

# TINJAUAN YURIDIS TENTANG PENGATURAN DAN KEDUDUKAN INTERNET PROTOKOL SEBAGAI ALAT BUKTI DALAM TINDAK PIDANA KEJAHATAN MAYANTARA (*CYBER CRIME*)

IVAN GIOVANI SEMBIRING

## Abstrak

Salah satu masalah yang muncul akibat perkembangan teknologi informasi internet adalah lahirnya suatu bentuk kejahatan baru yang sering disebut dengan *cyber crime* (kejahatan mayantara). Adapun tujuan penulisan skripsi ini adalah untuk mengetahui pengaturan alat bukti informasi elektronik berupa *internet protocol* dalam tindak pidana kejahatan mayantara berdasarkan UU No. 11/2008.

Rumusan masalah penelitian ini yaitu bagaimana pengaturan mengenai penggunaan alat bukti berupa informasi elektronik sebagai bukti dalam tindak pidana kejahatan mayantara (*cyber crime*) dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan bagaimana kedudukan Internet Protokol sebagai alat bukti dalam tindak pidana kejahatan mayantara (*cyber crime*). Pendekatan yang digunakan adalah konseptual. Materi penelitian diambil dari data primer data primer dan data sekunder, kemudian dianalisis secara kualitatif untuk menjawab permasalahan penelitian.

Kedudukan Internet Protokol sebagai alat bukti dalam kejahatan mayantara (*cyber crime*) adalah sebagai petunjuk dalam mencari kebenaran materiil dalam kasus kejahatan mayantara (*cyber crime*). Petunjuk diperoleh berdasarkan keterangan saksi, surat, dan keterangan terdakwa. Implikasi yuridisnya adalah dengan digunakannya Internet Protokol sebagai alat bukti dalam tindak pidana kejahatan mayantara atau *cyber crime*, maka setiap orang yang melakukan tindak pidana tersebut dapat dikenakan pemidanaan.

Kata kunci : Internet Protokol, Alat Bukti, Kejahatan Mayantara.

## A. Latar Belakang

Globalisasi pada dasarnya bermula dari awal abad ke 20, yakni pada saat revolusi transportasi dan elektronika mulai memperluas dan mempercepat perdagangan antar bangsa. Menurut Tholchah Hasan, di samping pertambahan dan kecepatan lalu lintas barang dan jasa, berkembang pula secara cepat globalisasi gagasan modern seperti negara, konstitusi, nasionalisme, kapitalisme, demokrasi, sekularisme, juga industri dan perusahaan media massa.<sup>1</sup>

Semakin berkembangnya teknologi informasi sekarang ini, baik berupa internet atau media lain yang sama, menimbulkan berbagai akibat. Ada akibat positif maupun akibat negatif yang timbul dari perkembangan teknologi informasi tersebut. Banyak kemudahan yang dapat kita peroleh dari pemanfaatan teknologi informasi tersebut, khususnya dari internet, dan tidak dapat dipungkiri juga, bahwa teknologi informasi khususnya internet tersebut dapat menjadikan kejahatan yang semula hanya bersifat konvensional seperti pencurian, penipuan, pengancaman, dan lain sebagainya menjadi lebih canggih melalui penggunaan media komputer secara online dengan resiko tertangkap yang sangat kecil.<sup>2</sup>

Internet sebagai hasil rekayasa teknologi bukan hanya menggunakan kecanggihan teknologi komputer tapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya. Apalagi pada saat internet sudah memasuki generasi kedua, perangkat komputer konvensional akan tergantikan oleh peralatan lain yang juga memiliki kemampuan mengakses internet.

Contoh kasus kejahatan internet adalah kejahatan dunia perbankan melalui Internet (*e-banking*) Indonesia dikejutkan oleh ulah seseorang bernama Steven

---

<sup>1</sup> Abdul Wahid dan Muhammad Habib. 2005. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama.

<sup>2</sup><http://ern.pendis.depag.go.id/DokPdf/jurnal/6.%20Achmad%20Tahir.pdf>, diakses tanggal 25 Nopember 2011, jam 20.30 Wib.

Haryanto, seorang *hacker* dan jurnalis pada majalah Master Web. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan internet banking Bank Central Asia, (BCA). Steven membeli domain-domain dengan nama mirip [www.klikbca.com](http://www.klikbca.com) (situs asli Internet banking BCA), yaitu domain [wwwklik-bca.com](http://wwwklik-bca.com), [kilkbca.com](http://kilkbca.com), [klikbca.com](http://klikbca.com), [klikca.com](http://klikca.com), dan [klikbac.com](http://klikbac.com). Isi situs-situs plesetan ini nyaris sama. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkat situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (*user id*) dan nomor identitas personal dapat diketahuinya.

Pada sebuah proses penyelesaian perkara pidana, proses pembuktian merupakan suatu proses pencarian kebenaran materiil atas suatu peristiwa pidana. Hal ini berbeda jika dibandingkan proses penyelesaian perkara perdata yang merupakan proses pencarian kebenaran formil. Proses pembuktian sendiri merupakan bagian terpenting dari keseluruhan proses pemeriksaan persidangan.

Hukum acara pidana di dalam bidang pembuktian mengenal adanya Alat Bukti dan Barang Bukti, di mana keduanya dipergunakan di dalam persidangan untuk membuktikan tindak pidana yang didakwakan terhadap terdakwa. Alat bukti yang sah untuk diajukan di depan persidangan, seperti yang diatur Pasal 184 Undang-undang Nomor 8 tahun 1981 Tentang Hukum Acara Pidana (KUHP) adalah: (a) Keterangan saksi; (b)Keterangan ahli; (c)Surat; (d)Petunjuk; (e)Keterangan terdakwa.<sup>3</sup>

Pada perkembangannya, alat bukti sebagaimana yang diatur dalam KUHP tidak lagi dapat mengakomodir perkembangan teknologi informasi, hal ini menimbulkan permasalahan baru. Salah satu masalah yang muncul akibat

---

<sup>3</sup> Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHP).

perkembangan teknologi informasi adalah lahirnya suatu bentuk kejahatan baru yang sering disebut dengan *cyber crime* (tindak pidana mayantara). Secara garis besar *cyber crime* terdiri dari dua jenis, yaitu kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas dan kejahatan yang menjadikan sistem dan fasilitas TI sebagai sasaran.

Proses pembuktian suatu alat bukti yang berupa data digital ini juga menyangkut aspek validasi data digital yang dijadikan alat bukti tersebut. Aspek lain terkait adalah masalah menghadirkan alat bukti tersebut, apakah dihadirkan cukup dengan perangkat lunaknya (*software*) ataukah harus dengan perangkat kerasnya (*hardware*).<sup>4</sup>

Sebagaimana telah dijelaskan terlebih dahulu, bukti digital tidak dikenal dalam KUHAP. Sebagai *lex specialis*, Undang-undang Nomor 11 Tahun 2008 memiliki kekhususan secara formil dibandingkan KUHAP. Salah satu kekhususan tersebut yang menjadi fokus dalam penulisan ini adalah terkait penggunaan alat bukti yang merupakan pembaharuan proses pembuktian konvensional dalam KUHAP.

Usaha mewujudkan cita-cita hukum (*rechtside*) untuk mensejahterakan masyarakat melalui kebijakan hukum pidana tidak merupakan satu-satunya cara yang memiliki peran paling strategis. Dikatakan demikian karena hukum pidana hanya sebagai salah satu dari sarana kontrol masyarakat (sosial). Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi

---

<sup>4</sup> Subekti. 1995. *Hukum Pembuktian*. Jakarta: Pradnya Paramita.

informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi arena efektif untuk melakukan perbuatan melawan hukum.

Perkembangan teknologi dan perkembangan hukum telah menyebabkan tergesernya bentuk media cetak menjadi bentuk media digital (*paper less*). Perlu diperhatikan dalam kejahatan dengan menggunakan komputer, bukti yang akan mengarahkan suatu peristiwa pidana adalah berupa data elektronik, baik yang berada di dalam komputer itu sendiri (*hardisk/floppy disc*) atau yang merupakan hasil *print out*, atau dalam bentuk lain berupa jejak (*path*) dari suatu aktivitas pengguna komputer.

Aktivitas-aktivitas yang dilakukan dengan media internet, atau dalam *cyberspace*, meninggalkan jejak-jejak elektronik. Pada saat kita mengakses sebuah website, akan tertinggal jejak-jejak elektronik di komputer kita yang namanya *log file*, atau lebih mudah lagi, apa yang kita akses melalui browser pasti meninggalkan jejak paling tidak di komputer si pengguna yang dikenal dengan history. Sehingga pemanfaatan internet tersebut baik untuk tujuan yang baik atau tujuan yang jahat dalam hal ini dijadikan sebagai media, alat atau sasaran kejahatan, tercatat atau meninggalkan jejak elektronis. Tinggal bagaimana para aparat hukum menggali serta menangani jejak-jejak elektronis itu sebagai bukti untuk membuat terang sebuah tindak pidana yang dilakukan.

Melihat fakta hukum sebagaimana diuraikan di atas, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *cyber crime* yang terjadi dapat dilakukan upaya

penanggulangannya dengan hukum acara pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya.<sup>5</sup>

Rumusan masalah dalam penelitian ini yaitu bagaimana pengaturan mengenai penggunaan alat bukti berupa informasi elektronik sebagai bukti dalam tindak pidana kejahatan mayantara (*cyber crime*) dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik? Dan bagaimana kedudukan Internet Protokol sebagai alat bukti dalam tindak pidana kejahatan mayantara (*cyber crime*)?

Seperti yang telah dikemukakan bahwa yang menjadi persoalan penting dalam proses perkara pidana adalah untuk menemukan kebenaran materil atau kebenaran yang sesungguhnya. Sumber utama di dalam menemukan kebenaran materil tersebut ialah adanya pembuktian yang menghendaki agar semua alat bukti yang diperlukan guna mendapatkan suatu kebenaran yang sesungguhnya dapat ditampilkan sedemikian rupa di muka pengadilan agar supaya hakim dapat memperoleh gambaran secara jelas tentang adanya suatu tindak pidana.

Menurut Undang-Undang Nomor 11 Tahun 2008, suatu informasi elektronik/dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tersebut, yaitu sistem elektronik yang andal dan aman, serta memenuhi persyaratan minimum sebagai berikut:<sup>6</sup>

1. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

---

<sup>5</sup> Widyopramono. 1994, *kejahatan di Bidang Komputer*. Jakarta: Pustaka Sinar Harapan.

<sup>6</sup> Ari Juliano Gema, dapat dilihat di <http://arijuliano.blogspot.com/2008/04/apakah-dokumen-lektronikdapat-menjadi.html>

2. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
4. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan 5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Kejahatan mayantara (*cyber crime*) dapat diartikan sebagai kegiatan ilegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global. Perbedaannya dengan kejahatan konvensional dapat dilihat dari kemampuan serbaguna yang ditampilkan akibat perkembangan informasi dan teknologi komunikasi yang semakin canggih. Sebagai contoh, komunikasi yang melalui internet membuat pelaku kejahatan lebih mudah beraksi melewati batas wilayah Negara untuk melakukan kejahatannya tersebut. Internet juga membuat kejahatan semakin terorganisir dengan tersedianya teknik yang semakin canggih guna mendukung dan mengembangkan jaringan untuk perdagangan obat, pencucian uang, perdagangan senjata ilegal, penyelundupan dan lain-lain. Bagi para *hacker* keadaan ini memberikan ruang yang cukup luas untuk mengaplikasikan keahlian komputer yang dimilikinya.<sup>7</sup>

Tujuan penelitian ini yaitu untuk mengetahui macam-macam alat bukti elektronik yang digunakan sebagai alat bukti dalam pembuktian pada kasus tindak

---

<sup>7</sup>Steven Furnell, 2002. *Cyber crime Vandalizing The Information Society*. United States of America: Pearson Education Limited, hal. 3.

pidana kejahatan mayantara yang terjadi di Indonesia. Selain itu penelitian ini juga bertujuan untuk mengetahui implikasi yuridis penggunaan alat bukti elektronik khususnya Internet Protokol sebagai alat bukti dalam tindak pidana kejahatan mayantara (*cyber crime*).

## **B. Metode Penelitian**

Adapun jenis penelitian termasuk penelitian hukum normatif (penelitian hukum doctrinal). Sifat penelitian yang peneliti lakukan adalah termasuk penelitian deskriptif, yakni penelitian hukum yang bersifat pemaparan dan bertujuan untuk memperoleh gambaran (deskripsi) lengkap tentang keadaan hukum yang berlaku.<sup>8</sup> Jenis data yang digunakan adalah bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Teknik pengumpulan data yaitu diperoleh dari bahan pustaka dari peraturan perundang-undangan, buku-buku, karya tulis, dan data yang didapat dari halaman-halaman internet. Setelah data terkumpul kemudian dianalisa menggunakan metode analisis kualitatif.

## **C. Hasil Penelitian dan Pembahasan**

Menurut Pitlo, pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya.<sup>9</sup> Menurut Subekti, yang dimaksudkan dengan membuktikan adalah meyakinkan hakim tentang kebenaran dalil ataupun dalil-dalil yang dikemukakan oleh para pihak dalam suatu persengketaan.<sup>10</sup> Pembuktian tentang benar tidaknya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting dalam

---

<sup>8</sup> Peter Mahmud Marzuki. 2008. *Penelitian Hukum*. Jakarta: Kencana Persada Media Group.

<sup>9</sup> Pitlo dalam Edmon Makarim, 2003. *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, Hlm. 417

<sup>10</sup> Subekti, R, 1995. *Hukum Pembuktian*, Pradnya Paramita, Jakarta, hlm. 1

hukum acara pidana.<sup>11</sup> 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:<sup>12</sup>

1. Dasar pembuktian yang tersimpul dalam pertimbangan keputusan pengadilan untuk memperoleh fakta-fakta yang benar (*bewijsgronden*).
2. Alat-alat bukti yang dapat digunakan oleh hakim untuk mendapatkan gambaran mengenai terjadinya perbuatan pidana yang sudah lampau (*bewijsmiddelen*).
3. Penguraian bagaimana cara menyampaikan alat-alat bukti kepada hakim di sidang pengadilan (*bewijsvoering*).
4. Kekuatan pembuktian dalam masing-masing alat-alat bukti dalam rangkaian penilaian terbuktinya suatu dakwaan (*bewijskracht*).
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*).

Dalam hukum pembuktian dikenal istilah *notoire feiten notorious* (*generally known*) yang berarti setiap hal yang sudah umum diketahui tidak lagi perlu dibuktikan dalam pemeriksaan sidang pengadilan.<sup>13</sup> Hal ini tercantum dalam Pasal 184 ayat (2) yang berbunyi, hal yang secara umum diketahui tidak perlu dibuktikan. Menurut Yahya Harahap, mengenai pengertian hal yang secara umum

---

<sup>11</sup> Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, Hlm. 245

<sup>12</sup> Bambang Poernomo, 2006. *Pokok-pokok Tata Cara Peradilan Indonesia*, Liberty, Jogjakarta, Hlm.39

<sup>13</sup> M.Yahya Harahap, 2006, *Pembahasan Permasalahan dan Penerapan KUHAP*, Edisi 2, Sinar Grafika, Jakarta, Hlm. 276.

sudah diketahui ditinjau dari segi hukum, tiada lain daripada perihal atau keadaan tertentu atau *omstandigheiden* atau *circumstances*, yang sudah sedemikian mestinya atau kesimpulan atau resultan yang menimbulkan akibat yang pasti demikian.<sup>14</sup>

Dalam penggunaan alat-alat bukti konvensional atas kejahatan terhadap kejahatan cyber, hakim memegang peranan penting dalam penyelesaian perkara dengan wajib menggali hukum yang hidup dalam masyarakat. Hakim harus membuat terobosan hukum jika belum ada undang-undang yang mengaturnya. Keyakinan hakim untuk menerima alat bukti di persidangan menjadi hal yang signifikan. Begitu pentingnya peran hakim dalam kasus *cyber crime*, hakim harus mempunyai kemampuan dalam ilmu teknologi informasi dan pandangan yang luas dalam penafsiran hukum.

Dalam teori pembuktian, KUHAP menggunakan sistem negatif *Wettelijk* yaitu hakim terikat pada alat bukti minimum ditambah keyakinan. Alat bukti di sini terikat pada apa yang ditentukan oleh undang-undang. Menurut A. Karim Nasution, istilah negatif *wettelijk* berarti *wettelijk* adalah berdasarkan Undang-Undang sedang negatif artinya bahwa walaupun dalam suatu perkara terdapat cukup bukti sesuai dengan undang-undang, maka hakim belum boleh menjatuhkan hukuman, sebelum ia yakin akan kesalahan terdakwa. Alat bukti yang sah menurut pasal 184 KUHAP adalah Keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Seperti yang sudah dijelaskan di atas, KUHAP menggunakan sistem negatif *wettelijk*, artinya alat bukti yang sah hanyalah alat bukti yang tertera dalam undang-undang saja.<sup>15</sup>

---

<sup>14</sup> *Ibid*, hlm. 276.

<sup>15</sup> Nasution, Karim A. 1996. *Masalah Hukum Pembuktian Dalam Proses Pidana*, Rajagrafindo Persada, Jakarta, hlm. 84.

Barang bukti dengan alat bukti mempunyai hubungan yang erat dan merupakan rangkaian yang tidak terpisahkan. Dalam persidangan setelah semua alat bukti diperiksa, selanjutnya dilanjutkan dengan pemeriksaan barang bukti. Barang bukti dalam proses pembuktian biasanya diperoleh melalui penyitaan. Dengan penyitaan maka penyidik akan mencari keterhubungan antara barang yang ditemukan dengan tindak pidana yang dilakukan.<sup>16</sup> Barang bukti mempunyai nilai/fungsi dan bermanfaat dalam upaya pembuktian, walaupun barang bukti yang disita oleh petugas penyidik tersebut secara yuridis formal bukan sebagai alat bukti yang sah menurut KUHAP. Akan tetapi, dalam praktik peradilan, barang bukti tersebut ternyata dapat memberikan keterangan yang berfungsi sebagai tambahan dari alat bukti yang sah dalam bentuk keterangan saksi, keterangan ahli (*visum et repertum*), maupun keterangan terdakwa. Misalnya sebuah benda berupa senjata api atau senjata tajam setelah disita menjadi barang bukti kemudian ditunjukkan dan ditanyakan kepada saksi dan saksi tersebut memberikan keterangan bahwa barang bukti tersebut oleh tersangka telah digunakan untuk melakukan pembunuhan atau penganiayaan. Demikian pula mayat korban pembunuhan setelah dilakukan pemeriksaan ilmiah oleh Ahli Kedokteran Kehakiman (Laboratorium Forensik) kemudian hasil pemeriksaannya dituangkan dalam *visum et repertum* yang isinya bersesuaian dengan keterangan saksi yang diperkuat oleh keterangan tersangka/terdakwa. Disamping itu, dengan diajakannya barang bukti di muka persidangan, maka hakim melalui putusannya dapat secara sekaligus menetapkan status hukum dari barang bukti yang bersangkutan, yaitu apakah diserahkan kepada pihak yang paling berhak menerimanya atau dirampas untuk kepentingan negara atau untuk dimusnahkan

---

<sup>16</sup>*Ibid*, hal. 447

atau dirusak sehingga tidak dapat dipergunakan kembali {Pasal 194 jo 197 ayat (1) huruf (i) KUHAP}.<sup>17</sup>

Dalam kasus *cyber crime*, proses penegakan hukum tidak dapat begitu saja dilepaskan dengan dalih kesulitan pada proses pembuktian. Apalagi jika terhadap perbuatan *cyber crime* tersebut telah dapat dikenakan delik-delik konvensional yang ketentuannya jelas dan tegas. Upaya yang dapat ditempuh adalah penelusuran bukti-bukti yang berkaitan dengan perbuatan pelaku *cyber crime* melalui jalur KUHAP. Artinya, bahwa tetap menggunakan alat-alat bukti berupa keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Minimalnya, kesalahan pelaku dapat terbukti dengan sekurang-kurangnya 2 (dua) alat bukti yang sah. Alat-alat bukti ini harus mampu membuktikan telah terjadi suatu perbuatan dan membuktikan adanya akibat dari perbuatan *cyber crime*.

Bukti-bukti elektronik (*Electronic Evidence*) yang digunakan untuk membuktikan perkara kejahatan dunia maya dalam pemeriksaan di Pengadilan adalah dapat berupa tampilan situs yang terkena *Deface* (yang dirubah tampilan *website*-nya) dan *Log-log file* (waktu terjadinya perbuatan tersebut) serta Internet Protocol (IP) yang dijadikan “tanda bukti diri” yang dapat mendeteksi pelaku kejahatan dunia maya atau *cyber crime* dan dapat menunjukkan keberadaan pengguna komputer itu sendiri. Dengan meneliti dan memeriksa pemilik nomor IP akan dapat diketahui lokasi pengguna IP tersebut.<sup>18</sup>

Kedudukan internet protokol sebagai alat bukti dalam kejahatan mayantara (*cyber crime*) adalah sebagai petunjuk dalam mencari kebenaran materiil dalam kasus kejahatan mayantara (*cyber crime*). Petunjuk diperoleh berdasarkan

---

<sup>17</sup> HMA. Kuffal, 2005, *Tata Cara Penggeledahan dan Penyitaan*, UMM Press, Malang, Hlm. 25-29.

<sup>18</sup> Ibid, hlm. 84.

keterangan saksi, surat, dan keterangan terdakwa. Implikasi yuridisnya adalah dengan digunakannya Internet Protokol sebagai alat bukti dalam tindak pidana kejahatan mayantara atau *cyber crime*, maka setiap orang yang melakukan tindak pidana tersebut dapat dikenakan pemidanaan.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 27-35, sebagai berikut :

- a. Pasal 27, menjelaskan tentang: Asusila (pornografi), Perjudian, Penghinaan, Pemeasaran.
- b. Pasal 28, menjelaskan tentang: Berita Bohong dan Menyesatkan, Berita Kebencian dan Permusuhan.
- c. Pasal 29, menjelaskan tentang: Ancaman Kekerasan dan Menakut-nakuti.
- d. Pasal 30, menjelaskan tentang: Akses Komputer Pihak Lain Tanpa Izin, *Cracking*. *Cracking* adalah kegiatan yang dilakukan oleh *cracker* untuk masuk ke dalam sebuah sistem komputer secara ilegal, dengan tujuan untuk merusak sistem keamanan suatu sistem komputer tersebut dan melakukan pencurian. *Cracking* ini berbeda dengan *hacking* yang dilakukan oleh seorang hacker, *cracker* ini adalah sifatnya merusak, sedangkan hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.
- e. Pasal 31, menjelaskan tentang: Penyadapan, Perubahan, Penghilangan Informasi.
- f. Pasal 32, menjelaskan tentang: Pemindehan, Perusakan dan Membuka Informasi Rahasia.
- g. Pasal 33, menjelaskan tentang : Virus, Membuat Sistem Tidak Bekerja atau *Denial of Service (DoS) Attack*. *DoS attack (Denial of Service)* merupakan

serangan yang bertujuan untuk melumpuhkan target (*hang, crash*) sehingga target tersebut tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial ataupun kerugian yang lainnya.

- h. Pasal 35, menjelaskan tentang : Menjadikan Seolah Dokumen Otentik (*phising*). *Phising* adalah kegiatan memancing pemakai komputer di internet (*user*) agar mau memberikan informasi data diri pemakai (*username*) dan kata sandinya (*password*) pada suatu *website* yang sudah di-*deface*. Sedangkan defacing adalah kegiatan mengubah halaman situs/*website* pihak lain.

#### **D. Kesimpulan dan Saran**

##### **1. Kesimpulan**

- a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur mengenai apa saja kriteria tentang alat bukti elektronik. Di dalam pasal-pasal undang-undang tersebut telah jelas menyebutkan dan mendefinisikan mengenai alat-alat bukti elektronik.
- b. Walaupun masih belum semuanya diatur mengenai perumusan-perumusan tentang alat bukti elektronik, akan tetapi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut merupakan payung hukum bagi penegakan *Cyber Law* di Indonesia.
- c. Kedudukan Internet Protokol sebagai alat bukti dalam kejahatan mayantara (*cyber crime*) adalah sebagai petunjuk dalam mencari kebenaran materiil dalam kasus kejahatan mayantara (*cyber crime*). Petunjuk diperoleh berdasarkan keterangan saksi, surat, dan keterangan terdakwa. Implikasi yuridisnya adalah dengan digunakannya Internet

Protokol sebagai alat bukti dalam tindak pidana kejahatan mayantara atau *cyber crime*, maka setiap orang yang melakukan tindak pidana tersebut dapat dikenakan pemidanaan.

## **2. Saran**

- a. Belum ada regulasi (kebijakan) yang secara jelas dan tegas mengatur mengenai bukti-bukti elektronik dalam hukum pembuktian di persidangan, maka seyogyanya hakim harus mencari dan menemukan hukumnya, yaitu melakukan penemuan hukum (*rechts-vinding*).
- b. Adanya kelemahan aparat penegak hukum yang gagap teknologi dalam penegakan hukum pidana khususnya perkara kejahatan mayantara menyebabkan semakin banyak kasus-kasus kejahatan mayantara yang tidak dapat dituntaskan. Untuk itu perlunya aparat penegak hukum (kepolisian, kejaksaan, kehakiman) dibekali keterampilan atau kemampuan menguasai teknologi komputer (internet) agar mampu menjadikan bukti elektronik sebagai alat bukti di persidangan.
- c. Hakim hendaknya menghukum seberat-beratnya pelaku kejahatan mayantara (*cyber crime*), karena sudah menggunakan intelektualitasnya untuk melakukan kejahatan dengan modus operandi yang merugikan orang lain.

## E. Daftar Pustaka

- Abdul Wahid dan Muhammad Habib. 2005. *Kejahatan Mayantara (Cyber Crime)*. Refika Aditama. Bandung..
- Ari Juliano Gema, dapat dilihat di <http://arijuliano.blogspot.com/2008/04/apakah-dokumen-lektronikdapat-menjadi.html>
- Furnell, Steven. 2002. *Cyber crime Vandalizing The Information Society*. Pearson Education Limited. USA.
- Hamzah, Andi. 2005. *Hukum Acara Pidana Indonesia*, Jakarta. Sinar Grafika.
- Harahap, M.Yahya. 2006. *Pembahasan Permasalahan dan Penerapan KUHAP*, Edisi 2, Jakarta. Sinar Grafika.
- HMA. Kuffal. 2005. *Tata Cara Penggeledahan dan Penyitaan*, Malang. UMM Press.
- <http://ern.pendis.depag.go.id/DokPdf/jurnal/6.%20Achmad%20Tahir.pdf>, diakses tanggal 25 Nopember 2011, jam 20.30 Wib.
- Marzuki, Peter Mahmud. 2008. *Penelitian Hukum*. Kencana Persada Media Group. Jakarta.
- Nasution, Karim A. 1996. *Masalah Hukum Pembuktian Dalam Proses Pidana*, Jakarta. Rajagrafindo Persada.
- Pitlo dalam Edmon Makarim. 2003. *Kompilasi Hukum Telematika*, Jakarta. Rajagrafindo Persada.
- Poernomo, Bambang. 2006. *Pokok-pokok Tata Cara Peradilan Indonesia*, Jogjakarta. Liberty.
- Subekti. R. 1995. *Hukum Pembuktian*. Pradnya Paramita. Jakarta
- Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP).
- Widyopramono. 1994. *kejahatan di Bidang Komputer*. Pustaka Sinar Harapan. Jakarta.