Pembuktian dalam Hukum Pidana Indonesia terhadap *Cyber Crime*

M. Yustia A.
Fakultas Hukum Universitas Bengkulu

Abstrak

Salah satu permasalahan yang dihadapi penegak hukum untuk menjerat pelaku tindak pidana mayantara (*cyber crime*) adalah masalah pembuktian tentang kesalahan terdakwa. Kenyataan tersebut menjadi suatu tantangan bagi kalangan penegak hukum untuk menyelesaikan segala persoalan yang terjadi akibat perkembangan teknologi yang sangat pesat. Permasalahan penelitian adalah bagaimana proses pembuktian kejahatan mayantara (*cyber crime*). Pendekatan normatif yang digunakan untuk memperoleh data sekunder melalui studi pustaka. Analisis data dilakukan dengan cara kualitatif. Hasil penelitian menunjukkan dalam mengungkapkan suatu kasus kejahatan mayantara (*cyber crime*) yang sangat rumit, kompleks, yang bersifat spesifik, keterangan ahli telematika sebagai alat bukti pada kejahatan mayantara (*cyber crime*) dalam proses peradilan pidana merupakan alat bukti yang sah menurut undang-undang. Berkaitan dengan permasalahan yang dibahas mengenai pembuktian tindak pidana *cyber crime* yang menggunakan sarana *internet* maka ketentuan hukum pembuktian yang dipakai tetap mengacu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kata Kunci*: pembuktian, kejahatan, mayantara*

I. PENDAHULUAN

Kemajuan teknologi informasi sekarang dan kemungkinannya di masa yang akan datang tidak lepas dari dorongan yang dilakukan oleh perkembangan teknologi komunikasi dan teknologi komputer. Perpaduan teknologi komunikasi dan teknologi komputer melahirkan internet yang menjadi tulang punggung teknologi informasi.

Internet merupakan sebuah dimensi baru dalam kehidupan manusia. Internet adalah sebuah alat penyebaran informasi secara global, sebuah mekanisme penyebaran informasi dan sebuah media untuk berkolaborasi dan berinteraksi antar-individu dengan menggunakan komputer tanpa terhalang batas geografis (Riyeke Ustadiyanto, 2001:1)

Perkembangan teknologi pada saat ini memunculkan berbagai media komunikasi yang sangat cepat dalam memberikan berbagai informasi dalam ruang dan waktu yang sangat singkat. Penemuan alat komunikasi berupa komputer memunculkan suatu sistem komunikasi baru yang sering disebut jaringan kerja (*network*) yang bisa diakses melalui internet dengan menggunakan komputer. Kehadiran teknologi komunikasi memberikan kemudahan dan manfaat yang besar kepada manusia sebagai pengguna yakni untuk membantu menyelesaikan permasalahan terhadap kegiatan-kegiatan yang dilakukan manusia dari tingkat kesulitan yang sederhana hingga yang

kompleks, hal ini guna tercapainya efektivitas dan efisiensi dalam setiap kegiatan penyelesaian permasalahan yang dihadapi manusia, khususnya komunikasi.

Perkembangan internet di Indonesia memang seperti tidak terduga sebelumnya. Beberapa tahun yang lalu internet dikenal oleh sebagian kecil orang yang mempunyai minat di bidang komputer. Namun, dalam tahun-tahun terakhir ini pengguna jasa internet meningkat secara sangat pesat, meski ada pendapat yang mengatakan bahwa kebanyakan pengguna internet di Indonesia hanya sebatas untuk hiburan dan percobaan.

Seiring dengan semakin pesatnya perkembangan komunikasi melalui internet, memunculkan pula berbagai kejahatan yang dilakukan dengan media internet. Tidak dapat dipungkiri bahwa penggunaan internet yang canggih dan cepat tersebut memunculkan pula kejahatan yang sangat canggih dan sulit untuk diketahui pelakunya. Hal ini disebabkan karena internet merupakan suatu media komunikasi yang tidak terlihat (maya), sehingga pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat diketahui dengan jelas. Terlepas dari manfaat yang diperoleh dengan kemajuan teknologi di bidang komputer, belakangan muncul persoalan ketika jaringan-jaringan komputer yang dipergunakan oleh berbagai pihak tersebut disalahgunakan oleh pihak-pihak tertentu untuk kepentingan yang berseberangan, atau dikenal dengan kejahatan komputer (*computer crime*). Dalam istilah lain, kejahatan ini lebih dikenal dengan *cyber crime* atau tindak pidana mayantara *(cyber space*) (Barda Nawawi Arief, 2002: 239). Dunia sekarang tanpa batas, sehingga telah menyebabkan perubahan sosial secara signifikan yang berlangsung dengan begitu pesatnya perubahan masyarakat akibat berkembangnya teknologi informasi dan komunikasi, sehingga dunia telah diibaratkan seperti mengekerut. Bermacam-macam peristiwa, termasuk kejahatan, dari berbagai belahan bumi, gambar dan beritanya dapat dihadirkan seketika, bahkan ada yang dapat disajikan secara real tim.

Fenomena perkembangan *cyber crime* ini, sebenarnya bukan hanya sekdar masalah nasional, reginal, atau kawasan suatu negara tertentu, tetapi sudah menjadi perhatian dunia internasional karena memang jangkauan *cyber crime* ini bersifat global *(boarderless)*. Itulah sebabnya dalam berbagai forum internasional seperti *Internasional Information Industry* (IIIC) 2000 *Mellenium Congress* yang diselenggarakan di *Quebec* pada 19 September 2000, Asosiasi Teknologi Informasi Canada *(Information Technology Association of Canada)* sangat mengkhawatirkan permasalah ini. Bahkan Panitia Kerja Perlidungan Data *(Data Protection Working Party)* Dewan Eropa menyatakan bahwa *cyber crime* merupakan bagian sisi paling buruk dari masyarakat Informasi *(cyber crime is part of the seamy side of the information society)* (Barda Nawawi Arief, 2002:239). Sehubungan dengan hal tersebut upaya penanggulangannya dilakukan dengan melakukan kriminalisasi terhadap *cyber crime.*

Kehadiran sistem jaringan informatika dalam bentuk jaringan dalam berbagai bidang tersebut, juga menimbulkan kesempatan bagi pihak-pihak lain untuk mengakses jaringan tersebut untuk kepentingannya sendiri yang pada akhirnya dapat merugikan pihak tertentu. Komputer merupakan serangkaian atau kumpulan mesin elektronik yang bekerja bersama-sama dan dapat melakukan rentetan atau rangkaian pekerjaan secara otomatis melalui instruksi atau pekerjaan yang diberikan kepadanya (Andi Hamzah, 1992:1).

Internet merupakan produk dari hasil pengembangan teknologi informasi membawa perubahan yang sangat besar terhadap pemberdayaan informasi dan telekomunikasi, yang di dalamnya melahirkan konsep yang disebut dengan globalisasi informasi, di mana semakin berkurangnya batasan ruang dan waktu dalam kegiatan berinteraksi dan berbagai informasi mengenai berbagai hal yang dibutuhkan manusia, menggunakan internet yang didalamnya terdapat

internet service provider (ISP), menjadikan komputer yang satu dengan komputer yang lain seolah-olah terhubung tanpa kabel dengan tanpa dibatasi oleh tempat.

Hingga kini, dengan semakin luasnya penggunaan jaringan komputer, kejahatan di bidang komputer juga semakin meningkat, banyak kasus terjadi, namun tidak banyak yang sampai ke pengadilan. Salah satu permasalahan yang dihadapi penegak hukum untuk menjerat pelaku adalah masalah pembuktian tentang kesalahan terdakwa. Kenyataan tersebut menjadi suatu tantangan bagi kalangan hukum yang harus diterima untuk menyelesaikan segala persoalan yang terjadi akibat perkembangan teknologi yang sangat pesat. Kejahatan menggunakan teknologi informasi khususnya internet telah mencapai tahap yang mencemaskan. Kemajuan teknologi informasi selain membawa ke dunia bisnis yang revolusioner *Digital Revolutioner Area* yang serba praktis ternyata juga memiliki sisi gelap yang mengerikan seperti kejahatan komputer, pornografi, terorisme, perjudian, penipuan, pencurian dan lain sebagainya.

Pembuktian merupakan masalah yang memegang peranan dalam proses pemeriksaan sidang pengadilan, dengan pembuktian ini ditentukan nasib terdakwa. Apabila hasil pembuktian dengan alat-alat bukti yang ditentukan undang-undang tidak cukup membuktikan kesalahan yang didakwakan kepada terdakwa, terdakwa dibebaskan dari hukuman, sebaliknya jika terdakwa dapat dibuktikan dengan alat-alat bukti disebut dalam Pasal 184 KUHAP, terdakwa harus dinyatakan bersalah dan kepadanya akan dijatuhkan hukuman. Oleh karena itu, para hakim harus hati-hati, cermat, dan matang dalam menilai dan mempertimbangkan masalah pembuktian. Meneliti sampai di mana batas minimum "kekuatan pembuktian" atau "*bewijs kracht*" dari setiap alat bukti yang disebut dalam Pasal 184 KUHAP.

II. METODE PENELITIAN

Penelitian ini adalah penelitian hukum yang mengkaitkan keberadaan peraturan perundang-undangan yang ada yang selama ini dipakai sebagai acuan dengan peraktek di lapangan. Penelitian utamanya dilakukan dengan studi kepustakaan untuk memperoleh data sekunder terhadap bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Analisis data dilakukan terhadap seluruh peraturan hukum yang berkaitan dengan pokok masalah yang dibahas dan diargumentasikan secara teoritik berdasarkan konsep hukum pidana dengan menggunakan metode analisis kualitatif.

III. HASIL PENELITIAN DAN PEMBAHASAN

Bentuk-Bentuk Tindak Pidana Mayantara (*Cyber Crime*)

Berkaitan dengan perkembangan yang terjadi saat ini telah banyak kejahatan yang muncul merupakan perbuatan kejahatan dunia maya (*cyber crime*). Menurut Setiadi, Penyidik Senior di Markas Bes Kepolisian Republik Indonesia (Mabes Polri), secara terminalogi *cyber crime* yang populer digunakan masarakat dapat diartikan kejahatan dunia maya atau tidak riil. Sehingga seolah-olah tidak ada tindak pidana atau kejahatan karena suatu tindak pidana harus pasti obyek dan subyek hukumnya, *locus delicti* serta *tempus delictinya*. Guna menjelaskan tindak pidana tersebut maka penulis menggunakan istilah dunia maya (*cyber crime*) (Budi Raharjo, 2002:32).

Menurut Setiadi, perbuatan yang dapat dikategorikan sebagai kejahatan di bidang *cyber crime* dapat dibagi menjadi 2 (dua) kategori antara lain:

1) Kejahatan umum yang menjadikan komputer sebagai alat atau sarana (bantu) untuk melakukan kejahatan tersebut. Dalam hal ini langsung atau tidak langsung komputer berperan dalam proses terjadinya tindak pidana lain misalnya;

a. Carding atau penipuan/penyalahgunaan kartu kredit, yaitu penggunaan kartu kredit secara ilegal/tidak sah untuk memesan atau membeli barang via internet dengan cara mencantumkan nomor kartu kredit milik orang lain untuk pembayaran barang yang dipesan.
b. Penipuan internet banking, yaitu melalui media internet melakukan tranfer atau pengambilan atau transaksi perbankan dengan mengunakan website salah satu bank dan dunia perbankan melalui internet
c. Pengancaman/Terorisme, yaitu melalui internet dan pemerasan terhadap pihak lain untuk mencapai tujuanya.
d. Pornografi, yaitu penyebaran gambar porno serta wanita panggilan melalui internet.

2) Kejahatan dengan sasaran targetnya adalah fasilitas komputer serta sistem teknologi informasi sehingga komputer selain sebagai sasaran/korban atau secara umum dikenal sebagai istilah *kacking/cracing* yang menyerang program-program operasi jaringan komputer misalnya:
a. *Dos Attack* yaitu menyerang sistem operasi pada setiap komputer
b. *Defacing,* yaitu merubah (menambah dan mengurangi) tampilan suatu website/homepage tertentu secara ilegal
c. *Phreking* yaitu penyerangan dengan virus atau *worm* dan program-program jahat lainya *Bonet atau robot Network* yaitu jaringan dari para pemilik mesin-mesin akan masuk kedalam pusat komputer yang dikontrol oleh pelaku (Budi Raharjo, 2002:32).

Menurut Budi Raharjo selama ini perusahaan pengaman jaringan komputernya banyak menagani masalah kejahatan dunia maya (*cyber crime*) beberapa perbuatan dalam bentuk:

1. Pencurian dan penggunaan *account* internet milik orang lain. Salah satu kesulitan dari sebuah ISP (*internet service provider*/penyedia layanan internet) adalah adanya *account* pelanggan mereka yang dicuri yang digunakan secara tidak sah. Yang dicuri hanya informasi sehingga orang yang kecurian tidak merasakannya. Pencurian akan terasa efeknya apabila informasi tersebut digunakan oleh yang tidak berhak, akibat pencurian ini pengguna dikenakan biaya atas penggunaan *account* tersebut.
2. Membajak *situs web*.
   Kegiatan ini adalah kegiatan yang paling sering dilakukan *cracker* yaitu mengubah halaman *web*, yang lebih dikenal dengan *deface*. Pembajakan dilakukan dengan mengeksploitasi lubang keamanan suatu situs.
3. Probing dan *Port scaning*
   Salah satu langkah yang dilakukan *cracker* sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan *port scaning* atau probing untuk melihat servis-servis apa saja yang tersedia di server target. Yang bersangkutan memang belum melakukan kegiatan pencarian atau penyerangan akan tetapi kegiatan yang dilakukan sudah mencurigakan.
4. Virus
   Penyebaran virus pada umumnya melalui email, dan sering kali juga orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Kemudian virus ini dikirimkan ke tempat lain melalui emailnya.
5. *Denail of Service (DoS)* dan *Distributed DoS (DoS) attack*
   DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target sehingga tidak dapat memberikan pelayanan. Serangan ini tidak melakukan pencurian, penyadapan atau pemalsuan data akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial.

DoS attack merupakan peningkatan dari serangan *DoS attack* dengan melakukannya dari puluhan komputer seara serentak. Efek yang dihasilkan lebih dasyat dari *DoS attack* saja.

6. Kejahatan yang berhubungan dengan nama domain (*Domain name*).
   Nama domain digunakan untuk mengidentifikasikan perusahaan atau merk dagang. Namun banyak orang mencari keuntungan dengan mendaftarkan nama domain perusahaan orang lain dan menjualnya dengan harga yang lebih mahal. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain (Budi Raharjo, 2002:32).

Badan Pembinaan Hukum Nasional dalam sebuah terbitannya mengidentifikasikan bentuk-bentuk perbuatan yang berkaitan dengan aktifitas di *cyber space* (dunia maya) antara lain:

a. *Joycomputing*, diartikan sebagai perbuatan seseorang yang menggunakan komputer secara tidak sah atau tanpa ijin dan menggunakannya melampui wewenang yang diberikan.
b. *Hacking*, diartikan sebagai perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa ijin (dengan melawan hukum) Dari pemilik sah jaringan komputer tersebut.
c. *The Trojan Horse*, diartikan sebagai suatu prosedur untuk menambah, mengurangi atau mengubah instruksi pada sebuah program, sehingga program tersebut selain menjalankan tugas yang sebenarnya juga akan melaksanakan tugas lainnya yang tidak syah.
d. *Data Leakage*, diartikan sebagai pembocoran data rahasia yang dilakukan dengan cara menulis data-data rahsia tersebut ke dalam kode-kode tertentu sehingga data dapat dibawa keluar tanpa diketahui oleh pihak yang bertanggung jawab.
e. Data *Daddling*, diartikan sebagai suatu perbuatan yang mengubah data valid atau syah dengan cara yang tidak syah yaitu dengan mengubah input data dan output data.
f. Penyia-nyiaan data komputer, diartikan sebagai suatu perbuatan yang dilakukan dengan suatu kesengajaan untuk merusak atau menghancurkan media disket dan media penyimpanan lainnya yang berisikan data atau program komputer (Budi Raharjo, 2002:32).

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, mengkategorikan beberapa perbuatan ke dalam perbuatan kejahatan dunia maya. Perbuatan tersebut mencakup:

a. Kejahatan terhadap nama domain (Pasal 16).
b. Kejahatan terhadap hak kekayaan intelektual dan hak atas informasi rahasia dalam kegiatan teknologi informasi (Pasal 19)
c. Kejahatan terhadap hak-hak pribadi (Pasal 22)
d. Kejahatan pornografi (Pasal 41)

Memahami uraian di atas diketahui bahwa suatu perbuatan dapat dikatakan sebagai suatu tindak pidana apabila telah ada undang-undang yang telah mengaturnya saat ini kejahatan dunia maya (c*yber crime)* belum dapat dikategorikan sebagai suatu perbuatan tindak pidana karena belum ada undang-undang yang mengaturnya namun dalam hal ini pada kenyataan di masyarakat suatu perbuatan dapat dikategorikan sebagai suatu tindak pidana apabila perbuatan tersebut merugikan dan meresahkan masyarakat. Sehingga kejahatan dunia maya yang belum memiliki peraturan perundang-undangan yang mengaturnya dapat dikategorikan sebagai suatu tindak pidana karena perbuatan tersebut telah menyebabkan banyak kerugian pada masyarakat dan perbuatan kejahatan dunia maya dapat dikriminalisasikan agar terdapat suatu kepastian hukum terhadap suatu perbuatan tindak pidana.

Perbuatan-perbuatan yang telah diatur dalam undang-undang maupun yang telah banyak terjadi dan telah dianggap oleh masyarakat sebagai suatu perbuatan kejahatan dunia maya *(cyber*

crime) dapat dianalisis untuk memformulasikan penetapan suatu perbuatan merupakan perbuatan kejahatan dunia maya dengan cara:

a. Menjelaskan istilah-istilah yang terdapat dalam pengertian dunia maya (*cyber crime*) seperti program komputer, jaringan komputer, internet, disket, *database, password*, data elektronik, tandatangan digital, *website, input* dan *output* dan lain-lain.
b. Membagi perbuatan dalam kejahatan dunia maya (*cyber crime*) mencakup pada perbuatan yang terjadi dalam hardware. *Software* maupun dalam jaringan (*network*), baik perbuatan tersebut, dilakukan oleh orang maupun badan hukum.

Pembuktian di dalam Hukum Pidana Indonesia terhadap *Cyber Crime*

Pembuktian terhadap suatu tindak pidana merupakan ketentuan-ketentuan yang berisi pengarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa, pembuktian juga merupakan ketentuan yang mengatur alat-alat bukti yang dibenarkan undang-undang dan yang boleh dipergunakan Hakim membuktikan kesalahan yang didakwakan. Pembuktian dapat dipadang sebagai titik sentral dalam proses persidangan di Pengadilan, karena dalam pembuktian ini, akan ditentukan nasib dari terdakwa. Apabila hasil pembuktian dengan alat-alat bukti yang ditentukan oleh undang-undang tidak cukup untuk membuktikan kesalahan yang didakwakan kepada terdakwa, maka terdakwa dibebaskan dari hukum. Sebaliknya ketika kesalahan terdakwa dapat dibuktikan, maka terdakwa dinyatakan bersalah, dan oleh karenanya dijatuhi pidana.

Menurut Pitlo, pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya. (Edmon Makarim, 2004:417). Pembuktian tentang benar tidaknya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting dalam hukum acara pidana. Membuktikan berarti memberi kepastian kepada hakim tentang adanya peristiwa-peristiwa tertentu. Adapun enam butir pokok yang menjadi alat ukur dalam teori pembuktian, dapat diuraikan sebagai berikut:

1. Dasar Pembuktian

   Yang dimaksud dengan Dasar Pembuktian adalah dasar-dasar yang dipergunakan untuk mendapatkan suatu kebenaran atas fakta-fakta. Dengan kata lain dasar pembuktian itu adalah isi/materi dari alat bukti itu sendiri. Dapatlah dikatakan bahwa jikalau alat bukti itu adalah wadahnya, maka dasar pembuktian adalah isi dari wadah tersebut.

2. Alat Pembuktian

   Alat Pembuktian adalah alat-alat yang dipergunakan untuk menggambarkan atau menerangkan suatu keadaan atau peristiwa pidana berdasarkan fakta-fakta yang terjadi diwaktu yang lampau guna keperluan proses pidana.

3. Penguraian Alat Pembuktian

   Penguraian Pembuktian adalah cara-cara yang dipergunakan untuk menguraikan suatu peristiwa atau keadaan berdasarkan penggunaan alat bukti yang dipergunakan untuk melakukan tindak pidana. Penguraian Pembuktian memegang peranan yang sangat penting didalam pemeriksaan perkara di pengadilan, karena berdasarkan bukti-buktilah Hakim menetapkan keyakinannya.

4. Kekuatan Pembuktian

   Yang dimaksud Kekuatan Pembuktian disini adalah kekuatan pembuktian dari masing-masing alat bukti. Dalam perkara pidana biasanya kekuatan pembuktian terletak pada fakta-fakta, dimana pembuktiannya didasarkan atas kebenaran dari fakta-fakta yang telah teruji kebenarannya oleh Hakim.

5. Beban pembuktian yang diwajibkan oleh undang-undang untuk membuktikan tentang dakwaan di muka sidang pengadilan (*bewijslast*).
6. Bukti minimum yang diperlukan dalam pembuktian untuk mengikat kebebasan hakim (*bewijsminimum*)

Pada hakekatnya, pembuktian dimulai sejak adanya suatu peristiwa hukum. Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan (serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyelidikan menurut cara yang diatur dalam undang-undang ini), dan dalam Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian dalam pasal 1 angka 13, penyidikan ialah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.

Berdasarkan Pasal 184 ayat (1) Kitab Undang-Undang Hukum Acara Pidana (KUHAP) disebutkan alat bukti yang sah adalah:

a. Keterangan Saksi
b. Keterangan Ahli
c. Surat
d. Petunjuk
e. Keterangan Terdakwa

Dalam Pasal 5 Undang Undang tentang Informasi dan Transaksi Elektronik dinyatakan bahwa:

Ayat (1) Informasi elektronik dan atau hasil cetak dari informasi elektronik merupakan alat bukti yang sah dan memiiki akibat hukum yang sah.

Ayat (2) Informasi elektronik dan atau hasil cetak dari informasi elektronik sebagaimana dimaksud dalam ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Berkaitan dengan permasalahan yang dibahas mengenai tindak pidana mayantara (*cyber crime*) yang menggunakan sarana internet maka ketentuan hukum yang dipakai tetap mengacu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-undang tentang Informasi dan Transaksi Elektronik

Kejahatan *cyber* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar KUHP. Perkembangan teknologi informasi yang demikian pesatnya haruslah di antisipasi dengan hukum yang mengaturnya dimana kepolisian merupakan lembaga aparat penegak hukum yang memegang peranan penting di dalam penegakan hukum. Agar suatu perkara pidana dapat sampai pada tingkat penuntutan dan pemeriksaan di sidang pengadilan, maka sebelumnya harus melewati beberapa tindakan-tindakan pada tingkat penyidik.

Pada dasarnya proses pidana melalui tahap-tahap sebagai berikut:

1. Tahap penyidikan oleh aparat kepolisian
2. Tahap penuntutan oleh Jaksa (Penuntut Umum)
3. Tahap pemeriksaan di pengadilan.

Pada proses penyidikan, aparat penyidik melakukan serangkaian tindakan yang diperlukan guna mendapatkan alat bukti yang nantinya diperlukan dipersidangan. Apabila tidak cukup bukti, atau peristiwa tersebut ternyata bukan tindak pidana atau penyidikan dihentikan demi hukum

maka penyidik berwenang untuk menghentikan proses penyidikan, begitu juga sebaliknya apabila bukti-bukti telah terpenuhi dan peristiwa tersebut adalah merupakan tidak pidana maka penyidik akan melanjutkan proses penyidikan dengan membuat berita acara (pemberkasan perkara) untuk diserahkan kepada penuntut umum.

Tindak pidana Mayantara (*cyber crime*) menggunakan sarana internet sulit sekali mencari dan mengumpulkan alat bukti untuk menjerat pelaku, baik pelaku penyedia sarana internet maupun pelaku pemain perjudian itu sendiri, dikarenakan kejahatan ini merupakan tindak pidana dunia maya (*Cyber Crime*), dimana data-data jaringan internet atau komputer sulit untuk ditembus oleh aparat penegak hukum, sehingga aparat kesulitan dalam mengumpulkan bukti bukti untuk menjerat pelaku tindak pidana.

Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan (serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyelidikan menurut cara yang diatur dalam undang-undang ini), dan dalam Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian dalam pasal 1 angka 13, penyidikan ialah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.

Menurut Petrus Reinhard Golose, seperti yang tertuang didalam artikelnya di buletin hukum, Dia menjelaskan bahwa untuk itu hal atau langkah-langkah yang dilakukan oleh Polri dalam menangani kasus *cyber* atau kasus-kasus perusakan terhadap komputer melalui jaringan, adalah sebagai berikut":

1) Pembuatan Laporan Polisi, yang diikuti dengan pemanggilan Saksi dari pemilik ISP (*Internet Service Provider*) yang telah diketahui bahwa ISP tersebut digunakan oleh si pelaku (*hacker*);
2) Pemeriksaan di Tempat Kejadian Perkara (TKP) dan warnet atau café net yang digunakan pelaku, sekaligus untuk mengumpulkan, melacak dan/atau melakukan penyitaan terhadap bukti elektronik (*digital evidence*) yang ada di TKP, seperti *hard disk*;
3) Melakukan pemeriksaan terhadap para saksi dan ahli yang memiliki keahlian dibidang teknologi informasi, baik dari Universitas Indonesia (UI), Universitas Padjajaran (UNPAD) atau lembaga-lembaga lainnya;
4) Pemeriksaan terhadap tersangka, setelah didahului dengan upaya paksa penangkapan dan/atau penahanan, berdasarkan bukti permulaan dan/atau alat bukti yang cukup;
5) Pemberkasan dan penerapan pasal-pasal pidana yang dapat disangkakan terhadap tersangka. didalam melakukan kegiatan penyidikan diperlukan suatu bukti permulaan yang cukup yaitu alat bukti untuk menduga adanya suatu tindak pidana dengan mensyaratkan adanya minimal laporan polisi ditambah salah satu alat bukti. Hal tersebut tentunya berkaitan dengan beban pembuktian yang telah disyaratkan Undang-Undang dalam hal ini yakni minimal dua alat bukti.

Dalam melakukan penyidikan suatu kasus kejahatan dunia maya, seorang penyidik dapat menggunakan alat-alat investigasi standar (*standartinvestigative tools*), antara lain:

a. Informasi sebagai dasar bagi suatu kasus

Informasi dapat diperoleh dari observasi, pengujian bukti elektronik yang tersimpan dalam *hard disk* atau bahkan masih dalam memori. Bagi penyidik,sangat penting untuk memperoleh

informasi melalui *crime scene search* (penyidikan di tempat kejadian perkara) yang bertumpu pada komputer.

b. *Interview* dan Interogasi

Alat ini dipergunakan untuk memperoleh informasi dari pihak-pihak yang terlibat dalam kejahatan dunia maya. Wawancara ini meliputi perolehan informasi dengan memberikan pertanyaan kepada saksi-saksi, korban, dan pihak lain yang mungkin memiliki informasi relevan untuk memecahkan kasus tersebut. Sedangkan interogasi meliputi perolehan informasi dengan memberikan pertanyaan kepada tersangka dan saksi. Adapun tekniknya dilakukan dengan pendekatan simpatik yang meliputi:

a) Pendekatan logis

Menggunakan alasan-alasan untuk meyakinkan tersangka untuk mengakui perbuatannya;

b) *Indifference*

Dengan berpura-pura tidak memerlukan pengakuan karena penyidik telah memiliki cukup bukti walaupun tanpa pengakuan. Hal tersebut efektif untuk kasus dengan banyak tersangka, dimana keterangan yang bersangkutan saling dikonfrontir;

c) *Facing-saving approach*

Dengan membiarkan tersangka memberikan alasan-alasan atas tindakannya dan menunjukkan pengertian mengapa yang bersangkutan melakukan tindakan tersebut.

c. Instrumen

Kegunaan teknologi dalam memperoleh bukti-bukti. Dalam kasus kejahatan dunia maya, penggunaan data teknik *recovery* untuk menemukan informasi yang "*deleted*" dan "*erased*" dalam *disk* merupakan salah satu tipe instrumennya.

Selain itu, contoh-contoh tradisional lainnya meliputi teknik forensik untuk mengumpulkan dan menganalisis bukti-bukti dan analisis DNA.

6) Menyusun laporan kasus

Setelah semua bukti fisik telah dikumpulkan dan didokumentasikan serta interogasi telah dilaksanakan, langkah yang harus dilakukan ialah penyusunan laporan kasus yang memuat:

a.Laporan penyelidikan;
b.Laporan penyidikan kasus pidana yang ditindaklanjuti dari laporan penyelidikan;
c.Dokumentasi bukti-bukti elektronik
d.Laporan laboratorium dari ahli forensik komputer;
e.Pernyataan-pernyataan tertulis dari saksi-saksi, tersangka, dan ahli;
f. Laporan TKP, foto-foto dan rekaman video;
*g.*Print out dari bukti-bukti digital yang berkaitan.

7) Pemeriksaan berkas perkara oleh Jaksa Penuntut Umum Penuntut umum memberikan arahan kepada penyidik atas kelemahankelemahan berkas perkara dan tambahan informasi atau bukti tambahan yang perlu diperoleh atau klarifikasi fakta-fakta dalam rangka memperkuat tuntutan serta menyiapkan saksi-saksi untuk proses persidangan jika kasus tersebut dilimpahkan ke pengadilan.

8) Membuat keputusan untuk menuntut Jika berkas perkara dinyatakan lengkap, penuntut umum melakukan penuntutan hukum kepada tersangka dalam suatu persidangan yang sangat tergantung dari yuridiksi dan prosedur yang ditentukan oleh undang-undang. Dalam tahap ini pilihan jenis tuntutan ditetapkan berdasarkan hukum pembuktian yang diatur dalam KUHAP. (Petrus Reinhard Golose, 2006:15).

Pada proses penuntutan seorang jaksa yang bertindak selaku penuntut umum membuat surat dakwaan, dimana dalam surat dakwaan tersebut didasari atas alat-alat bukti yang telah diteliti, diperiksa dan disimpan oleh jaksa. Sesuai dengan sistem pembuktian yang dianut oleh KUHP, maka jaksa dalam menyusun tuntutannya juga harus berpedoman pada isi Pasal 183 KUHAP yakni minimal ada dua alat bukti yang sah menurut Undang-Undang, yang apabila telah memenuhi syarat-syarat perkara tersebut diteruskan pada proses pemeriksaan di sidang pengadilan.

Berkaitan dengan tindak pidana mayantara (*cyber crime*) dengan menggunakan sarana internet pihak kejaksaan berkoordinasi dengan pihak kepolisian selaku penyidik untuk menjerat pelaku tindak pidana tetapi apabila tidak ditemukan bukti yang kuat, serta ketentuan atau peraturan perundang-undangan yang mengatur mengenai tindak pidana tersebut maka terhadap pelaku dapat dilakukan penghentian proses penyidikan maupun penuntutan.

Berdasarkan uraian tersebut di atas dapat dianalisis bahwa cara yang harus ditempuh oleh pihak kepolisian dan Kejaksaan apabila terjadi suatu tindak pidana *cyber crime* adalah melakukan investigasi kasus dengan cara mencari alamat *ip address web* dan mencari bukti elektronik. Karena *ip address web* adalah bukti pertama yang kuat didalam pengungkapan *kasus cyber*. Menurut pasal 5 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi elektronik yang berbunyi:
(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. (2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. (3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

Adanya terobosan hukum baru karena Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara. Tetapi untuk "mensahkan" bukti elektronik tersebut di hadapan pengadilan adalah dengan cara memproses bukti elektronik tersebut dari bentuk elektronik yang dihasilkan dari sistem komputer menjadi *output* yang dicetak ke dalam media kertas. Yakni, bukti elektronik tersebut diubah perwujudannya dalam bentuk *hardcopy*, yaitu di-*print*, tanpa adanya modifikasi apapun dari manusia. Lalu untuk memperkuatnya, *print out* tersebut bisa diserahkan kepada saksi ahli untuk dianalisa dan disampaikanvaliditasnya di hadapan pengadilan (Petrus Reinhard Golose, 2006:19).

Proses pemeriksaan di sidang pengadilan, Hakim melakukan penilaian atas kekuatan alat-alat bukti yang diajukan oleh penuntut umum di dalam dakwaannya. Hakimpun dalam hal ini berpedoman pada sistem pembuktian negatif menurut Undang-Undang yaitu Pasal 183 kUHAP yang menentukan minimal dua alat bukti dengan disertai keyakinan. Permasalahan terkadang di dalam suatu proses perkara pidana mengalami kesulitan untuk mendapatkan suatu kebenaran yang mutlak karena kurangnya bukti-bukti yang ada, atau juga bukti-bukti yang ada kurang mendukung untuk menyelesaikan perkara tersebut sehingga hal tersebut mengakibatkan banyaknya kasus-kasus yang tak terselesaikan dan menumpuk di tingkat penyidikan/kepolisian. Banyaknya kasus-kasus yang menumpuk tersebut biasanya tersendat pada tingkat kepolisian karena jaksa dalam hal ini biasanya menolak berkas perkara yang diserahkan penyidik karena kurangnya bukti-bukti yang menguatkan dakwaan.

Mengingat suatu kejahatan yang dilakukan senantiasa agar tidak diketahui oleh orang lain maka pelaku tindak pidana berusaha semaksimal mungkin untuk menghilangkan barang bukti, hal tersebut merupakan upaya pencegahan untuk menghindarkan pembenaran dari suatu pembuktian baik dalam tingkat penyidikan maupun pada tingkat pemeriksaan. Oleh sebab itu peran pembuktian sangatlah penting di dalam proses pidana sehingga dapat dikatakan pembuktian merupakan jantung dari hukum acara pidana.

Memahami uraian di atas dapat dianalisis bahwa untuk membuktikan suatu tindakan kejahatan *cyber* dalam persidangan. Untuk itu didalam sistem pembuktian dipersidangkan harus berdasarkan sistem pembuktian berdasarkan undang-undang secara positif . Yang mana undang-undang menetapkan secara limitatif alat-alat bukti yang mana yang boleh dipakai hakim. Jika alat-alat bukti tersebut telah dipakai secara sah seperti yang ditetapkan oleh undang-undang, maka hakim harus menetapkan keadaan sah terbukti, meskipun hakim ternyata berkeyakinan bahwa yang harus dianggap terbukti itu tidak benar. Menurut D. Simmon, sistem ini berusaha untuk menyingkirkan semua pertimbangan subjektif hakim dan mengikat hakim dengan peraturan pembuktian yang keras. "Sistem ini disebut juga dengan teori pembuktian formal (*formele bewijstheorie*)". (Andi Hamzah; 247). Teori ini ditolak oleh Wirjono Prodjodikoro untuk dianut di Indonesia, karena katanya bagaimana hakim dapat menetapkan kebenaran selain dengan cara menyatakan kepada keyakinannya tentang hal kebenaran itu, lagipula keyakinan seorang hakim yang jujur dan berpengalaman mungkin sekali adalah sesuai dengan keyakinan masyarakat" (Andi Hamzah, 247)

Untuk pembuktian kasus didunia maya didalam persidangan harus juga memakai sistem pembuktian berdasarkan keyakinan hakim atas alasan yang logis (*la conviction raisonee*) sistem pembuktian ini, hakim memegang peranan yang penting disini. Hakim baru dapat menghukum seorang terdakwa apabila ia telah meyakini bahwa perbuatan yang bersangkutan terbukti kebenarannya. Keyakinan tersebut harus disertai dengan alasan-alasan yang berdasarkan atas suatu rangkaian pemikiran (logika). "Hakim wajib menguraikan dan menjelaskan alasan-alasan yang menjadi dasar keyakinannya atas kesalahan terdakwa". Sistem pembuktian ini mengakui adanya alat bukti tertentu tetapi tidak ditetapkan secara limitatif oleh undang-undang (Andi Hamzah, 247)

Pembuktian seperti ini jelas terlihat bahwa suatu alat bukti bukanlah alat bukti, minimal sekurang-kurangnya dua alat bukti yang harus disertai dengan Keyakinan Hakim. Walaupun telah cukup bukti tetapi hakim tidak yakin atau hakim telah yakin tetapi alat-alat bukti tidak cukup, maka hakim tidak boleh menjatuhkan hukuman atas terdakwa. Dalam teori *Negatief Wetterlijk* terlihat jelas keterkaitan hubungan antara alat-alat bukti dengan keyakinan hakim dimana hakim terikat pada aturan Undang-Undang dan ia memperoleh keyakinan bahwa bukti-bukti telah diberikan sehingga hukuman dapat dijatuhkan.

Berdasarkan uraian di atas dapat dianalisis bahwa tidaklah sederhana menerapkan aturan hukum terhadap pelaku yang terlibat dalam *cyber crime*. Hal ini mengingat internet bersifat lintas batas wilayah. Banyak pihak yang bersinggungan satu dengan yang lain dan ini akan menyulitkan dalam proses pemeriksaan di pengadilan. Karena itu, harus dicari solusi agar pelaku yang terlibat dalam *cyber crime* dapat dihadirkan ke meja hijau.

Hukum mana yang berlaku sebenarnya tidaklah sesulit seperti yang berlangsung selama ini, pelaku yang terlibat dalam *cybercrime* ini dapat dijatuhi hukuman pidana sesuai dengan ketentuan yang berlaku (hukum positif) sesuai dengan status kewarganegaraan dari pelaku itu berada. Kemudian juga dimungkinkan bagi warga asing yang melakukan tindak pidana di wilayah

Indonesia untuk dipidana dengan menggunakan hukum pidana Indonesia. Hal ini sesuai dengan prinsip nasionalitas pasif. Yang harus dilakukan jika kita ingin menggunakan hukum Indonesia untuk menjaring pelaku luar negeri adalah melakukan perjanjian ektradisi dengan negara asal pelaku. Pasalnya, dalam proses penyelidikan dan penyidikan, *cybercrime* tidaklah bisa dilakukan sendirian dan perlu dilakukan koordinasi dengan interpol, FBI, dan yang lainnya.

IV. KESIMPULAN

Keterangan ahli telematika dalam proses pemeriksaan perkara tindak pidana mayantara, baik pada tahap pemeriksaan penyidikan maupun pada pemeriksaan disidang pengadilan sangat penting dan dibutuhkan, terutama untuk membantu penyidik, penuntut umum ataupun hakim dalam mengungkapkan suatu kasus kejahatan mayantara (*Cyber Crime*) yang sangat rumit, kompleks yang bersifat spesifik. Berkaitan dengan permasalahan yang dibahas mengenai pembuktian tindak pidana *cyber crime* yang menggunakan sarana *internet* maka ketentuan hukum pembuktian yang dipakai tetap mengacu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang merupakan alat bukti yang sah menurut undang-undang.

DAFTAR PUSTAKA

Buku

Asril Sitompul, *Hukum Internet*, PT. Citra Aditya Bakti, Bandung, 2001

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Bandung, 2005.

Barda Nawawi Arief, *Tindak Pidana Mayantara*, PT. Raja Grafindo, Jakarta, 2006

Budi Agus Riswandi, *Hukum Cyberpace*, Gita Nagari, Yogyakarta, 2006.

_____, *Hukum dan Internet di Indonesia*, UII Yogyakarta, 2003

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law*, PT. Refika Aditama, Bandung, 2005

Edmon Makarim, *Kompilasi Hukum Telematika*, PT. Raja Grafindo. Jakarta, 2004.

Merry Magdalena dan Maswigrantoro Roes Setiyadi, *Cyberlaw Tidak Perlu Takut*, CV. Andi Offest, Yogyakarta, 2007.

Petrus Reinhard Golose, *Perkembangan* Cybercrime *dan Upaya Penanganannya di Indonesia oleh Polri*, Buletin Hukum, 2006

Riyeke Ustadiyanto, *Framework E-Commerce*, ANDI Yogyakarta, 2001.

Subekti, *Hukum Pembuktian*, Pradnya Paramita, Jakarta, 2002.

WirjonoProjodikoro, *Tindak-Tindak Pidana Tertentu di Indonesia*, PT. Eresco, Jakarta, 2006

Peraturan Perundang-Undangan

Undang-Undang No 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana

Undang-Undang No 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana

Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang No 2 Tahun 2002 tentang Kepolisian RI

Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elekronik

Rancangan Undang-Undang KUHP

Sumber Lain

Kamus Besar Bahasa Indonesia, Edisi kedua, cetakan kedua, Balai Purtaka, Jakarta.

Kejahatan dalam Dunia Cyber.http*://www.lkhtnet.com.*LKHT FH UI