIK PADA PERADILAN PERKARA *CYBERCRIME* DI INDONESIA

A. Proses Pembuktian Pada Perkara *Cybercrime*

Proses pembuktian adalah suatu hal yang sangat penting dalam suatu peradilan, karena merupakan pertimbangan hakim dalam memutuskan suatu perkara. Hasil pembuktian menjadi salah satu faktor penentu bagi sebuah putusan hakim, begitu pula dalam perkara pidana yang terjadi atau dilakukan melalui dan atau menggunakan media teknologi informasi atau dikenal dengan sebutan *cybercrime*, proses pembuktian menjadi penentu bagi seorang Terbukti atau tidaknya perbuatan terdakwa sebagai perbuatan pidana dan terbukti atau tidaknya unsur kesalahan terdakwa, sangat ditentukan oleh hasil pembuktian dalam perkara tersebut.

Pada praktiknya proses pembuktian pada perkara *cybercrime* tetap mengikuti ketentuan hukum mengenai pembuktian secara umum dalam perkara pidana. Sampai saat ini belum ada ketentuan yang secara khusus mengatur tentang proses pembuktian secara elektronik pada perkara *cybercrime*. Sistem pembuktian yang dianut oleh KUHAP adalah sistem pembuktian menurut undang-undang secara negatif, karena merupakan perpaduan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *Conviction in Time Theory*. Hal ini terlihat dari ketentuan Pasal 183 KUHAP yang menegaskan bahwa hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah diperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya.

Berbicara mengenai proses pembuktian tidak akan terlepas dari pembahasan tentang alat bukti. Ketentuan yang digunakan saat ini dalam pembuktian pada perkara *cybercrime* mendasarkan pada ketentuan Pasal 5 ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang antara lain menyatakan bahwa informasi dan atau dokumen elektronik dianggap sebagai alat bukti yang sah dan dianggap sebagai perluasan dari ketentuan mengenai alat bukti yang berlaku dalam hukum acara, dalam hal ini hukum acara pidana, yakni Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang menentukan alat-alat bukti yang sah dalam peradilan pidana yaitu :

1. Keterangan saksi;
2. Keterangan ahli;
3. Surat;
4. Petunjuk;
5. Keterangan terdakwa.

Melihat bahwa pada praktiknya proses pembuktian pada perkara *cybercrime* tetap mendasarkan pada ketentuan KUHAP, maka proses pembuktian dalam perkara *cybercrime* ini secara prinsip tidak berbeda dengan proses pembuktian biasa. Ada beberapa hal yang juga bersifat mendasar dalam proses pembuktian pada perkara *cybercrime* tersebut yang sangat berbeda dengan proses pembuktian pada perkara biasa. Berdasarkan ketentuan mengenai alat-alat bukti yang sah sebagaimana diatur dalam Pasal 184 KUHAP, proses pembuktian dapat diawali dari keterangan saksi. Keterangan saksi sebagai alat bukti pertama pada perkara pidana, akan sulit didapatkan pada perkara-perkara pidana yang melibatkan teknologi informasi (*cybercrime)*, karena segala sesuatu atau semua perbuatan pelaku dalam perkara tersebut tentu dilakukan di dunia maya dan perbuatan itu dapat dilakukan kapan pun, di manapun sekalipun hanya sendiri. Kondisi tersebut menimbulkan kesulitan dalam mendapatkan alat bukti berupa keterangan saksi pada perkara-perkara *cybercrime.* Ada beberapa perkara *cybercrime*, yang dimungkinkan adanya keterangan

saksi, yakni apabila pada saat melakukan sesuatu di tempat pelaku atau korban ditemani pihak lain yang memang tidak berkepentingan.

Alat bukti kedua adalah keterangan ahli, dalam perkara *cybercrime* sangat dibutuhkan, karena berdasarkan ilmu dan keahlian yang dimilikinya seseorang yang dianggap ahli di bidang tertentu akan diminta keterangannya untuk memperjelas sesuatu terkait perkara yang sedang diperiksa atau disidangkan. Pada perkara-perkara *cybercrime* keterangan ahli yang sangat dibutuhkan antara lain adalah keterangan dari ahli teknologi informasi, yang dapat memberi penjelasan tentang sesuatu yang terkait dengan perkara.

Alat bukti surat juga merupakan alat bukti yang sangat penting. Pada perkara *cybercrime* alat bukti surat yang dimaksud dapat berupa *paperless*, artinya surat elektronik atau informasi dan atau dokumen elektronik, sebagaimana dijelaskan dalam Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Berdasarkan Pasal 1 angka (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik disebutkan pula bahwa informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange (EDI)*, surat elektronik *(electronic mail)*, telegram, teleks, *telecopy*, atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Pasal 1 angka 4 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyebutkan bahwa yang dimaksud dengan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengan melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada

tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Proses pembuktian pada perkara *cybercrime* ini tentu saja tetap dapat dilakukan dengan mengajukan bukti surat berupa informasi dan atau dokumen elektronik tersebut yang dapat dilaksanakan langsung di persidangan dengan menyampaikan hasil *print out* informasi atau dokumen elektronik itu atau hakim dapat langsung mengakses informasi atau dokumen elektronik yang bersangkutan.

Berbicara mengenai alat bukti petunjuk, tidak terlepas dari ketentuan Pasal 188 (2) KUHAP yang membatasi kewenangan hakim dalam memperoleh alat bukti petunjuk, yang secara limitatif hanya dapat diperoleh dari [1]:

1. Keterangan saksi;
2. Surat;
3. Keterangan terdakwa.

Berdasarkan hal di atas, alat bukti petunjuk hanya dapat diambil dari ketiga alat bukti di atas. Pada umumnya, alat bukti petunjuk baru diperlukan apabila alat bukti lainnya belum mencukupi batas minimum pembuktian yang diatur dalam pasal 183 KUHAP di atas. Alat bukti petunjuk merupakan alat bukti yang bergantung pada alat bukti lainnya yakni alat bukti saksi, surat dan keterangan terdakwa. Alat bukti petunjuk memiliki kekuatan pembuktian yang sama dengan alat bukti lain, namun hakim tidak terikat atas kebenaran persesuaian yang diwujudkan oleh petunjuk, sehingga hakim bebas untuk menilai dan mempergunakannya dalam upaya pembuktian[2]. Petunjuk sebagai alat bukti tidak dapat berdiri sendiri membuktikan kesalahan terdakwa, karena hakim tetap terikat pada batas minimum pembuktian sesuai ketentuan Pasal 183 KUHAP. informasi dan/atau dokumen

[1] Munir Fuady, *Op.Cit*., hlm 294.
[2] M.Yahya Harahap, *Op.Cit.,*hlm. 296.

elektronik merupakan perluasan dari alat bukti surat sebagai bahan untuk dijadikan petunjuk bagi hakim dalam membuktikan suatu perkara.

Alat bukti terakhir dalam hukum acara pidana adalah keterangan terdakwa, dalam hal ini seorang terdakwa akan diminta keterangannya dalam persidangan untuk menemukan bukti-bukti apakah terdakwa memang bersalah telah melakukan perbuatan pidana yang didakwakan atau tidak. Seorang terdakwa walaupun memberikan keterangan yang tidak sebenarnya pun tetap dlindungi, berbeda dengan seorang saksi yang apabila memberikan keterangan yang tidak benar maka dapat dikenakan sanksi pidana telah memberikan keterangan palsu.

Proses pembuktian di persidangan dalam perkara *cybercrime* harus tetap mendasarkan pada ketentuan pembuktian Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan peraturan perundang-undangan lainnya seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

B. Perkara-Perkara *Cyber Crime* Di Indonesia

Ada beberapa perkara *cybercrime* yang terjadi di Indonesia dan pembuktian merupakan salah satu faktor penting yang diperlukan dalam mengadili perkara *cybercrime* tersebut, antara lain :

1. Kasus Artalyta Suryani sebagai tersangka pada tindak pidana percobaan penyuapan terhadap Jaksa Urip Tri Gunawan dalam rangka meloloskan Syamsul Nursalim sebagai Tersangka pada kasus BLBI Bank Dagang Nasional Indonesia, dengan cara meminta dikeluarkannya Surat Penghentian Penyelidikan Perkara (SP3) dan memang Kejaksaan Agung mengeluarkan SP3 tersebut, dalam hal ini KPK dapat mengungkap percobaan penyuapan itu dengan adanya bukti percakapan antara Artalyta Suryani dengan pejabat Kejaksaan Agung melalui telepon yang berhasil disadap oleh KPK, sehingga Artalyta dan Jaksa Urip Tri Gunawan dapat segera

ditangkap. Pada perkara ini harus dilihat sampai sejauh mana kewenangan KPK dapat melakukan penyadapan terhadap percakapan seseorang secara pribadi melalui fasilitas komunikasi ini, karena keabsahan kewenangan KPK ini menentukan pula keabsahan hasil penyadapan tersebut sebagai alat bukti.

2. Kasus lain yang ditangani KPK dengan cara melakukan penyadapan dalam penyelidikan dan penyidikannya, antara lain kasus Mulyana W. Kusumah yang saat itu diduga terlibat dalam tindakan penyuapan terhadap petugas Badan Pemeriksa Keuangan (BPK), yang mendapat tugas audit investigasi dari KPK pada tanggal 9 April 2005,
3. Kasus Al Amin Nasution sebagai anggota Komisi IV DPR RI yang terlibat kasus alih fungsi hutang lindung di Pulau Bintan, yang terhadapnya telah dilakukan penyadapan oleh KPK.
4. Beberapa kasus penyebaran virus komputer lainnya di tahun 2003, yaitu :
    a. Randon menyebarkan dirinya melalui *IRC chat channels* dan komputer yang dibagi dan terhubung di dalam sebuah jaringan. Virus tersebut mempunyai ciri-ciri yang khusus yaitu mempunyai *malicious code* yang merupakan sebuah dropper jenis *worm* yang menyusup pada beberapa file di komputer yang terinfeksi, beberapa di antaranya adalah virus yang mempunyai efek yang dapat berubah-rubah. A*ctions they carry out include opening ports, running applications, propagating dan memasukkan Denial of Service* (DoS) serta melakukan penyerangan, dan lain-lainnya. Randon dapat menghubungi ke web page dan mendownload sebuah backdoor jenis Trojan. Sebuah petunjuk kehadiran dari worm ini di dalam sebuah komputer adalah adanya peningkatan *network traffic* melalui ports 445 dan 6667.
    b. *Worm Lentin.P* menyebar melalui *e-mail* dalam sebuah *message* dengan ciri khas yang berubah-rubah. Virus ini juga memanfaatkan kelemahan pada *Internet*

Explorer versi 5.01 dan 5.5 yang akan bekerja secara automatis ketika message yang membawa *worm* ditampilkan melalui *Outlook Preview Pane*, yang menyebar melalui *network*, dan setiap hari Rabu akan mengcopikan dirinya sendiri pada komputer yang disharing di dalam sistem jaringan. *Lentin.P* mematikan program antivirus dan *firewall*, melancarkan dapat menyerang dengan menggunakan DoS, dan menutup *Windows Task Manager*.

4. Kasus *phishing* pun menimpa nasabah *Internet banking* Bank Niaga sejak Bulan Januari 2008 lalu.[3] Nasabah menerima *e-mail* dari Bank Niaga dengan subjek ”Website Niaga *Global Access* (NG@) Dlam Perbaikan Membutuhkan Verifikasi Anda". Modus serangannya terlihat dari isi surat elektronik tersebut yang mengharuskan penerima *e-mail* meng*klik link* alamat tertentu. Berikut isi surat elektronik yang dikirim oleh *phisher* :

   “Untuk mengantisipasi adanya kesalahan di dalam *database server* kami, mohon anda *login* ke *account* NiAGA Global@ccsess anda dan mengecek kebenaran Data Info yang ada. Silahkan klik di sini untuk mengakses NIAGA Global@ccsess atau klik LOGIN dibawah ini,"

   Apabila mengklik link tersebut, maka penerima akan dipandu untuk mengunjungi dan melakukan *login* ke situs NIAGA GLOBAL @CCESS palsu. Sekilas situs dengan alamat http://secure.bank2home.com.cn/ib-niaga/Log.html mirip dengan situs asli NIAGA GLOBAL @CCESS. Padahal, alamat asli NIAGA GLOBAL @CCESS adalah https://secure.bank2home.com/ib-niaga/ Login.html. Melalui pengisian menu login di situs NIAGA GLOBAL @CCESS palsu tersebut, maka pelaku *phishing* dapat memanfaatkannya data pribadi seperti nomor *Personal Identification Number* (PIN),

[3] http://web.bisnis.comedisi-cetakedisi-harianteknologi-informasi655687.html, diakses pada Tanggal 13 Maret 2010 pukul 23:00 WIB

Password atau rekening penerima *e-mail* melalui transaksi *Internet banking*. Alamat situs palsu berakhiran com.cn tersebut menunjukkan bahwa pelaku kejahatan memiliki *web server* di China. Akan tetapi, bisa jadi mereka juga melibatkan orang-orang dari Indonesia, karena surat elektronik tersebut ditulis dalam format bahasa Indonesia yang cukup tersusun rapi, setidak-tidaknya pelaku *phishing* itu melibatkan orang yang dapat berbahasa Indonesia.

Menurut *Electronic Delivery Group Head* PT Bank Niaga Tbk, pelaku phishing mengambil daftar alamat *e-mail* nasabah NIAGA GLOBAL @CCESS dari *mailing list*. Sasarannya dilakukan secara acak dari nasabah yang bergabung dalam komunitas *mailing list* dimulai sejak Januari 2008. Media *mailing list* tersebut bukan merupakan *maillist* internal nasabah Bank Niaga, melainkan *mailing list* eksternal yang dikuti para nasabah.

5. Kasus *phishing* di Indonesia lainnya dialami oleh pelanggan/pengguna situs internet banking milik Bank BCA yaitu “klikbca.com”. Pada tahun 2001, ada situs internet palsu yang sangat mirip penulisannya dengan situs klikbca.com, yaitu “kilkbca.com. Pada kasus ini terlihat calon korban tidak akan sadar bahwa salah tulis satu huruf saja akibatnya sangat fatal, akibatnya banyak pengguna *internet banking* Bank BCA memasukkan *username*, *password* dan nomor *Personal Identification Number* (PIN) ke dalam situs yang bukan seharusnya tersebut. Pemilik situs palsu dengan leluasa menggunakan identitas korban untuk masuk ke situs klikbca yang sebenarnya dan mentransfer seluruh uang korban ke rekening miliknya. Hal tersebut terjadi karena tampilan situs asli dan yang palsu persis sama, sehingga korban tidak akan sadar sama sekali.[4]

Melihat berbagai kasus *cybercrime* di atas, terdapat berbagai alat bukti elektronik yang dapat diungkapkan dalam persidangannya. Alat bukti elektronik termaksud antara lain :

[4] http://buletin.melsa.net.idjan1001phishing7.html, diakses pada Tanggal 13 Maret 2010, pukul 21:55 WIB

informasi elektonik, dokumen elektronik atau hasil penyadapan sebagai bagian dari teknologi informasi yang dapat dianggap sebagai alat bukti petunjuk. Semua alat bukti elektronik di atas diakui keabsahannya secara hukum dengan mendasarkan pada ketentuan Pasal 5 ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.