



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

- a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
- b. Pengutipan tidak merugikan kepentingan yang wajar Unand.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Unand.

PERANAN PENYELENGGARAAN SISTEM ELEKTRONIK DALAM PEMBUKTIAN ALAT BUKTI ELEKTRONIK TINDAK PIDANA MAYANTARA DI INDONESIA

SKRIPSI



ARISMAN

06 940 055

**PROGRAM STUDI HUKUM
FAKULTAS HUKUM
UNIVERSITAS ANDALAS
PADANG 2011**



Tiada kuasa yang lebih maha selain Allah

Seluruh kehidupan selalu atas kuasa-Nya

Puji bagimu ya Allah.....

Atas semua yang Engkau berikan

Selangkah tapakku mulai kulangkahkan

Menuju bagian baru dalam kehidupanku

Terima kasih ya allah atas ilmu yang Kau berikan

Dan akan selalu kusyukuri ilmu yang kuperoleh

“Allah akan mengangkat orang-orang yang beriman di antara kamu dan orang-orang yang berilmu pengetahuan beberapa derajat” (Al-Mujadalah 58/11).

Tak lupa saya ucapakan, thank's to:

My family, ibuku Zetri Dewita, ayahku Samardi Panut (alm) yang tidak bisa melihat kelulusanku, kakakku Kaltrisman dan adikku Joko Sumarta.

Rekan-rekan selama kuliah, anak-anak geng 06, Hendra Goreng, Hendra Brow, Mas Her, Toge, Jac, Petruk, Bams (bam Samson imitasi), Havid, Amin, Adit Langang, Agung, Mamak (angkatan 03), bang toyo (angkatan 03), Dan friend lainnya yang tak tersebut.

Tidak lupa pula teman-teman diluar perkuliahan, Yuri Papercraft (insya allah kita akan jadi rokstar bro), Ikhsan “seakan-akan”, Raga Qhiting, Pink Power, Bony, Cuk'en, Hendrik Pakpol (rekan-rekan bandku selama SMA), dan brow-brow lainnya yang membantu memotifasiku.

**PERANAN PENYELENGGARA SISTEM ELEKTRONIK
DALAM PEMBUKTIAN ALAT BUKTI ELEKTRONIK
TINDAK PIDANA MAYANTARA DI INDONESIA**

(Arisman, 06940055, Fakultas Hukum Reguler Mandiri Universitas Andalas, 79 Halaman, 2011)

ABSTRAK

Adanya kemajuan yang dicapai dalam bidang teknologi informasi dan komunikasi telah memunculkan *cyber space*. *Cyber space* menawarkan manusia untuk "hidup" dalam dunia alternatif yang penuh dengan harapan, kesenangan, kemudahan dan pengembaraan seperti komunikasi, informasi, kegiatan perdagangan, ataupun transaksi elektronik dan lain-lain. Dalam *cyber space* juga terdapat sisi gelap yang disebut pula dengan tindak pidana mayantara. Tindak pidana mayantara merupakan fenomena yang timbul akibat penyelewengan pemanfaatan *cyber space* yang mengakibatkan kerugian ataupun efek negatif bagi orang lain atau masyarakat. Penegakan hukum tindak pidana mayantara di Indonesia masih cukup sulit, oleh karena penemuan alat buktinya berupa elektronik masih sangat lemah di persidangan. Untuk itulah perlu adanya alat bukti lain yang dapat memperkuat alat bukti elektronik tersebut, sehingga barulah alat bukti ini dapat memiliki keabsahan di persidangan. Peran Penyelenggara Sistem Elektronik dalam menyelenggarakan Sistem Elektronik sangat berguna untuk memberikan kekuatan dan kejelasan terhadap alat bukti elektronik. Hal itu disebabkan karena alat bukti elektronik berasal dari Sistem Elektronik yang dijalankan oleh Penyelenggara Sistem Elektronik. Adapun metode penelitian yang digunakan adalah menggunakan pendekatan masalah yuridis normatif yaitu dengan melihat hubungan antara aspek-aspek hukum terhadap peranan Penyelenggara Sistem Elektronik dalam penemuan alat bukti elektronik. Jenis data yang digunakan dalam penelitian ini mencakup data primer yang didapat langsung dari penelitian dan data sekunder Merupakan informasi-informasi dari bahan studi kepustakaan yang dijadikan data bagi penelitian. Sedangkan teknik pengumpulan data adalah teknik studi dokumen yang digunakan untuk memperoleh informasi dari buku-buku, dokumen-dokumen, surat-surat, memo-memo, dan bahan tertulis lainnya yang berkaitan dengan penelitian. Kemudian data yang diperoleh diolah dan di analisis secara kualitatif sehingga mendapatkan informasi yang tepat. Setelah melakukan penelitian didapatlah hasil penelitian: pertama, Penyelenggara Sistem Elektronik memiliki tanggung jawab terhadap Sistem Elektroniknya berdasarkan pasal 15 Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, sehingga dapat mengetahui dan bertanggung jawab terhadap beroperasi sistem tersebut. Oleh sebab itu ketika terjadi tindak pidana mayantara dalam Sistem Elektroniknya, PSE dianggap tahu dan memperlihatkan terpenuhinya syarat sebagai saksi dalam Kitab Undang-Undang Hukum Acara Pidana. Kedua, Penyelenggara Sistem Elektronik merupakan pihak dapat dimintai keterangannya mengenai alat bukti ataupun petunjuk-petunjuk baru untuk menemukan alat bukti ataupun jejak pelaku. Ketiga, Penyelenggara Sistem Elektronik juga merupakan pihak yang memberikan keabsahan terhadap alat bukti elektronik dalam persidangan seperti diperlukannya berita acara pengalihan dokumen elektronik di persidangan.

THE ROLE PROVIDER ELECTRONIC SYSTEM IN VERIFICATION APPLIANCE EVIDENCE ELECTRONIC DOING A CYBER CRIME IN INDONESIA

(Arisman, 06940055, Faculty Of Law Regular Independent Of Andalas University, Pages
79 , 2011)

ABSTRACT

The existence of the progress made in the field of information and communication technology have led to cyber space. Cyber space offers a man to "live" in the alternate world full of hope, pleasure, convenience and wanderings, such as communication, information, trade events, or electronic transactions and others. In cyber space there is also a dark side which is also called the cyber crime. Cyber crime is a phenomenon arising from the misuse of cyber space utilization resulting in losses or negative effects for others or the public. Mayantara criminal law enforcement in Indonesia is still quite difficult, because the evidence in the form of an electronic discovery tool is still very weak in the trial. For that there needs to be other evidence that can strengthen the electronic evidence, so then this evidence may have validity in court. Role Providers Electronic Systems Electronic Systems in organizing very useful to provide the strength and clarity of electronic evidence. That's because electronic evidence comes from the Electronic Systems Electronic Systems is run by the Operator. The research method is using a normative juridical approach to the problem by looking at the relationship between aspects of laws with the implementation of Electronic System Operator in the discovery of electronic evidence, the type of data used include the primary data obtained directly from research and secondary data is information from literature study material which is used as data for research. While the data collection technique is document study technique, used to obtain information from books, documents, letters, memos, and other written materials relating to the research. Then the data obtained are processed and analyzed qualitatively so getting the right information. After doing research, the results of the first study, Electronic System Operator has responsibility for electronic system based on Article 15 of Law No. 11 Year 2008 About Information And Electronic Transactions, in order to know and be responsible for operating the system. Therefore, when the cyber crime occurred in electronic system, PSE is considered to know and demonstrate the fulfillment of conditions as witnesses in the draft Criminal Procedure Code. Second, the Electronic System Operator is a party to questioning about the evidence or new clues to find the evidence or trace the perpetrators. Third, the Electronic System Operator is also the party providing the validity of electronic evidence in a trial such as the need for the minutes of the transfer of electronic documents in court.

KATA PENGANTAR

Alhamdulillahirabbil'alamin. Segal puji bagi Allah, Tuhan semesta alam, berkat rahmat-Nya penulis dapat menyelesaikan penulisan skripsi ini yang berjudul "Peran Penyelenggara Sistem Elektronik Dalam Menemukan Alat Bukti Elektronik Tindak Pidana Mayantara" dibuat sebagai persyaratan untuk mendapat gelar sarjana di Fakultas Hukum Reguler Mandiri Universitas Andalas. Dalam penulisan ini, penulis mendapat banyak bantuan dari berbagai pihak.

Pada kesempatan ini perkenankan penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Terima kasih tak terhingga penulis aturkan kepada kedua orang tua penulis yang telah bayak memberikan kasih sayang, pengorbanan, do'a dan nasehat pada penulis dalam proses pembuatan skripsi ini. Tiada satu katapun yang berharga dapat penulis persembahkan kepada semuanya kecuali anturan do'a semoga amal budi baik beliau dibalas oleh Allah SWT.
2. Bapak Prof. Dr. Yuliandri, SH. MH sebagai Dekan Fakultas Hukum Universitas Andalas.
3. Bapak Yoserwan, SH. MH. LLM sebagai Pembantu Dekan I Fakultas Hukum Universitas Andalas.
4. Bapak Frenadin Ade Gustara, SH. MS sebagai Pembantu Dekan II Fakultas Hukum Universitas Andalas.

5. Bapak Dr. Kurniawarman, SH. MH sebagai Pembantu Dekan III Fakultas Hukum Andalas.
6. Bapak Apriwal Gusti, SH sebagai Ketua Program Reguler Mandiri Fakultas Hukum Universitas Andalas.
7. Ibuk Afriani, SH. MH sebagai sekretaris Program Reguler Mandiri Fakultas Hukum Universitas Andalas.
8. Bapak Prof. Dr. Ismansyah, SH. MH sebagai Ketua Bagian Hukum Pidana dan sekaligus Pembimbing I penulisan skripsi penulis.
9. Ibuk Nani Mulyati, SH. MCL sebagai Pembimbing II penulisan skripsi penulis.
10. Ibuk Elfren Nova, SH. MH sebagai sekretaris Bagian Hukum Pidana Fakultas Hukum Universitas Andalas.
11. Semua Dosen dan pegawai yang berada pada lingkup Fakultas Hukum Reguler Mandiri Universitas Andalas.
12. Ibuk Adelia, SH Sebagai jaksa Muda Pidana Khusus di Kejaksaan Negeri Padang.
13. Bapak Muhammad Nazif, SH sebagai Kepala Sub Bagian Pembinaan di Kejaksaan Negeri Padang.
14. Pegawai Kejaksaan Negeri Padang.
15. Saudara Sukmi Tumi Pengata, SH sebagai salah-satu penyelenggara Web Persatuan Mahasiswa Hukum Indonesia (PERMAHI) cabang Padang.

16. Saudara Yuri Hendriyanto, S.Kom sebagai *Web Design*.

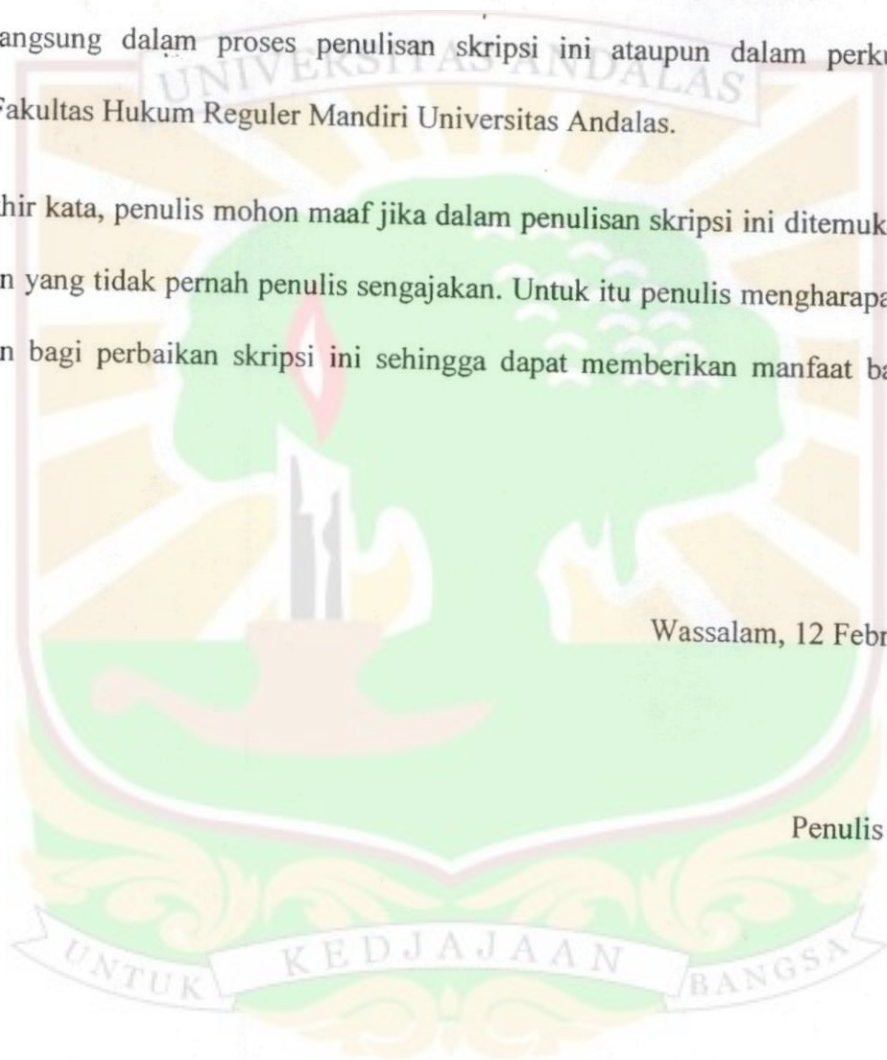
17. Semua teman-teman penulis angkatan 2006 ataupun rekan angkatan lainnya yang telah memberikan semangat pada penulis untuk selalu berjuang.

18. Serta semua yang membantu penulis baik secara langsung ataupun secara tidak langsung dalam proses penulisan skripsi ini ataupun dalam perkuliahan di Fakultas Hukum Reguler Mandiri Universitas Andalas.

Akhir kata, penulis mohon maaf jika dalam penulisan skripsi ini ditemukan banyak kesalahan yang tidak pernah penulis sengajakan. Untuk itu penulis mengharapkan kritik dan saran bagi perbaikan skripsi ini sehingga dapat memberikan manfaat bagi semua orang.

Wassalam, 12 Februari 2011

Penulis



DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	iii
DAFTAR ISI	vi
BAB I PENDAHULUAN	
A. Latar Belakang.....	1
B. Perumusan Masalah.....	11
C. Tujuan Masalah.....	12
D. Manfaat Penulisan.....	12
E. Kerangka Teoritis dan Konseptual.....	13
F. Metode Penelitian.....	17
BAB II TINJAUAN KEPUSTAKAAN	
A. Perkembangan Secara Umum Mengenai Tindak Pidana Mayantara.....	20
1. Istilah Dan Pengertian.....	21
2. Perkembangan Tindak Pidana Mayantara.....	22
B. Bentuk-Bentuk Tindak Pidana Mayantara.....	26
1. Tindak Pidana Mayantara Di Bidang Pornografi.....	26
2. Tindak Pidana Mayantara Di Bidang Perbankan.....	29
3. <i>Hacking, Cracking, Dan Viruses</i>	30
4. <i>Piracy</i> (Pembajakan).....	33
5. <i>Criminal Communication</i>	34
C. Alat Bukti Elektronik Dalam Sistem Hukum Di Indonesia.....	34
1. Asas-Asas Pembuktian Untuk Alat Bukti Elektronik.....	34
2. Alat Bukti Elektronik Dalam Beberapa Undang Undang.....	37

D. Pihak-Pihak Dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.....	42
1. Penyelenggara Sistem Elektronik.....	42
2. Penyelenggara Agen Elektronik.....	43
3. Penyelenggara sertifikat Elektronik.....	43
4. Lembaga Setifikat Keandalan.....	44
5. Penanda Tangan.....	44
6. Pengirim Dan Penerima.....	45
7. Badan Usaha.....	46

BAB III PEMBAHASAN

A. Kedudukan Hukum Penyelenggara Sistem Elektronik Dalam Penyelenggaraan Sistem Elektronik.....	47
1. Syarat Penyelenggaraan Sistem Elektronik.....	47
2. Tanggung Jawab Penyelenggara Sistem Elektronik.....	54
B. Peranan Penyelenggara Sistem Elektronik Dalam Menemukan Alat Bukti Elektronik.....	64
C. Pentingnya Keterangan Penyelenggara Sistem Elektronik Terhadap Kekuatan Suatu Alat Bukti Elektronik.....	68

BAB IV PENUTUP

A. Kesimpulan.....	76
B. Saran.....	77

DAFTAR PUSTAKA

LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang

Kemajuan ilmu pengetahuan sekarang ini telah memberikan perkembangan terhadap dunia informasi dan telekomunikasi. Di antara perkembangan di bidang informasi dan telekomunikasi yang dapat dirasakan manfaatnya secara nyata adalah dengan munculnya teknologi informasi. Teknologi informasi telah memberikan pengaruh terhadap gaya hidup manusia dalam berinteraksi dan komunikasi. Diantara perwujudan teknologi informasi yang dapat dirasakan adalah adanya internet. Internet (*interconnected Network*) adalah konvergensi telematika yang merupakan perpaduan antara teknologi komputer, media dan teknologi informasi.¹ Teknologi informasi dengan memanfaatkan media internet telah mengubah kebiasaan masyarakat dalam memperoleh informasi yang dulunya hanya melalui media cetak, sekarang mulai berkembang ke arah media elektronik dengan memanfaatkan perangkat lunak/komputer.

Dalam dekade tahun 2000, jaringan internet telah berkembang sangat pesat. Arah pengembangan telah mencakup ribuan bahkan jutaan jaringan komputer independent yang dihubungkan satu dengan yang lainnya dan menuju sistem jaringan komputer/internet dengan mobilitas tinggi.² Fenomena ini telah membawa masyarakat ke dalam dunia baru yang disebut *cyber space* atau dunia maya, dimana tidak ada batasan

¹ Suhartono, *Penanggulangan Kejahatan Hacking Di Indonesia (Suatu Kajian dalam Perspektif Kebijakan Hukum Pidana : Saat ini dan Wacana Kebijakan Hukum Pidana Akan Datang)*. <http://www.google.com> dari suhartono_71@yahoo.com, Diakses tanggal 29 September Tahun 2009, hal. 2.

² Abdul Wahid dan Mohammad Labib, 2005. *Kejahatan Mayantara (Cyber Crime)*. Jakarta: Refika Aditama, hal. 4.

lagi dalam mendapat informasi dan komunikasi, dimanapun dan kapanpun pengguna teknologi informasi dapat mengakses informasi secara bebas.

Internet telah memberikan peluang bagi sebagian pihak untuk memanfaatkannya lebih banyak lagi dengan menggunakan Sistem Elektronik. Menurut Pasal 1 Butir 5 Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik. Dengan menggunakan Sistem Elektronik sebagai fasilitas dan jaringan internet sebagai media, membuat kegiatan di dunia maya semakin beragam, seperti Transaksi Elektronik, kegiatan komunikasi elektronik dan perdagangan elektronik (*E-commerce*). perdagangan elektronik contohnya, yang memungkinkan seseorang dapat melakukan kegiatan jual-beli dimanapun dan kapanpun berada. Dengan begitu kegiatan perdagangan elektronik dapat menghemat waktu, tenaga dan biaya sehingga transaksi dapat dilakukan dengan cepat. Selain itu, kegiatan-kegiatan tersebut juga memberikan dampak pada peningkatan fungsi dari sebuah internet, bukan hanya sebagai wadah informasi tetapi juga menjadi dunia komunikasi dalam interaksi dunia maya.

Seiring peningkatan fungsi sebuah internet sebagai sarana pengaksesan informasi secara bebas, internet juga sering dimanfaatkan oleh sebagian pihak untuk sarana memperoleh keuntungan dan kepentingan dirinya sendiri dengan menggunakan Sistem Elektronik, sehingga mengakibatkan timbulnya kerugian bagi pengguna internet atau orang lain baik berupa materil maupun formil. Penyalahgunaan tersebut sangat meresahkan masyarakat pengguna teknologi informasi, bukan hanya karena sarana yang digunakan adalah menggunakan internet yang dimana hampir setiap lapisan masyarakat

memanfaatkannya, melainkan perbuatan ini juga mengakibatkan kerugian materil yang cukup besar. Perbuatan ini disebut juga dengan tindak pidana mayantara.

Tindak pidana mayantara adalah istilah bahasa Indonesia yang dipakai oleh Barda Nawawi Arief dalam mendefinisikan kejahatan dibidang mayantara atau komputer. Sebenarnya selain tindak pidana mayantara masih banyak lagi istilah lain yang dipakai oleh para ahli hukum Indonesia dalam mendefinisikan perbuatan tersebut diantaranya, *cyber crime* digunakan oleh Agus Raharjo, M. Ramli Ahmad dan Heru Sutadi, kejahatan mayantara oleh Abdul Wahid dan Muhammad Labib, tindak pidana di dunia *cyber* oleh Indra Safitri dan masih banyak lagi istilah lainnya.

Di dunia internasional istilah tindak pidana mayantara tersebut juga terdapat beragam istilah. Diantaranya dalam dua dokumen Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian tindak pidana mayantara, yaitu *cyber crime* dan *computer related crime*. Dalam *back ground paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah tindak pidana mayantara juga dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*. Kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut:³

1. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of*

³ Barda Nawawi Arief, 2007. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana Predana Media Group, hal. 24.

computer system and the data processed by them, yang artinya *cyber crime* dalam arti sempit (kejahatan komputer): setiap perilaku sah yang diarahkan pada operasi elektronik yang targetnya keamanan komputer dan pemrosesan data didalamnya.

2. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network*, yang artinya *cyber crime* dalam arti luas (kejahatan terkait dengan komputer): setiap perilaku yang tidak sah yang dilakukan dalam hubungannya dengan, suatu sistem komputer atau jaringan, mencakup kepemilikan tidak sah, atau menyebarkan informasi atas bantuan sistem komputer atau jaringan.

Tindak pidana mayantara memiliki berbagai bentuk perbuatan antara lain, *hacking, cracking, viruses, booting, troyan horse, spamming* dan lain sebagainya. Diantara bentuk tindak pidana mayantara tersebut, *hacking* adalah salah-satu perbuatan yang paling meresahkan masyarakat pengguna teknologi informasi. Hal ini dikarenakan *hacking* menyangkut pembobolan Sistem Elektronik milik orang lain, dimana di dalam sistem tersebut tersangkut hal-hal yang sangat penting dan rahasia. Mengenai tata cara *hacking* dapat dilihat dari beberapa tahapan-tahapan berikut ini:⁴

⁴ Deris Setiawan, 30 Agustus 2003. *Bagaimana Menjadi Hacker (Talk Show Computer Easy di Radio SONORA FM)*. Kerjasama Radio SONORA FM dan PT. Elex Media Komputindo, hal. 4.

1. *Foot printing*. Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi baik dengan cara sederhana maupun menggunakan *software* seperti *search engine*, *whois* dan *DNS zone transfer*, contoh: mencari informasi seperti tanggal lahir, nama, hobi dari pemilik akun Sistem Elektronik.
2. *Scanning*. Terhadap sasaran tertentu dicari pintu masuk yang paling mungkin untuk dimasuki, biasanya bagian Sistem Elektronik paling lemah *vulnerability holes* (celah kelemahan suatu program) digunakan *ping sweep* dan *port scan*.
3. *Enumeration*. Menelaah intensif komputer sasaran, contoh; mencari *user account* yang absah, *network resource and share*, dan aplikasi untuk mendapatkan bagian yang proteksinya lemah.
4. *Gaining Access*. Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran, meliputi mengintip dan merampas *password*, menebak *password* berdasarkan *foot printing*, serta melakukan *buffer overflow* (aplikasi penyangga jika lupa *password*).
5. *Escalating Privilege*. Bila sudah mendapatkan user password, ditahap ini diusahakan mendapatkan *privillage admin* (usaha untuk mendapatkan akses admin) dengan mencoba *password cracking* atau *exploit*.
6. *Pilfering*. Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses *trusted system* (akses penyelenggara sistem) .

7. *Covering Tracks*. Begitu control penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan *network log* atau informasi yang tertinggal dari admin.
8. *Creating Backdoors*. Pintu belakang diciptakan pada berbagai bagian sistem untuk memudahkan masuk kembali ke sistem ini dengan membentuk *user account* palsu, dan menambahkan service lainnya.
9. *Denial of Service*. Bila usaha diatas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Meliputi SYN flood, teknik ICMP, dan lain-lain.

Tindak pidana mayantara sekarang ini telah menjadi perhatian serius bagi masyarakat termasuk dunia internasional. Perhatian internasional mengenai tindak pidana mayantara diantaranya ditunjukkan dengan diselenggarakannya ITAC (*Information Technology Association of Canada*) pada *International Information Industry Congress (IIIC) 2000 Millenium Congress* di Quebec pada tanggal 19 September tahun 2000 and *social development*, yang menyatakan bahwa “*cyber crime is real and growing threat to economic around the world.*” *Information technology touches every aspect of human life and so can electronically enable crime.* Sehubungan dengan kekhawatiran akan ancaman/bahaya tindak pidana mayantara ini karena berkaitan erat dengan *economic crimes and organized crime*, kongres PBB mengenai *The Prevention of crime and the treatment of offender* (yang diselenggarakan tiap lima tahun) telah pula ini diagendakan, yaitu pada kongres VII/1990 di Havana dan pada kongres X/2000 di Wina.⁵

⁵ ITAC, 2000. *IIIC Common Views Paper On: Cyber Crime*. IIIC 2000 Millenium Congress, September 19th, hal. 2.

Di Indonesia masalah mengenai tindak pidana mayantara juga telah menjadi perhatian khusus. Dibuktikan dengan disahkannya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, telah menjadikan tindak pidana mayantara sebagai perbuatan dilarang dan mempunyai sanksi pidana.

Walaupun telah ada aturan yang mengatur tindak pidana mayantara, tetapi tetap saja masih terdapat kesulitan-kesulitan/hambatan-hambatan dalam penegakan hukumnya. Dokumen Kongres PBB X/2000 sendiri mengakui bahwa ada beberapa kesulitan dalam menanggulangi tindak pidana mayantara dengan sarana penal, antara lain:⁶

1. Perbuatan jahat yang dilakukan berada di lingkungan elektronik. Oleh karena itu penanggulangan tindak pidana mayantara memerlukan keahlian khusus, prosedur investigasi dan kekuatan/dasar hukum yang mungkin tidak tersedia di negara yang bersangkutan, sehingga menimbulkan kesulitan dalam menemukan alat bukti;
2. Tindak pidana mayantara melampaui batas-batas negara, sedangkan upaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah teritorial negaranya sendiri;
3. Struktur terbuka dari jaringan komputer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum (negara) yang belum mengkriminalisasikan tindak pidana mayantara. Terjadi "*data havens*" (negara tempat berlindung/singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha negara lain untuk memberantas kejahatan itu.

⁶ Barda Nawawi Arif, 1991. *Dalam United Nations (Eighth UN Congress On The Prevention Of Crime And The Treatment Of Offenders Report)*, hal. 9.

Pemerintah dalam hal ini telah menyadari kelemahan-kelemahan/hambatan-hambatan tersebut. Untuk itu dengan memperbaharui proses penyidikan seperti kerjasama dengan ahli telematika dan penyidik negara lain akan dapat mengatasi kelemahan-kelemahan tersebut. Selain upaya kerjasama dengan berbagai pihak, dalam penegakannya diperlukan juga alat bukti baru untuk menjangkau tindak pidana mayantara yang berada pada lingkungan elektronik. Oleh karena itu alat bukti dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa, tidaklah cukup dalam penegakan hukumnya.

Pembuktian dalam hukum pidana merupakan subsistem kebijakan kriminal sebagai *science of response* yang mencakup berbagai disiplin ilmu.⁷ Dengan mengacu pada hal tersebut dapat disimpulkan bahwa alat bukti dalam penegakan hukum sebenarnya dapat dikembangkan sesuai dengan disiplin ilmu yang telah berkembang di dunia dengan memegang teguh prinsip-prinsip logika, dimana batasan alat bukti tersebut mengandung dalil-dalil yang masuk akal.

Pasal 44 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah menetapkan sistem pembuktian baru untuk tindak pidana mayantara berdasarkan dalil masuk akal sesuai disiplin ilmu yaitu:

- a. Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
- b. Alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

⁷ M. Yahya Harahap, 2000. "*Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*", Edisi Kedua. Jakarta: Sinar Grafika, hal. 251.

Penemuan alat bukti adalah hal yang terpenting dalam penegakan hukum pidana termasuk tindak pidana mayantara. Namun bagi alat bukti elektronik sedikit rumit, hal itu disebabkan karena alat bukti elektronik tidak dapat berdiri sendiri dan membutuhkan alat bukti lainnya untuk memperoleh keyakinan bahwa suatu tindak pidana benar-benar telah terjadi atau sah oleh hakim.⁸ Misalnya keterangan saksi yang mengetahui pembuatan E-mail atau keterangan saksi ahli yang menerangkan keaslian E-mail sebagai suatu alat bukti bagi pihak-pihak yang terkait dengan tindak pidana mayantara.

Penyelenggara Sistem Elektronik (selanjutnya disebut PSE) adalah sebagian pihak yang memiliki andil dalam memberikan kedudukan terhadap alat bukti khususnya alat bukti elektronik. Hal ini dikarenakan PSE merupakan pihak yang menyelenggarakan Sistem Elektronik tempat Informasi dan Dokumen Elektronik didapat. Menurut Pasal 1 butir 6 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat. Sebagai pihak yang memiliki kewenangan dalam menyelenggarakan Sistem Elektronik untuk pengguna Sistem Elektronik, PSE memiliki kewenangan dan dianggap mengetahui terhadap semua Informasi Elektronik yang terdapat dalam Sistem Elektronik yang diselenggarakannya. Penyelenggaraan Sistem Elektronik sendiri oleh PSE dapat berupa kegiatan perbankan oleh bank-bank seperti BCA, Mandiri, juga perdagangan elektronik seperti Plasa.com, dan kegiatan Informasi Elektronik lainnya.

Mengenai pentingnya peranan PSE dapat dilihat dari kasus www.anshar.net tahun 2007, dimana situs ini diduga digunakan untuk menyampaikan informasi terorisme atas pesanan Noordin M. Top sebagai media informasi perjuangannya. Isi dari informasi para

⁸ Barda Nawawi Arief, 2006. *Tindak Pidana Mayantara (Perkembangan Kajian Cyber Crime Di Indonesia)*. Jakarta: PT Raja Grafindo Persada, hal. 45.

teroris itu seputar materi-materi Tauziah Syaikh Mukhlas, Tauhid, Jihad, Wacana, Islamiah dan Askariah, antara lain mengajarkan penyerangan dengan cara memanfaatkan antrian di jalan atau pintu masuk atau keluar kantor, pusat perbelanjaan, hiburan, olahraga, hotel dan tempat pameran. Kasus tersebut tengah dalam proses persidangan di Pengadilan Negeri Semarang dengan Nomor Perkara 84/PID/B/2007 PN SMG. Dalam pemeriksaan Agung Setyadi dan M. Agung Prabowo Max Fiderman alias Kalingga alias Maxhaser, mahasiswa salah satu universitas di kota Semarang sebagai Penyelenggara anshar.net dimintai keterangannya terkait alat bukti elektronik yang mengarah pada mereka sebagai pihak mengetahui tentang adanya upaya terorisme.⁹

Dalam kasus diatas tersirat keterangan mengenai keterkaitan PSE terhadap alat bukti khususnya elektronik. Secara garis besar tindak pidana mayantara terdiri dari dua jenis, yaitu kejahatan yang menggunakan teknologi informasi/Sistem Elektronik sebagai fasilitas dan kejahatan yang menjadikan Sistem Elektronik/fasilitas Teknologi Informasi sebagai sasaran.¹⁰ Peranan PSE dalam penemuan alat bukti dapat dilihat dari hal tersebut, dimana PSE adalah Penyelenggara Sistem Elektronik dan tindak pidana mayantara menyangkut Sistem Elektronik. Oleh sebab itu ketika terjadi tindak pidana mayantara, PSE memiliki kaitan yang penting terlebih ketika dikaitkan dengan Pasal 15 ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Eletronik yang menyatakan Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya. Berdasarkan hal itu PSE dapat diposisikan sebagai pihak yang mengetahui dan terkait dengan penemuan alat bukti elektronik.

⁹ Rakyat Merdeka, 24 Agustus 2006. *Teroris Semarang Terlibat Anshar.Net*. <http://www.rakyatmerdeka.co.id>. Diakses tanggal 30 Desember 2009.

¹⁰ Abdul Wahid dan Mohammad Labib. *Op.cit*, hal. 26.

Di negara dengan tradisi Common Law, memiliki kecenderungan prinsip pertanggungjawaban bergeser menuju prinsip pertanggungjawaban mutlak atau *strict liability*. Pertanggungjawaban mutlak maksudnya suatu tindakan dapat dihukum atas dasar perilaku yang merugikan (*harmful conduct*) tanpa mempersoalkan ada tidaknya kesengajaan (*intention*) atau kelalaian (*negligence*).¹¹ Prinsip ini menegaskan adanya hubungan kausalitas antara subjek yang bertanggung jawab dan kesalahan dibuatnya baik karena kelalaian ataupun kesalahan, dengan memperhatikan adanya *force majeure* sebagai faktor yang dapat melepaskan diri dari tanggung jawab. Pertanggungjawaban mutlak diutamakan diterapkan terhadap Sistem Elektronik yang berdampak besar, dan berpotensi merugikan kepentingan umum yang lebih luas. Pertanggungjawaban mutlak yang dibebankan tersebut mengakibatkan adanya suatu kewajiban pemberian bantuan dalam penemuan alat bukti oleh PSE sebagai bentuk tanggung jawab terhadap Sistem Elektronik yang diselenggarakannya.

Berdasarkan uraian di atas, penulis merasa tertarik untuk mengkaji dan membahas masalah ini kedalam suatu tugas akhir dengan judul “PERANAN PENYELENGGARA SISTEM ELEKTRONIK DALAM PEMBUKTIAN ALAT BUKTI ELEKTRONIK TINDAK PIDANA MAYANTARA DI INDONESIA.”

B. Perumusan Masalah

Perumusan masalah sangatlah penting untuk menentukan mengenai apa saja hal yang akan dituangkan dalam suatu penelitian. Adapun permasalahan yang ingin dibahas dalam penulisan skripsi ini adalah:

¹¹ Agus Santoso dan Dyah Pratiwi, Desember 2008. *Tanggung Jawab Penyelenggara Sistem Elektronik Perbankan Dalam Kegiatan Transaksi Elektronik pasca Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik*. Jurnal Legislasi Indonesia Vol 5 No 4, hal. 82.

1. Bagaimanakah kedudukan hukum Penyelenggara Sistem Elektronik dalam Penyelenggaraan Sistem Elektronik ketika telah terjadi tindak pidana mayantara di Sistem Elektroniknya?
2. Seberapa besar peranan Penyelenggara Sistem Elektronik dalam pembuktian suatu alat bukti elektronik?
3. Terkait dengan keabsahan dari alat bukti elektronik, Sejauh mana pentingnya keterangan Penyelenggara Sistem Elektronik terhadap kekuatan hukum suatu alat bukti elektronik?

C. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1. Untuk mengetahui kedudukan hukum Penyelenggara Sistem Elektronik dalam Penyelenggaraan Sistem Elektronik ketika telah terjadi tindak pidana mayantara di Sistem Elektroniknya.
2. Untuk mengetahui peranan Penyelenggara Sistem Elektronik dalam pembuktian suatu alat bukti elektronik.
3. Untuk mengetahui pentingnya pemberian keterangan oleh Penyelenggara Sistem Elektronik terhadap kekuatan dan keabsahan suatu alat bukti elektronik.

D. Manfaat Penelitian

Didalam sebuah penelitian penulis tentunya mempunyai harapan agar penelitian ini dapat bermanfaat bagi penulis ataupun orang banyak. Adapun manfaat dari penulisan ini adalah:

1. Manfaat Teoritis

- a. Menambah pengetahuan penulis mengenai kedudukan Penyelenggara Sistem Elektronik dalam Penyelenggaraan Sistem Elektronik ketika telah terjadi tindak pidana mayantara di Sistem Elektroniknya.
- b. Menambah pengetahuan penulis mengenai peranan Penyelenggara Sistem Elektronik dalam pembuktian suatu alat bukti elektronik.
- c. Menambah pengetahuan penulis mengenai arti penting keterangan Penyelenggara Sistem Elektronik terhadap kekuatan alat bukti elektronik.

2. Manfaat Praktis

- a. Memberikan pengetahuan kepada pembaca mengenai pentingnya peranan Penyelenggara Sistem Elektronik dalam penegakan hukum terhadap tindak pidana mayantara.

E. Kerangka Teoritis dan Konseptual

1. Kerangka Teoritis

Penulisan ini diberi judul “PERANAN PENYELENGGARA SISTEM ELEKTRONIK DALAM PEMBUKTIAN ALAT BUKTI ELEKTRONIK TINDAK PIDANA MAYANTARA DI INDONESIA” dimana pada latar belakang telah dijelaskan pengangkatan judul ini didasari beberapa masalah yang menarik dibahas dan diteliti.

Pada kerangka teoritis, penulis membuat beberapa ruang lingkup pembahasan terhadap bahan-bahan hukum yang terkait dengan penelitian ini. Bahan-bahan hukum

tersebut khususnya bahan hukum primer yang terdiri atas perundang-undangan yang mana pasal-pasalanya terkait dengan penelitian ini:

a. Undang-Undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Dalam Bab IV bagian kedua Pasal 15, dikatakan bahwa:

- 1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
- 2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
- 3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Ketentuan dalam pasal diatas menegaskan adanya pertanggungjawaban Penyelenggara Sistem Elektronik terhadap Sistem Elektronik yang diselenggarakannya. Pertanggungjawaban ini dapat bergeser kearah koordinasi dengan penegak hukum baik sebagai saksi maupun korban sesuai yang diamanatkan Kitab Undang-Undang Hukum Acara Pidana.

b. Bahan hukum lainnya yang terkait dengan peranan Penyelenggara Sistem Elektronik dalam pembuktian alat bukti elektronik untuk tindak pidana mayantara di Indonesia diantaranya:

- 1) Undang-Undang Nomor 7 Tahun 1992 jo Undang-Undang No.10 Tahun 1998 Tentang Perbankan.
- 2) Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan.
- 3) Kitab Undang-Undang Hukum Pidana dan Kitab Undang-Undang Hukum Acara Pidana.
- 4) Dan Undang-Undang lain yang terkait dengan masalah yang diangkat dalam penulisan ini.

2. Kerangka Konseptual

Agar tidak terjadi kerancuan dalam mendefinisikan arti dan maksud dari judul penelitian ini, maka perlulah diberikan konsep-konsep yang meliputi hal-hal sebagai berikut:

1) Peranan

Dalam Kamus Besar Bahasa Indonesia (KBBI), kata peranan memiliki arti fungsi seseorang atau sesuatu dalam kehidupan.¹²

2) Penyelenggara Sistem Elektronik

Penyelenggara Sistem Elektronik merupakan pihak yang menyelenggarakan Sistem Elektronik baik itu sebagai negara, Orang, Badan Usaha, dan/atau masyarakat. Sesuai dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Pasal 1 butir 6, "Penyelenggaraan Sistem Elektronik adalah pemanfaatan

¹² Depatemen Pendidikan Nasional, 2008. *Kamus Bahasa Indonesia*. Jakarta: Pusat Bahasa Departemen Pendidikan Nasional, hal. 1155.

Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.”

3) Alat Bukti Elektronik

Dalam hal ini tidak ada keterangan yang mangartikan kata alat bukti elektronik. Alat bukti elektronik sendiri merupakan data digital yang berasal dari komputer ataupun teknologi informasi lainnya. Sedangkan untuk memahaminya dapat dilihat dari hakikat pembuktian itu sendiri. Menurut Subekti hakikat pembuktian adalah upaya meyakinkan hakim tentang kebenaran dalil-dalil dalam suatu perkara/persengketaan.¹³

4) Tindak Pidana Mayantara

Barda Nawawi Arief menyatakan:

“Istilah tindak pidana mayantara dapat dibagi menjadi dua yaitu tindak pidana dan mayantara. Tindak pidana berasal dari suatu istilah dalam hukum Belanda yaitu *strafbaarfeit*. Ada pula yang mengistilahkan menjadi *delict* yang berasal dari bahasa latin *delictum*. *Strafbaarfeit* telah diterjemahkan dalam bahasa Indonesia sebagai perbuatan yang dapat dihukum. Sedangkan mayantara dapat diartikan sebagai dunia maya yang berhubungan dengan peralatan pemerosesan data listrik, *magnetic*, *optic*, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan

¹³ Subekti, 1983. *Hukum Pembuktian*. Jakarta: Pradnya Paramita, hal. 7.

mesin ketikotomatis atau *tipe-setter*, sebuah kalkulator tangan atau peralatan serupa lainnya.”¹⁴

F. Metode Penelitian

Metode penelitian sangatlah penting untuk membahas masalah yang dirumuskan, dalam hal ini penulis memakai metode sebagai berikut:

1. Metode Pendekatan

Metode pendekatan dalam penelitian ini adalah dengan menggunakan pendekatan masalah yuridis normatif yaitu dengan melihat hubungan aspek-aspek hukum terhadap peranan Penyelenggara Sistem Elektronik dalam pembuktian alat bukti elektronik.

2. Jenis Data

Jenis data dalam penelitian ini adalah:

a. Data Primer

Merupakan data yang didapat langsung dari penelitian, dengan cara meneliti keterkaitan suatu fenomena kegiatan elektronik dengan alat bukti elektronik berdasarkan hubungan hukum dan akibat hukum yang terjadi terhadap pihak-pihak yang terlibat didalamnya sehubungan dengan tindak pidana mayantara di Indonesia.

b. Data Sekunder

¹⁴ Barda Nawawi Arif, 2001. *Menggunakan istilah tindak pidana mayantara untuk jenis kejahatan cyber*, (Seminar Nasional Cyber Law, Bandung, 9 April 2001).

Merupakan informasi-informasi dari bahan studi kepustakaan yang dijadikan data bagi penelitian. Data sekunder ini berguna sebagai penjelasan bagi bahan yang didapat dari penelitian. Data sekunder ini berguna sebagai penjelasan bagi bahan yang didapat dari lapangan atau data primer yang belum diolah. Data sekunder terdiri dari:

- 1) Bahan hukum primer, merupakan bahan yang mempunyai kekuatan mengikat terdiri dari:
 - a) Kitab Undang-Undang Hukum Pidana dan Kitab Undang-Undang Hukum Acara Pidana.
 - b) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
 - c) Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan.
 - d) Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.
 - e) Dan Undang-Undang lainnya yang terkait dengan masalah yang diangkat dalam penulisan ini.
- 2) Bahan hukum sekunder, merupakan bahan ilmu pengetahuan yang berkaitan dengan tindak pidana mayantara.
- 3) Bahan hukum tersier, merupakan bahan penunjang pemahaman. Digunakan untuk memperjelas maksud maupun arti dari bahan yang didapat baik dari undang-undang, ilmu pengetahuan maupun bahan yang didapat dari

penelitian. Bahan hukum tersier yaitu seperti kamus hukum, Kamus Besar Bahasa Indonesia (KBBI), serta bahan hukum lainnya yang diambil dari internet.

3. Teknik Pengumpulan Data.

a. Teknik Studi Dokumen

Teknik ini digunakan untuk memperoleh informasi dari buku-buku, dokumen-dokumen, surat-surat, memo-memo, dan bahan tertulis lainnya yang berkaitan dengan penelitian yang didapat dari Perpustakaan, internet dan buku milik penulis sendiri.

4. Pengolahan dan Analisis Data

a. Pengolahan Data

Pengolahan data dilakukan dengan cara data yang didapat dari penelitian kemudian diseleksi dengan melakukan koreksi terhadap data yang tidak menyangkut dengan permasalahan yang dicari sehingga diperoleh data yang akurat.

b. Analisis Data

Setelah data diperoleh dari penelitian maka data tersebut diolah dengan analisis secara kualitatif. Analisis ini dilakukan dengan mempelajari setiap hasil penelitian yang kemudian dijabarkan secara sistematis kedalam suatu karya ilmiah.

BAB II

TINJAUAN KEPUSTAKAAN

A. Perkembangan Secara Umum Mengenai Tindak Pidana Mayantara

1. Istilah Dan Pengertian

Tindak pidana mayantara adalah istilah bahasa Indonesia yang dipakai oleh Barda Nawawi Arief dalam mendefinisikan kejahatan dibidang mayantara atau komputer. Sebenarnya selain tindak pidana mayantara masih banyak lagi istilah lain yang dipakai oleh para ahli hukum Indonesia dalam mendefinisikan perbuatan tersebut diantaranya, *cyber crime* digunakan oleh Agus Raharjo, M. Ramli Ahmad dan Heru Sutadi, kejahatan mayantara oleh Abdul Wahid dan Muhammad Labib, tindak pidana di dunia *cyber* oleh Indra Safitri dan masih banyak lagi istilah lainnya.

Di dunia internasional istilah tindak pidana mayantara tersebut juga terdapat beragam istilah. Diantaranya dalam dua dokumen Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian tindak pidana mayantara, yaitu *cyber crime* dan *computer related crime*. Dalam *back ground paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah tindak pidana mayantara juga dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*. Kedua, *cyber crime* dalam

arti luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut:¹⁵

- a. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them*, yang artinya *cyber crime* dalam arti sempit (kejahatan komputer): setiap perilaku sah yang diarahkan pada operasi elektronik yang targetnya keamanan komputer dan pemrosesan data didalamnya.
- b. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network*, yang artinya *cyber crime* dalam arti luas (kejahatan terkait dengan komputer): setiap perilaku yang tidak sah yang dilakukan dalam hubungannya dengan, suatu sistem komputer atau jaringan, mencakup kepemilikan tidak sah, atau menyebarkan informasi atas bantuan sistem komputer atau jaringan.

Selain istilah tersebut dalam hal mendefinisikan pengertianpun para sarjana juga memiliki berbagai macam dedinisi. Barda Nawawi Arief mendefinisikan tindak pidana mayantara adalah Istilah tindak pidana mayantara dapat dibagi menjadi dua yaitu tindak pidana dan mayantara. Tindak pidana berasal dari suatu istilah dalam hukum Belanda yaitu *strafbaarfeit*. Ada pula yang mengistilahkan menjadi *delict* yang berasal dari bahasa latin *delictum*. *Strafbaarfeit* telah diterjemahkan dalam bahasa Indonesia sebagai

¹⁵ Barda Nawawi Arief, 2007. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana Predana Media Group, hal. 24.

perbuatan yang dapat dihukum. Sedangkan mayantara dapat diartikan sebagai dunia maya yang berhubungan dengan peralatan pemerosesan data listrik, *magnetic*, *optic*, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketikotomatis atau *tipe-setter*, sebuah kalkulator tangan atau peralatan serupa lainnya.¹⁶

Indra Safitri mengemukakan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.¹⁷

Menurut Kepolisian Inggris, Cyber Crime/tindak pidana mayantara adalah segala macam penggunaan jaringan komputer untuk tujuan criminal dan/atau criminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.¹⁸

2. Perkembangan Tidak Pidana Mayantara

Perkembangan ilmu pengetahuan dan teknologi (IPTEK) saat ini telah menjadi suatu tuntutan bagi manusia. Hal ini dikarenakan tujuan perkembangan IPTEK itu sendiri adalah ingin membawa manusia kepada kehidupan masa depan yang lebih baik, mudah, murah, cepat dan aman.¹⁹ Salah-satu perkembangan IPTEK di bidang informasi

¹⁶ Barda Nawawi Arif, 2001. *Op.cit.*

¹⁷ Abdul Wahid dan Mohammad Labib, 2005. *Op.cit.* hal. 3.

¹⁸ *Ibid.*

¹⁹ The Liang Ge, 1996. *Pengantar Filsafat Teknologi*. Yogyakarta: Andi Offset, hal. 2.

dan telekomunikasi adalah dengan munculnya teknologi informasi (*information technology*).

Bagi umat manusia masalah akan selalu ada dalam kehidupan, begitu juga dalam teknologi informasi, selain mendatangkan nilai guna yang banyak namun tidak bisa dipungkiri juga membawa masalah tersendiri. Hal ini ibarat "*pisau bermata dua*" selain mendatangkan keuntungan bagi manusia juga mendatangkan kerugian bagi manusia.

Masalah dalam teknologi informasi erat kaitannya dengan penyelewengan suatu fungsi dari teknologi informasi yang dimana arahnya tidak lagi untuk mencapai tujuan IPTEK tapi malah mengarah pada kepentingan sendiri dengan melakukan perbuatan yang bertentangan dengan hukum atau disebut tindak pidana mayantara. tindak pidana mayantara telah menjadi masalah hukum dan dapat dikategorikan sebagai kejahatan yang digolongkan kepada *extra ordinary crime* (kejahatan luar biasa) karena dapat mengancam kehidupan masyarakat, bangsa dan bahkan negara lain dengan menimbulkan kerugian yang cukup besar terhadap pihak yang dirugikan. Kasus Cina dan Amerika Serikat adalah bukti dari berbahayanya kejahatan ini, pada tahun 2001 negara Cina dan Amerika Serikat sempat mengalami hubungan kurang baik, akibat dalam kasusnya situs FBI milik negara Amerika Serikat dirobah dengan gambar seorang pilot Cina yang tewas dalam suatu insiden di Laut Cina Selatan dengan pesawat pengintai Amerika Serikat yang berada di wilayah udara Cina. Dapat dibayangkan betapa tindak pidana mayantara sangat berbahaya dan membawa dampak buruk bagi hubungan kedua negara.²⁰

Bagi negara Indonesia sebagai negara yang berkembang dan kepulauan tidak luput dari pengaruh perkembangan teknologi informasi termasuk juga tindak pidana

²⁰ Kompas, 4 juni 2001, hal. 7.

mayantara sebagai kejahatan dalam teknologi informasi. Kejahatan ini perlu diwaspadai dan ditanggulangi supaya korban kejahatan ini dapat ditekan. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (untuk selanjutnya disebut Undang-Undang ITE) telah mengatur mengenai bentuk tindak pidana mayantara yaitu terdapat dalam BAB VII yang dirinci sebagai berikut:²¹

- a. Perbuatan mengenai mendistribusi dan mentransmisikan yang bermuatan pelanggaran kesusilaan, perjudian, pencemaran nama baik, pemerasan dan pengancaman (Pasal 27).
- b. Perbuatan mengenai penyebaran berita dan informasi bohong, menyesatkan, menimbulkan rasa permusuhan/kebencian yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik (Pasal 28).
- c. Perbuatan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29).
- d. Perbuatan mengenai sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (Pasal 30).
- e. Perbuatan melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik

²¹ Bab VII Undang-Undang No. 11 Tahun 2008.

- dan/atau Dokumen Elektronik yang sedang ditransmisikan (Pasal 31 ayat (1), (2)).
- f. Perbuatan melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan dan mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya (Pasal 32).
 - g. Perbuatan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya (Pasal 33).
 - h. Perbuatan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan dan sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33 (Pasal 34).
 - i. Perbuatan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik (Pasal 35).
 - j. Perbuatan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain (Pasal 36).

- k. Perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia (Pasal 37).

IPTEK telah menjadi kebutuhan pokok bagi manusia saat ini dan bahkan tidak dapat dipisahkan dari kehidupan, sehingga pada prinsipnya dari waktu-kewaktu selalu terus berkembang. Sama halnya dengan tindak pidana mayantara yang selalu mengalami perkembangan dari waktu-kewaktu, hal ini disebabkan karena tindak pidana mayantara adalah efek negatif dari perkembangan IPTEK. Oleh karena itulah antara teknologi informasi (dalam hal ini bagian dari IPTEK) dengan tindak pidana mayantara tidak dapat dipisahkan, dimana terjadi perkembangan di bidang teknologi informasi maka pada saat itu pula tindak pidana mayantara ada disitu dengan bentuk dan beragam macam modus.

B. Bentuk-Bentuk Tindak Pidana Mayantara

1. Tindak Pidana Mayantara Di Bidang Pornografi (*Cyber Porn*)

Pornografi merupakan hal yang telah lama menjadi permasalahan baik itu karena perbuatan itu berbenturan dengan kebudayaan maupun norma-norma yang hidup dalam masyarakat. Pornografi memiliki batasan yang cukup rumit karena memiliki persepsi yang berbeda pada setiap daerah dan lingkungan masyarakat, oleh sebab itulah pada saat rancangan Undang-Undang Nomor 44 tahun 2008 Tentang Pornografi akan ditetapkan, terjadi perselisihan dalam menentukan sesuatu perbuatan adalah pornografi atau tidak.

Menurut Pasal 1 butir 1 Undang-Undang Nomor 44 tahun 2008 Tentang Pornografi, "Pornografi adalah gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya melalui berbagai

bentuk media komunikasi dan/atau pertunjukan di muka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat.” Dari keterangan Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi, dapat diambil poin-poin kalimat yang menerangkan tentang pornografi di dunia maya atau *cyber porn* yaitu kalimat melalui berbagai media komunikasi. Walaupun kalimat itu telah memberikan sedikit inti dari *cyber porn*, namun *cyber porn* tetaplah harus diterangkan dengan jelas.

Menurut ensiklopedia bebas wikipedia dinyatakan bahwa *cyber sex/cyber porn* atau *computer sex* adalah pertemuan sex secara virtual/maya antara dua orang atau lebih yang terhubung melalui jaringan internet dengan mengirimkan pesan-pesan seksual yang menggambarkan suatu pengalaman sosial.²²

Pornografi sangat mudah sekali melekat pada berbagai aspek dalam masyarakat termasuk teknologi informasi. Dalam perkembangannya sekarang ini pornografi telah merambah ke media teknologi informasi seperti internet dan menjadikan pornografi termasuk kedalam tindak pidana mayantara. Tak hanya sebatas itu ternyata pada prakteknya pornografi juga telah menjadi topik terpopuler di dunia maya, terbukti 40% dari situs yang terdapat di internet menyediakan konten-konten yang berbau pornografi. Dalam tesis Golberg dikemukakan pula bahwa perdagangan bahan-bahan porno melalui internet sudah mencapai miliaran dollar US per tahun, sekitar 25% pengguna

²² Peter David Golberg. *An Explorator Study About The Impact That Cyber Sex (The Use Of The Internet For Sexual Purpose) Is Having On Families And The Practices Of Marriage And Family Therapists*. pedrogold@aol.com. Diakses tahun 2004.

mengunjungi lebih dari 60.000 situs sex tiap bulan, dan sekitar 30 juta orang memasuki situs seks tiap hari.²³

Dalam dunia internet, pornografi dapat dikategorikan ke dalam aplikasi multimedia. Hal ini dikarenakan bentuk pornografi berkisar pada gambar, suara dan film yang merupakan bagian aplikasi multimedia.. Format-format digital multimedia di antaranya:²⁴

- a. MIDI (*Musical Instrument Digital Interface*), format suara instrumen ini di perkenalkan pada tahun 1983 oleh perusahaan musik elektrik seperti Roland, Yamaha dan Korg. Format MIDI bersifat sangat kompak dengan ukurannya yang kecil, suara yang di hasilkan oleh MIDI dengan dukungan *sound card* yang memilik *synthesizer* (penghasil suara elektrik) sangatlah mirip dengan organ elektrik yang bisa memainkan berbagai alat musik.
- b. MP3, format suara yang terkenal saat ini berbeda dengan MIDI yang hanya instrument, MP3 merekam seluruh suara termasuk suara penyanyinya. Kualitas suara MP3 akan berbanding dengan ukuran penyimpannya. Kualitas yang banyak di gunakan untuk merekam musik adalah standar CD-ROM (44,2 KHz, 16 bit, stereo), sementara kualitas terendah adalah kualitas seperti telepon (5 KHz, 8 bit, mono).
- c. MPEG (*Moving Picture Experts Group*), merupakan format video yang disusun oleh ahli dari berbagai penjuru dunia untuk format multimedia.
- d. AVI (*Audio Video Interleave*), AVI di buat oleh Microsoft dan merupakan juga format video.

²³ Glorida G. Brame, 1996. *Boot Up And Turn On*. www.glorida-blame.com/glory/journ7.htm.

²⁴ Ivan Sudirman, 2003. *Perkembangan Software Komputer*. ilmukomputer.com, hal. 8.

- e. Quicktime, sama dengan AVI, Quicktime dapat digunakan baik di komputer berbasis Intel maupun Mac.

2. Tindak Pidana Mayantara Di Bidang Perbankan

Aktivitas perbankan saat ini tidak dapat dipisahkan dari kehidupan, khususnya yang terkait dengan dana (pemindahan/pengiriman/pembayaran uang). Perkembangan teknologi informasi telah memunculkan sistem baru dalam dunia perbankan. *electronic funds transfer system* (EFTS) adalah bentuk dari pengaruh teknologi informasi dunia perbankan yang memungkinkan transfer dana dapat dilakukan secara elektronik.

Dengan lahirnya EFTS sebagai sistem transfer dana, maka telah membuka munculnya beberapa sistem baru di dunia perbankan dengan memanfaatkan teknologi informasi seperti *internet banking*, *cyber bank*, *elektronik and cyber space commerce*, *online business* dan sebagainya.²⁵ Pemanfaatan teknologi informasi ini dalam kegiatan perbankan juga mendatangkan kesempatan bagi pelaku tindak pidana mayantara untuk mendapatkan apa yang mereka inginkan.

Tindak pidana mayantara di bidang perbankan erat kaitannya dengan kekayaan, sebab kebanyakan motif pelaku dalam melakukan kejahatan di bidang perbankan ini adalah untuk mendapatkan sejumlah uang. Berbagai cara dilakukan oleh pelaku untuk mendapatkan uang tersebut, baik dengan melakukan pembobolan ATM, pembobolan sistem keamanan perbankan dan pengalihan transaksi elektronik. Disamping bentuk kejahatan tersebut yang tak kalah uniknya yaitu kejadian Steven mengenai penipuan dengan memberikan nama domain Bank Central Asia (BCA). Steven membeli domain-

²⁵ Barda Nawawi Arief, 2006. *Op.cit*, hal. 74.

domain dengan nama mirip *www.klikbca.com* (situs asli Internet banking BCA), yaitu domain *wwwklik-bca.com*, *kilkbca.com*, *clikbca.com*, *klickca.com*, dan *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. Untungnya Steven melakukan ini hanya untuk mencoba menguji keamanan dari bank tersebut.²⁶

3. *Hacking, Cracking Dan Viruses*

a. *Hacking*

Istilah *hacker* ini berawal dari kata "*hack*" yang saat itu artinya teknik pemrograman kreatif yang mampu memecahkan masalah secara jauh dan lebih efisien daripada teknik biasa. *Hacking* dikenal juga dengan sebutan *computer trespass*, yakni tindakan yang melanggar hukum apapun bentuk alasan dan motivasinya.²⁷

Kejahatan *hacking* telah mempunyai sejarah perjalanan panjang, bermula di akhir perang dunia II sampai dengan tahun 60-an komputer masih merupakan barang langka, hanya beberapa departemen dan organisasi besar yang memiliki komputer. Pada awalnya beberapa mahasiswa yang berasal dari *Institute of Technology* (MIT) di Massachusetts melakukan eksperimen dengan menggunakan komputer institutnya. Mereka melakukan penyusupan-penyusupan dengan maksud agar penggunaan komputer tersebut dapat dilakukan kapan saja dan dimana saja. Para Mahasiswa tersebut membuat program yang bertujuan mengoptimalkan fungsi dan kerja komputer dan membantu pengembangan bahasa LISP karya John McCarthy. Saat itu, sebuah tindakan *hacking*

²⁶ Petrus Reinhard Golose, Agustus 2006. *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri*. Jakarta: Buliten Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, hal. 29-30.

²⁷ Suhartono. *Op.cit*, hal. 4.

computer sangat bermanfaat karena dapat meningkatkan kemampuan program dan lebih hemat.²⁸

Setelah semakin berkembangnya peradaban, hal positif yang didapat dari *hacking* semakin tidak lagi dimanfaatkan. *Hacking* sekarang berubah menjadi kejahatan yang meresahkan masyarakat pengguna teknologi informasi. Tindakan *hacking* sering disertai dengan penipuan, penggelapan atau pengrusakan Sistem Elektronik. Motifnya pun berbeda-beda, mulai dari iseng-iseng, mencoba mengganggu sistem keamanan data perusahaan untuk mendapatkan keuntungan financial, dan kemudian adapula menyebarkan *spam mail* untuk mengkampanyekan program politik tertentu. *Hacking* sendiri memiliki beberapa tahap-tahap dalam melakukannya:²⁹

- 1) *Foot printing*. Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi baik dengan cara sederhana maupun menggunakan software seperti *search engine*, *whois* dan *DNS zone transfer*, contoh: mencari informasi seperti tanggal lahir, nama, hobi dari pemilik akun Sistem Elektronik.
- 2) *Scanning*. Terhadap sasaran tertentu dicari pintu masuk yang paling mungkin untuk dimasuki, biasanya bagian Sistem Elektronik paling lemah *vulnerability holes* (celah kelemahan suatu program) digunakan *ping sweep* dan *port scan*.
- 3) *Enumeration*. Menelaah intensif komputer sasaran, contoh; mencari *user account* yang absah, *network resource and share*, dan aplikasi untuk mendapatkan bagian yang proteksinya lemah.

²⁸ *Ibid*, hal. 4.

²⁹ Deris Setiawan, 30 Agustus 2003. *Op.cit*, hal. 4.

- 4) *Gaining Access*. Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran, meliputi mengintip dan merampas *password*, menebak *password* berdasarkan *foot printing*, serta melakukan *buffer overflow* (aplikasi penyangga jika lupa *password*).
- 5) *Escalating Privilege*. Bila sudah mendapatkan user *password*, ditahap ini diusahakan mendapatkan *privillage admin* (usaha untuk mendapatkan akses admin) dengan mencoba *password cracking* atau *exploit*.
- 6) *Pilfering*. Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses *trusted system* (akses penyelenggara sistem).
- 7) *Covering Tracks*. Begitu control penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan *network log* atau informasi yang tertinggal dari admin.
- 8) *Creating Backdoors*. Pintu belakang diciptakan pada berbagai bagian sistem untuk memudahkan masuk kembali ke sistem ini dengan membentuk *user account* palsu, dan menambahkan service lainnya.
- 9) *Denial of Service*. Bila usaha diatas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Meliputi SYN flood, teknik ICMP, dan lain-lain.

b. Cracking

Cracking atau *cracker* merupakan perbuatan yang sebenarnya memiliki persamaan cara dalam melakukannya dengan hacking, perbedaannya hanyalah pada motif dari si pelaku. *Cracking* memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase,

dan penghancuran data pihak korban demi kepuasan batinnya. Hal ini dilakukan pelaku biasanya dengan latar belakang dendam. Sebagai contoh pada tahun 1994 City Bank AS di Inggris mengalami kebobolan senilai US \$ 400.000 oleh seorang craker dari Rusia. Pelaku akhirnya dapat ditangkap dan dijatuhi pidana tiga tahun serta harus mengembalikan sejumlah uang yang dijarah. Dalam kasus ini ternyata terbongkar, yang membantu *craker* Rusia tersebut adalah bekas staf karyawan dari City Bank tersebut yang diduga akibat kesal karena dipecat.³⁰

c. *Viruses*

Viruses atau program pengganggu (*malicious*) merupakan perangkat lunak yang dapat mengganggu ataupun merusak Sistem Elektronik, sehingga dapat membuat Sistem Elektronik tersebut tidak berjalan dengan biasanya.³¹

Penyebaran *viruses* sendiri sehingga dapat merusak Sistem elektronik sebenarnya memiliki beragam cara, diantaranya ada yang melalui pengaksesan internet yang menyebabkan virus yang ada di internet menjangkiti komputer atau Sistem Elektronik seseorang. Selain itu ada pula penyebarannya melalui flash disk, floppy disk atau barang elektronik yang dapat menyimpan dan menampilkan data-data elektronik.

4. *Piracy (Pembajakan)*

Fenomena pembajakan pada saat sekarang sudah tidak dapat dibendung lagi hampir apapun yang bersifat komersil telah dilakukan pembajakan misalnya saja, software, lagu-lagu, film dan lain-lain. Tentunya keadaan seperti ini sangatlah memprihatinkan apalagi nilai harga dari data tersebut sangatlah besar.

³⁰ NCIS Inggris, Mei 2001. "Cyber Crime : awas bandit dan vandalisme digital", Artikel. Republika, hal. 27.

³¹ *Ibid.*

Dalam melakukan pembajakan masing-masing pelaku mempunyai bermacam-macam cara diantaranya, meletakkan pada suatu situs supaya pengguna dapat mendownloadnya dengan gratis atau dikopi melalui video caset recorder seperti, *compact disk* (CD), *video compact disk* (VCD), dan DVD.³²

5. *Criminal Communication*

Dalam perbuatan ini layanan internet digunakan sebagai kegiatan komunikasi bagi para subjek kriminal seperti gengster, ataupun bagi teroris. *Criminal communication* merupakan media yang paling disukai oleh para kriminal karena mereka dapat leluasa mengorganisir setiap aksi yang akan dilakukannya. Contoh dari *criminal communication* dapat dilihat dari kasus www.anshar.net tahun 2007, dimana situs ini diduga digunakan untuk menyampaikan informasi terorisme atas pesanan Noordin M. Top sebagai media informasi perjuangannya. Isi dari informasi para teroris itu seputar materi-materi Tauziah Syaikh Mukhlas, Tauhid, Jihad, Wacana, Islamiah dan Askariah, antara lain mengajarkan penyerangan dengan cara memanfaatkan antrian di jalan atau pintu masuk masuk atau keluar kantor, pusat perbelanjaan, hiburan, olahraga, hotel dan tempat pameran.³³

C. Alat Bukti Elektronik Dalam Sistem Hukum Di Indonesia

1. Asas-Asas Pembuktian Untuk Alat Bukti Elektronik

Alat bukti adalah alat yang digunakan untuk dapat meyakinkan bahwa suatu tindak pidana benar-benar terjadi dan harus dapat membuktikan bahwa terdakwa benar-benar bersalah. Dalam Pasal 183 KUHP dijelaskan bahwa Hakim tidak boleh menjatuhkan

³² *Ibid*, hal. 28.

³³ Rakyat Merdeka, 24 Agustus 2006. *Op.cit.*

pidana kepada seseorang kecuali dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya. Dari rumusan pasal diatas jelaslah bahwa keberadaan alat bukti mutlak harus ada dalam sebuah kasus pidana. Bahkan disebutkan dalam pasal di atas harus ada minimal dua bukti.

Dalam sistem pembuktian di Indonesia, terdapat beberapa doktrin pengelompokan alat bukti, yang membagi alat-alat bukti kedalam beberapa kategori:³⁴

a. *Oral Evidence*

- 1) Perdata (keterangan saksi, pengakuan, dan sumpah).
- 2) Pidana (keterangan saksi, keterangan ahli, keterangan terdakwa).

b. *Documentary Evidence*

- 1) Perdata (surat dan persangkaan).
- 2) Pidana (surat dan petunjuk).

c. *Material Evidence*

- 1) Perdata (tidak Dikenal).
- 2) Pidana (barang yang digunakan untuk melakukan tindak pidana, barang yang digunakan untuk membantu tindak Pidana, barang yang merupakan hasil suatu tindak pidana, barang yang diperoleh dari suatu tindak pidana, dan informasi dalam arti khusus).

³⁴ Freddy Haris, *Cyber Crime Dari Perspektif Akademis*, Lembaga Kajian Hukum Dan Teknologi Fakultas Hukum Universitas Indonesia, <http://www.gipi.or.id>, hal. 15-16, diakses tanggal 30 Mei 2004.

d. *Electronic Evidence*

- 1) Konsep pengolompokkan alat bukti menjadi alat bukti tertulis dan alat bukti elektronik.
- 2) Konsep tersebut terutama berkembang di negara common law.
- 3) Pengaturannya tidak melahirkan alat bukti baru, tetapi memperluas cakupan alat bukti yang masuk kategori *documentary evidence*.

Dasar pertimbangan dipakainya *elektronik evidence* atau alat bukti elektronik dalam sistem pembuktian di Indonesia dapat dilihat dari sistem dan teori pembuktian.³⁵

- a. Sistem atau teori pembuktian berdasarkan undang-undang secara positif.

Pembuktian yang didasarkan kepada alat-alat pembuktian yang terdapat pada undang-undang secara positif (*positive wettelijk bewijstheorie*) memiliki arti jika tidak terbukti suatu perbuatan sesuai alat-alat bukti yang disebut undang-undang, maka keyakinan hakim diabaikan.

- b. Sistem atau teori pembuktian berdasar undang-undang secara negatif.

Teori ini memperlihatkan ada dua hal yang diperhatikan oleh hakim dalam mengambil keputusan mengenai pembuktian, pertama alat bukti yang ditentukan oleh undang-undang dan yang kedua keyakinan hakim sendiri atas alat bukti tersebut. Berdasarkan KUHAP, sistem atau teori pembuktian yang dianut dalam hukum pidana adalah sistem atau teori pembuktian berdasarkan undang-undang secara negatif.³⁶

³⁵ Dikdik M. Arief Mansyur Dan Elisatris Gultom, 2006. *Cyber Law (Aspek Hukum Teknologi Informasi)*, Bandung: Refika Aditama, hal. 105.

³⁶ Pasal 183 KUHAP.

- c. Sistem dan teori pembuktian berdasarkan keyakinan hakim melalui (*coviction in time*).

Berdasarkan teori ini, di dalam putusannya hakim tidak terikat dengan alat bukti yang ada. Dalam menyimpulkan putusan, hakim tidak harus mengikuti alat bukti yang ada pada persidangan, hakim boleh mengabaikan bukti yang ada dalam persidangan untuk mengambil putusan.

- d. Sistem dan teori pembuktian berdasarkan keyakinan hakim atas alasan logis (*conviction raionee*).

Dalam teori ini hakim dapat memutuskan seorang bersalah atau tidak berdasarkan keyakinannya, keyakinan hakim tersebut tentunya harus berdasarkan dengan suatu alasan-alasan logis. Sistem pembuktian ini disebut juga pembuktian bebas karena hakim bebas menyebutkan alasan-alasan keyakinannya. Indonesia sendiri termasuk yang menganut sistem ini.

2. Alat Bukti Elektronik Dalam Beberapa Undang-Undang

Berlakunya Undang-Undang ITE telah menciptakan suatu bidang kajian baru dalam hukum pidana menyangkut dunia maya. Kehadiran bidang baru ini membawa dampak perubahan bagi hukum di dalam hal kriminalisasi perbuatan-perbuatan yang ada di dunia maya. Jika dahulu perbuatan-perbuatan merugikan di dunia maya sulit untuk dibuktikan, maka dengan keberadaan UU ITE ini dapat terbantu.

Undang-Undang ITE juga telah menetapkan dengan jelas beberapa bentuk baru dari alat bukti yaitu elektronik seperti dinyatakan dinyatakan dalam Pasal 5:

- (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.
- (4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
 - a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
 - b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.

Dari pasal diatas, tegas disebutkan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya adalah alat bukti hukum yang sah dan merupakan perluasan dari alat bukti yang terdapat dalam KUHAP. Pasal ini digunakan untuk mengakomodir kebutuhan alat bukti pada kasus tindak pidana mayantara.³⁷

Sebenarnya sebelum diundangkannya Undang-Undang ITE, pengakuan data elektronik sebagai alat bukti sudah ada di Indonesia. Hanya saja, penggunaan alat bukti elektronik ini hanya dapat digunakan pada tindak pidana khusus saja seperti terorisme,

³⁷ Hukumonline, Senin 9 Februari 2009. *Berita Acara Pengalihan Dokumen Elektronik Perlu.* <http://www.hukumonline.com>, Diakses tanggal 12 Maret 2010.

korupsi, dan pencucian uang. Undang-undang yang telah mengakui alat bukti elektronik antara lain:³⁸

a. Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan

Kategori alat bukti *elektronik evidence* dalam sistem pembuktian di Indonesia pertama kali dipakai dalam Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan, yang telah mulai menjangkau kearah pembuktian elektronik. Dalam undang-undang ini pemerintah mulai berusaha mengatur pengakuan atas *microfilm* dan media lainnya (alat penyimpanan yang bukan kertas dan mempunyai tingkat pengamanan) yang dapat menjamin keaslian dokumen yang dialihkan atau ditranpormasi misalnya *Compact Disk-Read Only Memory* (CD-ROM) dan *write-one-many* (WORM), yang diatur dalam Pasal 12 Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan tersebut sebagai alat bukti.

Dalam Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan, yaitu Pasal 13 dan 14, dinyatakan juga bahwa sebuah dokumen perusahaan mempunyai kekuatan sebagai alat bukti yang sah setelah dilakukan proses pengalihan yang kemudian dilanjutkan dengan proses legalisasi. Setelah proses pengalihan dan legalisasi barulah dapat dikatakan bahwa alat bukti elektronik tersebut sah sebagaimana dinyatakan dalam Pasal 15 Undang-Undang Dokumen Perusahaan tersebut.³⁹

b. Undang-Undang Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-Undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi.

³⁸ Syailendra Wisnu, 28 Juli 2009. *Alat Bukti Elektronik dalam Undang-Undang Informasi dan Transaksi Elektronik*. de_rechter_2007@blog.uns.ac.id. Diakses tanggal 23 Februari 2010.

³⁹ Dikdik M. Arief Mansyur Dan Elisatris Gultom. *Op.cit*, hal. 109.

Berdasarkan undang-undang ini, ada perluasan mengenai sumber perolehan alat bukti yang sah berupa petunjuk. Berdasarkan KUHAP, alat bukti petunjuk hanya dapat diperoleh dari keterangan saksi, surat dan keterangan terdakwa, tetapi menurut Undang-Undang Nomor 20 Tahun 2001 Tentang Pemberantasan Tindak Pidana Korupsi, bukti petunjuk juga dapat diperoleh dari alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu tetapi tidak terbatas pada data penghubung elektronik (*elektronik data interchange*), surat elektronik (E-mail), telegram, teleks, faksimili dan dari dokumen. Dokumen yang dimaksud yakni setiap rekaman atau informasi yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.⁴⁰

c. Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.

Pasal 27 Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme, menerangkan tentang Alat bukti pemeriksaan tindak pidana terorisme yang meliputi:

- 1) alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana;
- 2) alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan

⁴⁰ Syailendra Wisnu. *Op.cit.*

3) data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada : (a) tulisan, suara, atau gambar; (b) peta, rancangan, foto, atau sejenisnya; (d) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

d. Undang-Undang Nomor 25 Tahun 2003 Tentang Pencucian Uang.

Dalam Pasal 38 huruf (b) Undang-Undang Nomor 25 Tahun 2003 Tentang Pencucian Uang, diterangkan pula alat bukti elektronik, yaitu “alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.”

e. Undang-Undang Nomor 21 Tahun 2007 Tentang Pemberantasan Tindak Pidana Perdagangan Orang.

Pasal 29 Undang-Undang Nomor 21 Tahun 2007 Tentang Pemberantasan Tindak Pidana Perdagangan Orang, mengatur mengenai alat bukti selain sebagaimana ditentukan dalam KUHP. Alat bukti yang dimaksud dapat pula berupa:

- 1) Informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau serupa dengan itu dan;
- 2) Data, rekaman atau informasi yang dapat dilihat, dibaca, dan/atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas atau yang terekam

secara elektronik, termasuk tidak terbatas pada: (1) Tulisan, suara atau gambar (2) Peta, rancangan, foto atau sejenisnya (3) Huruf, tanda, angka, simbol atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

D. Pihak-Pihak Dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Dalam Undang-Undang ITE terdapat beberapa pihak yang terlibat kedalam kegiatan telematika di Indonesia. Pihak-Pihak tersebut diantaranya:

1. Penyelenggara Sistem Elektronik

Berdasarkan Pasal 1 butir 6 Undang-Undang ITE, Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat. Penyelenggara Sistem Elektronik (PSE) memiliki kedudukan yang penting dalam kegiatan dan interaksi di dunia maya, karena pihak inilah yang menyediakan beberapa fasilitas yang dapat nantinya dinikmati oleh masyarakat pengguna dunia maya. Salah-satu contoh dari fasilitas yang yang diberikannya adalah fasilitas *internet banking* dan *E-mail* yang diselenggarakan oleh Bank dan Pemilik Web.⁴¹

Dalam hal kegiatan yang diselenggarakan oleh PSE, penyelenggara diletakkan pada posisi yang bertanggung jawab terhadap apa yang terjadi pada Sistem Elektroniknya baik itu secara pidana maupun perdata. Kesimpulan ini bisa ditarik dari rumusan Pasal 15 ayat (1) Undang-Undang ITE yang berbunyi “Setiap penyelenggara sistem elektronik harus

⁴¹ Hukumonline, Selasa, 21 Juli 2009. *Penyelenggara Sistem Elektronik Gunakan Prinsip Praduga Bersalah*. www.hukumonline.com, Diakses tanggal 13 Februari 2010.

menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.” Hal ini menyebabkan PSE diposisikan dalam keadaan bersalah yang dibebankan kewajiban untuk selalu bertanggung jawab, kecuali bila dapat dibuktikan bahwa kesalahan atas sistem elektronik bukan merupakan kesalahannya. Untuk lebih jelas mengenai PSE akan diterangkan dalam Bab III.

2. Penyelenggara Agen Elektronik

Dalam Undang-Undang ITE tidak jelas diterangkan mengenai pengertian Penyelenggara Agen Elektronik itu sendiri, namun dapat dipahami pernyataan-pernyataan yang tersirat dari undang-undang ini seperti, dalam Pasal 2 butir 8 Undang-Undang ITE yang menyatakan Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang, kemudian Pasal 21 ayat (1) huruf c yang menyatakan jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab Penyelenggara Agen Elektronik. Tanggung jawab Penyelenggara Agen Elektronik dapat terlepas jika dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.⁴²

3. Penyelenggara Sertifikat elektronik

Berdasarkan Pasal 1 butir 10 Undang-Undang ITE Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya,

⁴² Pasal 21 Ayat (5) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

yang memberikan dan mengaudit Sertifikat Elektronik. Penyelenggara Sertifikat Elektronik memiliki kewenangan dalam pembuatan tanda tangan elektronik. Tanda tangan elektronik itu sendiri menurut Pasal 1 butir 12 Undang-Undang ITE adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

4. Lembaga Sertifikasi Keandalan

Menurut Pasal 1 Butir 11 Undang-Undang, Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.

5. Penanda Tangan

Penanda Tangan erat kaitannya dengan Tanda Tangan Elektronik yang menurut Pasal 1 Butir 12 Undang-Undang ITE adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Sedangkan Penanda Tangan menurut Pasal 1 butir 13 adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.

Sama halnya dengan tanda tangan dalam perjanjian tertulis, Tanda Tangan Elektronik juga mengikat penanda Tangan terhadap Transaksi Elektronik yang terjadi antara para pihak Penanda Tangan dalam Sertifikat Elektronik seperti diuraikan Pasal 11 ayat (1) Undang-Undang ITE yang menguraikan:

(1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

- a. Data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
- b. Data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;
- c. Segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
- d. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
- e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatanganannya; dan
- f. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

6. Pengirim Dan Penerima

Menurut Pasal 1 butir 18 Undang-Undang ITE, Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik. Bila ada pengirim maka pasti ada penerima, Pasal 1 butir 19 Undang-Undang ITE menyatakan Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.

7. Badan Usaha

Kegiatan teknologi informasi tidak bisa lepas dari urusan finansial baik itu perdagangan elektronik ataupun juga yang bersifat pemasaran jasa maupun barang yang melibatkan Badan Usaha. Menurut Pasal 1 butir 22 Undang-Undang ITE, Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.



BAB III

PEMBAHASAN

A. Kedudukan Hukum Penyelenggara Sistem Elektronik Dalam Penyelenggaraan Sistem Elektronik

1. Syarat Penyelenggaraan Sistem Elektronik

Seiring perkembangan penggunaan Sistem Elektronik yang terus meningkat dari waktu-kewaktu, menyebabkan kegiatan di dunia maya semakin meluas. Kegiatan seperti transfer dan penarikan yang lewat anjungan tunai mandiri sampai kegiatan komunikasipun dapat dilakukan lewat dunia elektronik ini, hal ini diakibatkan oleh sifat hakiki manusia yang ingin mencari hal yang lebih baik dari sebelumnya sehingga kemudahan dan keefektifitasan menjadi alasan mengapa orang-orang menyukai media ini.

Pemanfaatan Sistem Elektronik sendiri harus diarahkan kepada yang benar dan dilakukan dengan bijak, karena sistem elektronik sendiri memiliki dampak yang sangat besar bagi perkembangan kehidupan manusia kedepannya. Di sinilah pentingnya tata kelola yang baik dalam Penyelenggaraan Sistem Elektronik. Penarapan tata kelola yang baik (*good pratice*) tidak hanya mengacu pada aspek teknik, tetapi juga manajemen dan hukum. Karena itu, menurut Edmon Makarim, perlu melihat bagaimana perwujudan pertanggungjawaban hukum Penyelenggara Sistem Elektronik (PSE).⁴³

⁴³ Hukumonline, Selasa, 21 Juli 2009. *Op.cit.*

Berdasarkan Pasal 16 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Undang-Undang ITE), PSE telah diberikan tugas dalam menyelenggarakan Sistem Elektronik yang harus memiliki persyaratan:

- a. Dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
- b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
- c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
- d. 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
- e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Ad. a Dapat Menampilkan Kembali Informasi Elektronik Dan/Atau Dokumen Elektronik Secara Utuh Sesuai Dengan Masa Retensi Yang Ditetapkan Dengan Peraturan Perundang-Undangan.

Proses menampilkan, menyimpan dan kemudian dapat menampilkan kembali Informasi dan Dokumen Elektronik adalah bentuk dari realisasi pengelolaan data yang dilakukan PSE terhadap Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan

Perundang-undangan. Dapat dikatakan Informasi Elektronik dan Dokumen Elektronik yang memenuhi syarat tersebut sah menurut hukum.

Setiap langkah pengelolaan tampilan Informasi Elektronik harus memperhatikan tahapan *input*, proses, dan *output* data. Pada tahapan *input*, prosedur yang harus dijalankan adalah prosedur akses data, prosedur transaksi data untuk memeriksa akurasi, kelengkapan, dan validitasnya, serta prosedur pencegahan kesalahan *input* data. Pada tahapan proses, prosedur yang harus dijalankan adalah prosedur pengolahan data, prosedur validasi dan editing, serta prosedur penanganan kesalahan. Sedangkan pada tahapan output, prosedur yang harus dijalankan adalah prosedur distribusi, penanganan kesalahan, dan keamanan data.⁴⁴

Ad. b Dapat Melindungi Ketersediaan, Keutuhan, Keotentikan, Kerahasiaan, Dan Keteraksesan Informasi Elektronik Dalam Penyelenggaraan Sistem Elektronik Tersebut.

Dalam melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan data, PSE harus memperhatikan persyaratan minimal aspek keamanan sistem dan keberlangsungan sistem, terutama sistem yang memfasilitasi layanan-layanan yang bersifat rahasia atau penting. Aspek keamanan dan keberlangsungan sistem minimal yang harus terpenuhi, mencakup hal-hal berikut ini:⁴⁵

- 1) *Confidentiality*: akses terhadap data/informasi dibatasi hanya bagi mereka yang punya otoritas.
- 2) *Integrity*: data tidak boleh diubah tanpa ijin dari yang berhak.

⁴⁴ Edmon Makarim, 22 Januari 2010. *Pembobolan Sistem Elektronik Dari Segi Hukum*. Koran Seputar Indonesia.

⁴⁵ Peraturan Menteri Komunikasi Dan Informatika Nomor: 41/PER/MEN.KOMINFO/11/2007 Tentang Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional.

- 3) *Authentication*: untuk meyakinkan identitas pengguna sistem.
- 4) *Availability*: terkait dengan ketersediaan layanan, termasuk up-time dari situs web.

Sedangkan mekanisme dasar yang harus dipenuhi untuk memastikan tercapainya aspek-aspek keamanan dan keberlangsungan sistem mencakup hal-hal berikut ini:⁴⁶

- 1) Untuk pengamanan dari sisi software aplikasi dapat diimplementasikan komponen standar sebagai berikut:
 - i. Metode *scripting* software aplikasi yang aman.
 - ii. Implementasi mekanisme otentikasi dan otorisasi di dalam software aplikasi yang tepat.
 - ii. Pengaturan keamanan sistem *database* yang tepat.
- 2) Untuk pengamanan dari sisi infrastruktur teknologi dapat diimplementasikan komponen standar sebagai berikut:
 - i. *Hardening* dari sisi sistem operasi.
 - ii. *Firewall*, sebagai pagar untuk menghadang ancaman dari luar sistem.
 - iii. *Intrusion Detection System/ Intrusion-Prevention Systems (IDS/IPS)* sebagai pendeteksi atau pencegah aktivitas ancaman terhadap sistem.
 - iv. *Network monitoring tool*, sebagai usaha untuk melakukan monitoring atas aktivitas di dalam jaringan.
 - v. *Log processor & analysis*, untuk melakukan pendeteksian dan analisis kegiatan yang terjadi di sistem.

⁴⁶ *Ibid.*

- 3) Untuk sistem kritikal dengan standar layanan aman yang ketat, dapat ditempuh melalui penyediaan sistem cadangan yang dapat secara cepat mengambil alih sistem utama jika terjadi gangguan ketersediaan (*availability*) pada sistem utama.
- 4) *Assessment* kerentanan keamanan sistem (*security vulnerability system*) secara teratur sesuai dengan kebutuhan.
- 5) Penyusunan IT *Contingency Plan* khususnya yang terkait dengan proses kegiatan kritikal yang diuji validitasnya secara teratur sesuai dengan kebutuhan.

Ad. c Dapat Beroperasi Sesuai Dengan Prosedur Atau Petunjuk Dalam Penyelenggaraan Sistem Elektronik Tersebut.

Proses operasi Sistem Elektronik merupakan hal yang harus diperhatikan termasuk penyampaian layanan informasi elektronik sebagai bagian dari dukungannya kepada proses manajemen kepada pihak-pihak yang membutuhkan sesuai spesifikasi minimal yang telah ditentukan sebelumnya. Manajemen sistem haruslah bertanggung jawab atas beroperasinya layanan-layanan dalam Sistem Elektronik.

Seluruh layanan yang diselenggarakan oleh PSE harus mematuhi ketentuan-ketentuan operasi sistem yang dapat dijelaskan seperti:

- 1) Manajemen tingkat layanan.
- 2) Keamanan dan keberlangsungan sistem.
- 3) Manajemen *software* aplikasi.
- 4) Manajemen infrastruktur.
- 5) Manajemen data.

Aspek minimal yang harus tercakup dalam setiap sistem layanan elektronik mencakup:⁴⁷

- 1) Waktu yang diperlukan untuk setiap layanan yang diterima oleh konsumen.
- 2) Presentase tingkat ketersediaan (*availability*) sistem.
- 3) Waktu yang diperlukan untuk penyelesaian pengaduan insiden atau permasalahan dengan beberapa tingkatan kritikal sesuai dengan kebutuhan.

Setiap pengoperasian infrastruktur teknologi selalu memperhatikan kontrol yang terkait dengan faktor *auditability* yang memungkinkan *audit* atas kinerja dan sejarah transaksi jika sistem elektronik dimanfaatkan untuk transaksi elektronik. Data dari setiap software aplikasi secara kumulatif juga didukung (*dibackup*) secara terpusat dalam media penyimpanan data (*data storage*), terutama *software* aplikasi yang penting.

Ad. d Dilengkapi Dengan Prosedur Atau Petunjuk Yang Diumumkan Dengan Bahasa, Informasi, Atau Simbol Yang Dapat Dipahami Oleh Pihak Yang Bersangkutan Dengan Penyelenggaraan Sistem Elektronik Tersebut.

Informasi yang cukup jelas dan prosedur yang mudah akan memberikan pengguna suatu kenyamanan dalam pemanfaatan Sistem Elektronik, selain itu pengguna juga harus senantiasa berhati-hati, karena kelalaian tentu akan dapat mengakibatkan kerugian kepada diri sendiri dalam menggunakan sistem elektronik tersebut. Hal ini juga perlu diimbangi oleh Setiap pengoperasian Sistem Elektronik, yang harus disertai oleh dokumentasi berikut ini:⁴⁸

- 1) Dokumentasi hasil aktivitas tahapan-tahapan dalam Sistem Elektronik (*history*).

⁴⁷ *Ibid.*

⁴⁸ *Ibid.*

- 2) Manual pengguna, operasi, dukungan teknis dan administrasi.
- 3) Materi transfer pengetahuan dan materi training.

Setiap Sistem Elektronik dijalankan dengan software aplikasi harus selalu menyertakan prosedur *backup* dan *restore*, dan juga mengimplementasikan fungsionalitasnya di dalam *software* aplikasinya.

Ad. e Memiliki Mekanisme Yang Berkelanjutan Untuk Menjaga Kebaruan, Kejelasan, Dan Kebertangjawaban Prosedur Atau Petunjuk.

Mekanisme yang berkelanjutan merupakan upaya Pemeliharaan sistem dan memastikan bahwa seluruh sumber daya sistem dapat berfungsi sebagaimana mestinya dalam durasi waktu dan jangka waktu terus-menerus yang seharusnya dalam rangka mendukung operasi sistem secara optimal. Untuk melakukan hal tersebut perlu dilakukan pengujian secara teratur mekanisme *backup* dan *restore* data, untuk memastikan integritas dan validitas prosedur, serta implementasi mekanisme *inventori* atas media-media penyimpanan data, terutama media-media yang *off-line*.

Dalam beberapa aturan sebenarnya tidak ada menyatakan dengan tegas tentang bagaimana Penyelenggaraan Informasi dan Transaksi Elektronik dalam sistem elektronik yang baik, namun Peraturan Menteri Komunikasi Dan Informatika Nomor 41/PER/MEN.KOM.INFO/11/2007 Tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional mungkin bisa dijadikan panduan bagi PSE untuk menjalankan tugasnya dalam pengelolaan Sistem Elektroniknya.

2. Tanggung Jawab Penyelenggara Sistem Elektronik

a. Pendahuluan

Ada hal-hal yang menarik dipelajari sehubungan dengan kasus tindak pidana mayantara baru-baru ini terutama berkenaan dengan keberlakuan Undang-Undang ITE, khususnya ketentuan larangan melakukan tindak pidana mayantara dan tanggung jawab hukum terhadap penyelenggaraan sistem elektronik yang baik. Demi kepentingan publik, Undang-Undang ITE memberikan kewajiban pihak yang terkait dengan eksistensi Sistem Elektronik itu untuk menghargai dan menyelenggarakan sistem secara baik. Tidak hanya kepada pengguna untuk menjaga kelancaran Sistem Elektronik itu, melainkan juga keharusan penyelenggara untuk menyelenggarakan sistem secara baik. Tanggung jawab PSE dapat dilihat dalam Pasal 15 Undang-Undang ITE yang berbunyi:

- (1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
- (2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
- (3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pada dasarnya tanggung jawab yang dibebankan pada PSE menggunakan prinsip praduga bersalah, atau prinsip pertanggungjawaban berdasarkan atas kelalaian

(*negligence*), yang disebut juga *presumed liability*. Undang-Undang ITE juga menganut prinsip praduga bersalah. Simpulan ini bisa ditarik dari rumusan pasal 15 Undang-Undang ITE, yaitu Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. Penyelenggara diposisikan dalam keadaan bersalah yang dibebankan kewajiban untuk selalu bertanggung jawab, kecuali bila dapat dibuktikan bahwa kesalahan atas sistem elektronik bukan merupakan kesalahannya.⁴⁹

Sesuai yang diamanat pasal 1367 Kitab Undang-Undang Hukum Perdata yang menyatakan setiap orang harus bertanggung jawab atas orang atau benda yang berada di bawah penguasaannya. Namun dalam Undang-Undang ITE tetap terbuka peluang untuk menerapkan prinsip *strict liability* demi kepentingan umum yang lebih besar. Tanggung jawab ketat terutama diterapkan terhadap sistem elektronik yang berdampak besar, dan berpotensi merugikan kepentingan umum yang lebih luas.⁵⁰

Pasal 30 Undang-Undang ITE telah melarang tindakan setiap orang yang dengan sengaja mengakses sistem secara tanpa hak atau melawan hukum (*illegal access*). Kemudian Pasal 32 ayat (2) Undang-Undang ITE yang melarang tindakan memindahkan atau mentransfer informasi elektronik tanpa hak atau melawan hukum kepada sistem elektronik orang lain yang tidak berhak (termasuk dalam kategorisasi tindakan interferensi data (*data interference*)). Dalam menangani kasus-kasus tindak pidana mayantara tersebut, penegakan hukum juga perlu memikirkan keseimbangan resiko dengan kemanfaatan. Dalam konteks ini, pengadilan tetap terbuka menerapkan prinsip

⁴⁹ Hukumonline, 21 Juli 2009. *Op.cit.*

⁵⁰ Edmon Makarim, 22 Januari 2010. *Op.cit.*

strict liability meskipun pasal 15 Undang-Undang ITE menganut *presumed liability*. Meskipun ada peluang bagi hakim menyimpangi *presumed liability*, tapi hakim tetap harus melihat secara proporsionalnya. *Strict liability* selayaknya hanya untuk kasus-kasus tertentu dengan memperhatikan bagaimana penyelenggara melakukan pencegahan dan manajemen resiko. Kalau misalnya kesalahan terjadi karena konsumen tidak membaca dan mengisi data secara benar, unsur kesalahan tentu tidak dapat begitu saja dibebankan kepada PSE.

b. Tanggung Jawab Penyelenggara Sistem Elektronik Dalam Aktivitas Di Dunia Internet

Kegiatan teknologi informasi sekarang ini hampir selalu menggunakan layanan internet dalam pemanfaatannya. baik sebagai koordinasi lembaga pemerintahan maupun dalam hubungannya dengan masyarakat seperti pembayaran tagihan atau pelayanan lainnya. hal ini dapat dilihat dari Peraturan Menteri Komunikasi Dan Informatika Nomor 41/PER/MEN.KOM.INFO/11/2007 Tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional, yang juga mengatur penggunaan internet dalam kegiatan di pemerintahan.

Dengan adanya Undang-Undang ITE, setiap pemilik website (PSE) bisa saja digugat oleh pengunjung yang merasa dirugikan misalnya dalam kegiatan perdagangan elektronik ataupun ketika akunnya yang berisi hal yang penting dan rahasia diakses oleh seseorang. Hal ini dapat dilihat dari Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, yang mengatur tanggung jawab setiap penyedia layanan bagi masyarakat. Selain itu web juga bisa menjadi senjata, Jika pemilik web lalai

mengamankan sistem yang dimilikinya, lalu pihak lain menggunakannya untuk menghancurkan sistem komersial seseorang atau yang lebih parahnya lagi sistem pertahanan negara lain.

Website merupakan sarana penyebaran informasi yang cepat dan efektif dan juga sebuah skenario serangan yang disusun rapi dapat digunakan untuk membuat kacau sistem suatu lembaga. Pada awal Juli 2007 saham Surgutneftegaz perusahaan minyak Rusia nyaris jatuh karena informasi sesat yang disebarakan menggunakan *mailing list* resmi miliknya. Di tengah gelombang krisis keuangan yang melanda seperti itu, bukan hal mustahil tiba-tiba seluruh nasabahnya menarik uangnya beramai-ramai. Hal ini mungkin terjadi hanya karena penyerang yang membajak website bank tersebut berhasil menyisipkan informasi rahasia palsu bahwa bank akan dibekukan oleh Pemerintah Rusia dalam beberapa hari. Hal yang serupa juga terjadi dalam kasus negara Cina dan Amerika Serikat pada tahun 2001 negara China dan Amerika Serikat sempat mengalami hubungan kurang baik, akibat dalam kasusnya situs FBI milik negara Amerika Serikat dirobah dengan gambar seorang pilot Cina yang tewas dalam suatu insiden di Laut Cina Selatan dengan pesawat pengintai Amerika Serikat yang berada di wilayah udara Cina. Hal itu membuktikan tindak pidana mayantara bisa saja mengubah hubungan diplomatik antara negara.⁵¹

Dalam kasus web tersebut, server web adalah batu loncatan bagi pelaku untuk mencari celah dan mencoba menguasai Sistem Elektronik tersebut, bahkan setelah itu

⁵¹ Gildas Deograt Lumy, CISSP (*Information Security Senior Consultant*), 17 Maret 2009. *Risiko Dan Tanggung Jawab Pemilik Website*. www.CHIP.co.id/kolom-oplini.

pelaku mulai menguasai server-server yang mengatur keamanan jaringan komputer dan sistem tersebut akan kacau.⁵²

Pemanfaatan Sistem Elektronik seperti web biasanya digunakan untuk kegiatan finansial seperti perdagangan elektronik, penawaran suatu produk atau kegiatan lainnya oleh pelaku usaha yang disebut juga PSE. Menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, pelaku usaha memiliki bentuk-bentuk tanggung jawab, seperti:⁵³

1) *Contractual liability*

Yaitu tanggung jawab perdata atas dasar perjanjian atau kontrak dari pelaku usaha atas kerugian yang dialami konsumen akibat mengkonsumsi barang dan/atau jasa yang dihasilkan atau memanfaatkan jasa yang diberikannya.

2) *Product liability*

Adalah tanggung jawab perdata secara langsung (*strict liability*) dari pelaku usaha atas kerugian yang dialami konsumen akibat menggunakan produk yang dihasilkannya. Pertanggungjawaban ini diterapkan dalam hal tidak terdapat hubungan perjanjian (*no privity of contract*) antara pelaku usaha dan konsumen.

3) *Professional liability*

Dalam hal hubungan perjanjian merupakan prestasi yang terukur sehingga merupakan perjanjian hasil, tanggung jawab pelaku usaha didasarkan pada pertanggung jawaban

⁵² *Ibid.*

⁵³ Agus Santoso dan Dyah Pratiwi, Desember 2008. *Op.cit*, hal 82.

profesional yang menggunakan tanggung jawab perdata atas perjanjian/kontrak (*contractual liability*) dari pelaku usaha sebagai pemberi jasa atas kerugian yang dialami konsumen.

4) *Criminal liability*

Dalam hubungan pelaku usaha dengan negara dalam memelihara keamanan masyarakat, tanggung jawab pelaku usaha didasarkan pada pertanggungjawaban pidana (*criminal liability*).

Kebanyakan organisasi diluar pemerintahan di Indonesia seperti HMI dan PERMAHI tidak mampu mengadakan website sendiri, karena untuk mengadakan website sendiri perlu menyediakan komputer untuk akses internet atau server yang telah didaftarkan menurut hukum, selain itu sebuah komputer untuk server harus selalu aktif 24 jam dalam sehari dan komputer tersebut juga harus didedikasikan untuk server saja.⁵⁴ Untuk mengatasi hal itu, PSE yang tidak memiliki server dapat memanfaatkan *hosting* atau menggunakan jasa *web developer* (penyedia server) untuk menampilkan websitenya di internet. Banyak sekali *web developer-web developer* asing dan dalam negeri yang menyediakan layanan *hosting web*, mulai dari yang gratis sampai yang membayar seperti, www.rumahweb.com, www.000webhost.com, www.openhosting.com dan lain-lain.

Namun *hosting web* memiliki beberapa kelemahan, seperti kurang akuratnya identitas pengguna *hosting web*, dan kurangnya pengawasan pada kegiatan-kegiatan yang dilakukan, menyebabkan web-web hostinglah yang paling banyak melakukan kelalaian. Salah satu contoh kasusnya adalah kasus anshar.com yang memanfaatkan hosting dari

⁵⁴ Vita Prihatoni Purnomo, 2005. *Cara Mudah Membuat Website Sengan Dreamweaver Mx*. Jakarta: Dian Rakyat, hal.136.

www.openhosting.com yang (servernya) berada di Inggris.⁵⁵ Padahal sebenarnya Undang-Undang ITE telah mengatur mengenai tanggung jawab PSE dalam menyelenggarakan Sistem Elektroniknya, tapi tetap saja penyelenggara dengan memanfaatkan hosting yang paling rawan untuk terjadinya tindak pidana mayantara. Sebenarnya bagaimana bentuk perjanjian web developer dengan PSE tersebut.

Perjanjian hosting website mengandung beberapa muatan.⁵⁶

1) Tujuan kontrak perjanjian website:

- i. Memberikan kekuatan formal secara hukum keberadaan website.
- ii. Menegaskan posisi kepemilikan website.
- iii. Mengatur hak dan kewajiban antara *web developer (vendor)* dan pemilik website.
- iv. Memberikan suasana kondusif antara *vendor* dan pemilik website agar dicapai tujuan yang disepakati.
- v. Menciptakan bisnis indah dalam hidup tanpa konflik.

2) Materi kontrak perjanjian.

Secara garis besar, hal-hal yang akan diatur dalam kontrak perjanjian adalah :

- i. Menegaskan nama perusahaannya masing-masing, antara *vendor* dan pemilik website.
- ii. Merumuskan pola pembayaran.
- iii. Menegaskan jumlah revisi perbaikan website.

⁵⁵ Rakyatmerdeka, 24 Agustus 2006. *Op.cit.*

⁵⁶ Hendra W Saputro, Senin 9 Maret 2009. *Perjanjian Kontrak Website*. Baliorangecomunication.yahoo.com, Diakses tanggal 23 Mei 2010.

- iv. Memperjelas posisi kepemilikan domain name, web hosting, data digital, hak cipta desain dan program.
- v. Menjabarkan fasilitas website yang akan diterima oleh pelanggan.
- vi. Memberi batasan waktu pengerjaan website.
- vii. Mengatur kompensasi atau ganti rugi akibat dari pengingkaran isi kontrak.
- viii. Menjelaskan masa berlaku kontrak website.
- ix. Menjelaskan biaya perpanjangan tahun berikutnya.
- x. Menjabarkan hak dan kewajiban setelah masa perpanjangan kontrak.
- xi. Menjelaskan tanggung jawab hukum pengoperasian website dibebankan pada pemilik website.
- xii. Menyepakati jalan keluar jika terjadi permasalahan yang berkepanjangan.
- xiii. Tanda tangan antara *vendor* dan pemilik web.

Perjanjian web adalah bukti otentik sah secara hukum. Jika musyawarah antara pemilik website dan vendor mengalami kebuntuan, bukti perjanjian website dapat dijadikan bukti yang sah menurut hukum.

c. Tanggung Jawab Penyelenggara Sistem Elektronik Di Dunia Perbankan

Pertanggungjawaban PSE terhadap tindak pidana mayantara akan menjadi lebih berat (ditambah 2/3 dari pidana pokok) jika ternyata objek sistem elektronik tersebut adalah sistem elektronik yang bersifat strategis.⁵⁷ Seperti yang diketahui bahwa bidang perbankan merupakan kawasan kegiatan keuangan terjadi dan menyangkut kerugian yang besar, jika terjadi kejahatan disana. Oleh karena itulah Sistem Elektronik perbankan

⁵⁷ Edmon Makarim, 2004. *Pengantar Hukum Telematika*, Badan penerbit FH UI, Rajawali Pers, hal. 368.

adalah termasuk dalam kategori strategis pula. Dalam konteks perdata, ketentuan tersebut mengindikasikan adanya prinsip *presumed liability*, di mana si Penyelenggara Sistem Elektronik dalam kegiatan perbankan dinyatakan sebagai pihak yang harus bertanggung jawab terhadap segala macam kerugian sekiranya sistem tersebut diselenggarakannya secara melawan hukum sehingga menimbulkan kerugian kepada pihak lain.

PSE untuk kepentingan perbankan seharusnya juga bertanggung jawab berdasarkan “kepatutan” ataupun “kelaziman” dalam penyelenggaraan sistem pengamanan (*security*) yang baik. Sesuai yang diamanatkan Pasal 15 Undang-Undang ITE, PSE dibebankan bertanggung jawab kecuali dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik. Namun yang menjadi permasalahan adalah siapa yang harus dan wajib membuktikan hal tersebut. mengingat PSE adalah wujud penerapan teknologi informasi yang merupakan produk *high-tech*, tentu pengguna sistem tidak akan mempunyai kemampuan untuk membuktikan hal tersebut karena mereka mempunyai keterbatasan akses pada sistem. Oleh karena itu, dengan sendirinya demi keadilan, hal tersebut mengindikasikan adanya pembebanan pembuktian terbalik sebagaimana layaknya dianut dalam Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Tanggal 30 November 2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

Pengaturan tersebut antara lain ditujukan untuk meningkatkan keamanan, integritas data, dan ketersediaan layanan *electronic banking*, misalnya dengan mewajibkan seluruh penerbit kartu untuk menggunakan *chip* pada kartu-kartu pembayarannya, menggunakan

'two factors authentication' pada transaksi *on-line* yang bersifat *financial*, dan juga melakukan enkripsi pada transaksi *mobile banking*.⁵⁸

Penyusunan ketentuan mengenai Penerapan Manajemen Risiko Dalam penggunaan Teknologi Informasi Oleh Bank dalam PBI Nomor 9/15/PBI/2007 dimaksudkan untuk menjadi pokok-pokok penerapan manajemen risiko dalam penggunaan teknologi informasi yang harus diterapkan oleh Bank untuk memitigasi risiko yang berhubungan dengan penyelenggaraan teknologi informasi. Hal ini mengingat terdapat risiko yang dapat merugikan Bank dan nasabah seperti risiko operasional, risiko hukum, dan risiko reputasi selain risiko perbankan lainnya seperti risiko likuiditas dan risiko kredit.⁵⁹

Dalam PBI diatur bahwa Bank dapat menyelenggarakan teknologi informasi sendiri dan/atau menggunakan jasa pihak penyedia jasa teknologi informasi sepanjang memenuhi persyaratan antara lain:⁶⁰

- 1) Bank bertanggung jawab atas penerapan manajemen risiko.
- 2) Pihak penyedia jasa harus menjamin keamanan seluruh informasi termasuk rahasia bank dan data pribadi nasabah.
- 3) Pihak penyedia jasa tetap memberikan akses kepada auditor intern, ekstern dan Bank Indonesia.
- 4) Pihak penyedia jasa harus bersedia untuk kemungkinan *early termination* apabila menyulitkan fungsi pengawasan Bank Indonesia.

⁵⁸ PBI No. 7/52/PBI/2005 tanggal 28 Desember 2005 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu (PBI APMK).

⁵⁹ PBI No. 9/PBI/2007 tanggal 30 November 2007 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Oleh Bank Umum (PBI TSI).

⁶⁰ *Ibid.*

Perbankan adalah sektor yang strategis sehingga lumrah jika diberi standar penyelenggaraan yang lebih ketat dan dinamis sesuai dengan perkembangan sistem pengamanan. Selain proses pidana kepada para pelaku, perbaikan ketentuan administratif terkait penyelenggaraan sistem elektronik dalam lingkup perbankan perlu dilakukan.

B. Peranan Penyelenggara Sistem Elektronik Dalam Pembuktian Alat Bukti Elektronik

Topik-topik sebelumnya telah menerangkan mengenai tugas dan tanggung jawab PSE dalam Penyelenggaraan Sistem Elektronik. Topik tersebut telah memberikan pengetahuan bahwa antara Sistem Elektronik dan PSE tidak dapat dipisahkan, apapun yang terjadi di dalam sistem elektronik tersebut, PSE telah mengetahui dan menyadarinya. Hal itu selaras dengan Pasal 15 Undang-Undang ITE yang menyatakan tanggung jawab PSE terhadap Sistem Elektroniknya.

Seperti yang dinyatakan Pasal 1 butir 26 Kitab Undang-Undang Hukum Acara Pidana "saksi adalah orang yang dapat memberikan keterangan guna kepentingan penyidikan, penuntutan dan peradilan tentang suatu perkara pidana yang ia dengar, ia lihat sendiri dan ia alami sendiri." Dari pasal tersebut dapat diambil unsur orang-orang yang dapat dijadikan saksi yaitu:

1. Mendengar sendiri.
2. Melihat sendiri.
3. Dan mengalami sendiri.

Ketika PSE diharuskan mengetahui apapun yang terjadi pada Sistem Elektroniknya, maka hal ini mengidentasikan telah terpenuhinya unsur sebagai saksi bagi PSE ketika terjadi suatu tindak pidana mayantara dalam Sistem Elektronik yang diselenggarakannya. kategori mengetahui terjadinya suatu tindak pidana mayantara oleh PSE dapat dilihat dari beberapa syarat Penyelenggaraan Sistem Elektronik (Pasal 16 Undang-Undang ITE):

1. PSE menjadi saksi untuk dapat dimintakan keterangannya mengenai kejadian ataupun data pada saat terjadi tindak pidana mayantara oleh karena PSE dapat menampilkan Informasi Elektronik dan Dokumen Elektronik kembali.
2. PSE dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik, sehingga keterangan yang diberikan PSE dapat dipercaya karena data yang dimiliki PSE bersifat asli tanpa adanya perobahan.
3. Data atau informasi yang disampaikan PSE dapat dipercaya, karena pengoperasian Sistem Elektronik melalui kendalinya, sehingga untuk menampilkan Informasi Elektronik dapat dengan mudah diperoleh.
4. Keterangan yang diberikan mengenai alat bukti oleh PSE dapat dimengerti, karena PSE dapat memahami keterangan-keterangan yang terdapat di Sistem Elektronik yang diselenggarakannya. Pemahaman tersebut disebabkan PSE mengetahui simbol-simbol dan angka-angka dalam Sistem Elektronik tersebut.
5. Informasi yang ditemukan dapat diperoleh lagi dari PSE dalam jangka waktu yang berbeda, jika dalam pengembangan kasus terdapat keterangan baru dari

penyelenggara sehubungan dengan Sistem Elektroniknya yang memiliki mekanisme yang berkelanjutan.

Selain berperan sebagai saksi dalam tindak pidana mayantara, PSE juga mempunyai kedudukan khusus ketika terjadi tindak pidana mayantara yaitu membuktikan sendiri jika Sistem Elektroniknya telah disusupi oleh pihak lain ataupun terdapat tindak pidana mayantara di luar kendalinya. Beban membuktikan sendiri oleh PSE lahir dari tanggung jawabnya yang dimiliki sesuai Pasal 15 Undang-Undang ITE.

Pemahaman mengenai bentuk tanggung jawab PSE dimulai dari adanya hubungan hukum yang terjadi diantara kedua belah pihak. Hubungan hukum antara PSE sebagai penyedia jasa dan konsumen atau pengguna pada akhirnya melahirkan suatu hak dan kewajiban yang mendasari terciptanya suatu beban pembuktian, oleh karena akibat bentuk tindakan tidak bersalah atas tindak pidana yang terjadi pada Sistem Elektroniknya. Edmon Makarim mengatakan, kewajiban bagi Penyelenggara Sistem Elektronik adalah keandalan, keamanan dan pertanggungjawaban (Pasal 15 ayat 1) Undang-Undang ITE, pengecualian jika terjadi *force majeure*.⁶¹

Selain itu yang melatar belakangi terjadi pembuktian terbalik juga dapat dilihat dari posisi yang tidak seimbang antara korban dengan PSE. Hal ini karena korban tindak pidana mayantara pada umumnya tidak mengetahui mengenai cara kerja sistem elektronik sebab untuk memahaminya perlu orang yang memang kompeten dibidangnya. Menurut Profesor R. Subekti, S.H. dalam bukunya "Hukum Pembuktian" mengatakan bahwa, "beban pembuktian harus dilakukan dengan adil dan tidak berat sebelah, karena

⁶¹ Depkominfo, 26 Pebruari 2009. *Undang-Undang Informasi Dan Transaksi Elektronik Bantu Beri Pedoman Bagi Hakim*. <http://www.depkominfo.go.id>, Diakses tanggal 25 Maret 2010.

suatu pembagian beban pembuktian yang berat sebelah berarti *a priori* menjerumuskan pihak yang mendapat beban terlalu berat kedalam jurang kekalahan.”⁶² Berkaitan dengan beban pembuktian terhadap alat bukti elektronik, hendaknya dibebankan kepada pihak yang mempunyai alat-alat yang memadai untuk membuktikan bahwa tanda tangan elektronik tersebut dibuat dengan prosedur yang handal dan dapat dipertanggungjawabkan.

Pernyataan beban pembuktian PSE bukan tidak beralasan, sebab beban pembuktian PSE ini dapat dilihat dari Pasal 15 ayat (3) Undang-Undang ITE yang menyatakan tanggung jawab PSE dapat dilepaskan jika dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik. Beban pembuktian PSE juga dapat dilihat dalam Pasal 22 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen yang menegaskan bahwa beban pembuktian (ada tidaknya kesalahan) berada pada pelaku usaha dalam perkara pidana pelanggaran seperti Pasal 19 ayat (4), Pasal 20, dan Pasal 21 Undang-Undang Perlindungan Konsumen.

Selain pembuktian, petunjuk juga sangat berguna untuk membuat terang tindak pidana mayantara yang terjadi ataupun mengungkapkan pelaku yang terlibat.⁶³ Dalam memulai penyidikan tindak pidana mayantara, Polri menggunakan parameter alat bukti yang sah sesuai dengan Pasal 184 KUHAP yang dikaitkan dengan pembuktian pendukung untuk memenuhi aspek legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi. Keterangan PSE memiliki aspek petunjuk bagi penyidik karena dalam tahap ini penyidik akan membuktikan tindak pidana yang terjadi serta bagaimana dan sebab-sebab tindak pidana tersebut terjadi. Selain itu keterangan PSE juga

⁶² Subekti, 1983. *Op.cit*, hal. 34.

⁶³ Pasal 1 angka 13 Undang-Undang No 2 Tahun 2002 Tentang Kepolisian.

bisa digunakan untuk mencari jejak pelaku, sebab jika melihat PSE sebagai penyelenggara yang bertanggung jawab dan memenuhi syarat maka PSE tentu memiliki data dimana menerangkan kegiatan yang terjadi pada Sistem Elektroniknya. Seperti contoh, PSE dapat memfasilitasi aplikasi yang mengetahui alamat pengguna dalam sistem elektroniknya atau IP (*identity*) sehingga dapat diketahui alamat pengguna.

Dengan Adanya beban pembuktian pada PSE, maka menyebabkan PSE juga ikut dalam menemukan Alat bukti elektronik. Meskipun begitu, alat bukti elektronik yang dibuktikan PSE tidak begitu saja nanti menjadi alat bukti dalam suatu perkara pidana, butuh peran penyidik untuk menyaring dan menguji alat bukti tersebut untuk menjadi alat bukti yang sah.⁶⁴

C. Pentingnya Keterangan Penyelenggara Sistem Elektronik Terhadap Kekuatan Hukum Suatu Alat Bukti Elektronik

Di dalam hukum acara pembuktian perkara pidana, kedudukan alat bukti begitu penting mengingat alat buktilah yang menjadi suatu dasar bagi para pihak untuk membuktikan bersalah atau tidaknya seseorang dalam perkara yang digugat kepadanya. Tujuan dan guna pembuktian bagi para pihak yang terlibat dalam proses pemeriksaan persidangan adalah:⁶⁵

1. Bagi penuntut umum, pembuktian adalah merupakan usaha untuk meyakinkan hakim yakni berdasarkan alat bukti yang ada, agar menyatakan seorang terdakwa bersalah sesuai dengan surat atau catatan dakwaan.

⁶⁴ Agus Santoso dan Dyah Pratiwi, Desember 2008. *Op.cit*, hal. 81.

⁶⁵ Ahmad M Ramli, Desember 2004. *Prinsip-prinsip Cyber Law Dan kendala Hukum Positif Dalam Menanggulangi Cyber Crime*. Jakarta: Fakultas Hukum Universitas Padjajaran, hal. 103.

2. Bagi terdakwa atau penasehat hukum, pembuktian merupakan usaha untuk meyakinkan hakim, yakni berdasarkan alat bukti yang ada, agar menyatakan terdakwa dibebaskan atau dilepaskan dari tuntutan hukum atau meringankan pidananya. Untuk itu terdakwa atau penasehat hukum jika mungkin harus mengajukan alat-alat bukti yang menguntungkan atau meringankan pihaknya. Biasanya bukti tersebut di sebut bukti kebalikan.
3. Bagi hakim, dengan adanya alat-alat bukti yang ada dalam persidangan baik yang berasal dari penuntut umum atau penasehat hukum/terdakwa dibuat dasar untuk membuat keputusan.

Dalam Undang-Undang ITE terdapat karakteristik-karakteristik alat bukti baru yang harus mendapat pengkajian hukum lebih lanjut yaitu alat bukti elektronik seperti, Informasi Elektronik dan Dokumen Elektronik. Keberadaan alat bukti elektronik sebagai salah-satu bentuk alat bukti, memiliki suatu identitas baru yaitu sebagai salah satu bentuk metode pembuktian baru di dalam hukum pidana, hal ini selaras dengan Pasal 5 Undang-Undang ITE yang memberikan pernyataan bahwa alat bukti elektronik merupakan salah satu dari alat bukti yang sah (*wettige bewijsmiddelen*).⁶⁶

Masalah keabsahan adalah persoalan yang terkait dengan pengakuan data elektronik. Jika data atau dokumen elektronik tersebut diterima atau diakui secara hukum, dengan sendirinya proses otentikasi atas data tersebut akan megikutinya. Selayaknya kegiatan teknologi informasi yang dilakukan oleh para pihak harus dinyatakan *valid* dan memiliki nilai pembuktian di pengadilan. Hal ini penting, karena menyangkut persoalan

⁶⁶ Hwian Christianto, 2009. *Alat Bukti Email Dalam Perkara Pidana*. hwall4jc@yahoo.co.id, Diakses tanggal 12 Maret 2010.

siapa yang bertanggung jawab terhadap tindak pidana mayantara yang terjadi pada Sistem Elektronik.

Sebenarnya ada satu hal yang patut dipertimbangkan dalam pengakuan suatu data elektronik mengenai pembuktiannya dalam sidang pengadilan. Edmon Makarim mengatakan, Undang-Undang Informasi Dan Transaksi Elektronik (ITE) telah memberikan tempat bagi Informasi Elektronik untuk dapat diterima dan memberikan prosedur tertentu sebagai pedoman bagi hakim dalam pemeriksaan dan pembuktian. "Suatu Sistem Elektronik hanya dapat dipercaya apabila telah dilakukan pemeriksaan oleh para pihak yang terkait atau mempunyai kemampuan untuk itu," kata Edmon Makarim pada acara sosialisasi Undang-Undang ITE di hadapan pegawai pengadilan negeri dan pengadilan tinggi serta pejabat Biro Hukum Departemen atau Lembaga Negara di Jakarta, Kamis 26 Februari 2009.⁶⁷

Berdasarkan Pasal 6 Undang-Undang ITE yang menyatakan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Pasal tersebut jelas menerangkan alat bukti elektronik yaitu Informasi Elektronik dan Dokumen Elektronik dapat dikatakan sah apabila dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Padahal, suatu informasi dan Dokumen Elektronik diakses, ditampilkan, dijamin keutuhannya dan dipertanggungjawabkan adalah syarat operasi dari Sistem Elektronik oleh PSE menurut Pasal 16 Undang-Undang ITE. Sehingga jika sistem

⁶⁷ Depkominfo, 26 Februari 2009. *Op.cit.*

elektronik yang diselenggarakan PSE tidak memenuhi syarat yang ditentukan Pasal 16 Undang-Undang ITE, maka alat bukti tersebut tidak bisa diajukan sebagai alat bukti dalam pengadilan.

Pernyataan ini selaras dengan yang dinyatakan Pasal 7 Undang-Undang ITE yang berbunyi “Setiap Orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan. Menurut Edmon Makarim syarat yang harus dipunyai PSE agar bisa alat bukti elektronik dalam Sistem Elektroniknya diakui, maka PSE sebagai pelaku usaha harus memiliki sertifikasi keandalan yang dilakukan oleh Lembaga Sertifikasi Keandalan, karena sertifikasi keandalan merupakan bukti pelaku usaha melakukan perdagangan secara layak dan memiliki logo sertifikasi (*trust mark*).⁶⁸ Dalam hal inilah peran PSE sangat menentukan keabsahan suatu alat bukti elektronik.

Dalam beberapa kasus pidana seperti korupsi, terorisme, narkoba dan lain-lain, penggunaan alat bukti elektronik untuk penegakan hukum juga sudah mulai dilakukan. Alat bukti elektronik yang sering digunakan adalah alat bukti surat elektronik atau yang lebih dikenal seperti E-mail. Dipakainya E-mail sebagai alat bukti dalam beberapa kasus adalah karena E-mail memiliki banyak sekali kegunaan yang dapat difungsikan untuk berbagai wadah kegiatan seperti, Transaksi Elektronik (sebagai pemberitahuan transaksi telah berhasil), sebagai sarana kegiatan pendidikan, bisnis, perdagangan, sosial dan berbagai kegiatan lainnya. Hal ini dapat dilihat dari Pasal 5 ayat (1) Undang-Undang ITE

⁶⁸ *Ibid.*

yang menyatakan "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah." E-mail memiliki persamaan dengan alat bukti surat dalam KUHP yang terdiri dari:⁶⁹

1. Berita acara dan surat lain, dokumen dalam bentuk yang sesuai dibuat pejabat umum yang berwenang.
2. Surat yang di buat menurut ketentuan peraturan perundang-undangan tentang suatu keadaan.
3. Surat keterangan ahli yang diminta secara resmi.
4. Surat lain yang hanya berlaku jika berhubungan dengan isi dari alat pembuktian lain.

E-mail Sebagai salah-satu alat bukti elektronik juga dapat digolongkan sebagai alat bukti surat yang hanya berlaku jika berhubungan dengan isi dari alat bukti lain. Hal ini dikarenakan, E-mail pada awal proses pembuatannya tidak dimaksudkan sebagai alat bukti dari suatu peristiwa, sehingga baru dapat dianggap berlaku jika berhubungan dengan isi dari alat pembuktian lain.⁷⁰

E-mail sama halnya dengan alat bukti elektronik yang merupakan alat bukti yang tidak dapat berdiri sendiri dan membutuhkan alat bukti lainnya seperti keterangan saksi yang mengetahuinya. Dalam melakukan penyelidikan dan penyidikan untuk menemukan bukti-bukti kuat yang mendukung alat bukti elektronik, harus didukung saksi-saksi yang mengetahui peristiwa E-mail itu. Untuk inilah dibutuhkan keterangan PSE sebagai pihak yang mengetahui terjadinya E-mail tersebut, sebab lokasi terjadinya E-mail di fasilitasi

⁶⁹ Efa laela Fakhriah, 2009. *Bukti Elektronik Dalam Sistem Pembuktian Perdata*. Bandung: Alumni, hal. 148.

⁷⁰ *Ibid*, hal. 149.

oleh PSE dalam Sistem Elektroniknya. Oleh karena itu apabila ada perkara pidana dengan bukti berupa E-mail, akan dinilai sangat kurang bagi aparat penegak hukum untuk melakukan penangkapan pada tersangka jika tidak didukung dengan keterangan yang memperkuat E-mail seperti keterangan PSE.

Di beberapa negara, data elektronik dalam bentuk E-mail sudah menjadi pertimbangan bagi hakim dalam memutus suatu perkara. Kiranya, tidak perlu menunggu lama agar persoalan bukti elektronik, termasuk E-mail, untuk mendapatkan pengakuan secara hukum sebagai alat bukti yang sah di pengadilan.

Untuk membawa alat bukti elektronik ke persidangan perlu dilakukan pengalihan alat bukti elektronik kedalam media lainnya seperti *micofilm*, baik itu dalam bentuk CD, DVD, ataupun dicetak kedalam kertas, sehingga dapat dibawa kepersidangan. Namun yang menjadi persoalan apakah nanti pengalihan alat bukti elektronik tersebut sah dalam persidangan.

Menurut Pasal 13 Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan, pengalihan alat bukti elektronik wajib dilegalisasi. Dalam melakukan legalisasi diperlukan berita acara pengalihan yang mencakup:

1. Keterangan tempat, hari, tanggal, bulan, dan tahun dilakukannya legalisasi;
2. Keterangan bahwa pengalihan dokumen perusahaan yang dibuat di atas kertas ke dalam *mikrofilm* atau media lainnya telah dilakukan sesuai dengan aslinya; dan
3. Tanda tangan dan nama jelas pejabat yang bersangkutan.

Dalam proses legalisasi, PSE merupakan pihak yang memiliki hubungan hukum dengan alat bukti elektronik yang dialihkan, jika alat bukti tersebut didapat dalam Sistem

Elektroniknya. Oleh karena itu keterangan keaslian alat bukti dan tanda tangan PSE sangat diperlukan dalam berita pengalihan dokumen di pengadilan.

Menurut Direktur Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia, Brian A. Prasetyo, sependapat tentang perlunya berita acara pengalihan Dokumen Elektronik. Undang-Undang ITE tak menyinggung secara khusus kewajiban berita acara pengalihan tersebut. “Dengan *based on practice* yang ada sekarang, maka berita acara sudah seharusnya ada, karena kita harus lihat kepada fungsinya, yaitu satu fungsi pertanggungjawaban, dan kedua fungsi verifikasi dari berita acara.”⁷¹

Semua alat bukti elektronik tersebut dapat diakui secara hukum setelah mendengarkan pendapat (keterangan) saksi. Dokumen tersebut juga bisa diakui tanpa adanya keterangan, jika sebelumnya telah ada sertifikasi terhadap kegiatan elektronik. Cara kedua untuk mengakui dokumen elektronik adalah dengan menyandarkan pada hasil akhir komputer. Misalkan dengan *out put* dari sebuah program komputer yang hasilnya tidak didahului dengan campur tangan secara fisik. Contohnya, rekaman *log in internet*, rekaman telepon dan transaksi *Automatic Transfer Money (ATM)*.⁷² Artinya, dengan sendirinya bukti elektronik dan juga E-mail dapat diakui sebagai bukti elektronik dan memiliki kekuatan hukum. Kecuali bisa dibuktikan lain, data tersebut bisa dikesampingkan.

Alat bukti elektronik sangat penting bagi penyidik, baik untuk mengetahui siapa yang terlibat dalam suatu tindak pidana mayantara ataupun membuat jelas suatu perkara

⁷¹ Hukumonline, Senin, 9 Februari 2009. *Berita Acara Pengalihan Dokumen Elektronik Perlu*. <http://www.hukumonline.com>, Diakses 11 Juni 2010.

⁷² PTUN Mataram, 10 Februari 2009. *Kekuatan Email Dalam Proses Persidangan*. <http://ptun-mataram.go.id>, Diakses tanggal 23 Februari 2010.

pidana, Dengan mengetahui siapa yang mengirimkan, tergugat dapat menjadikan alat bukti elektronik tersebut sebagai dasar untuk melakukan gugatan atau penuntutan.



BAB IV

PENUTUP

A. Kesimpulan

Berdasarkan pada hasil penelitian dan pembahasan yang dilakukan penulis maka dalam penelitian ini dapat ditarik kesimpulan sebagai berikut:

1. Kedudukan PSE dalam Penyelenggaraan Sistem Elektronik, dapat dilihat Ketika PSE memanfaatkan Sistem Elektroniknya untuk pengguna, PSE dituntut harus mengetahui dan bertanggung jawab terhadap beroperasinya sistem tersebut (Pasal 15 Undang-Undang ITE). Oleh sebab itu, ketika terjadi tindak pidana mayantara dalam Sistem Elektroniknya, PSE dianggap tahu dan bertanggung jawab atas kejahatan tersebut kecuali dapat dibuktikan adanya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik. Selain itu syarat Penyelenggaraan Sistem Elektronik yang ditetapkan Pasal 16 ayat (1) Undang-Undang ITE, membuat PSE semakin memperkuat peranannya dalam membantu pembuktian dan penemuan alat bukti elektronik tindak pidana mayantara.
2. Peranan PSE dalam pembuktian alat bukti elektronik tindak pidana mayantara dapat dilihat dari tugas dan tanggung jawabnya yang menggambarkan bahwa ia mengetahui apa yang terjadi dalam Sistem Elektroniknya. Dalam hal ini kedudukan hukum PSE memperlihatkan terpenuhinya syarat sebagai saksi dalam Kitab Undang-Undang Hukum Acara Pidana. Dalam perannya sebagai saksi PSE juga mempunyai keistimewaan lain, keistimewaan tersebut dapat dilihat dari Pasal 15 ayat (3) Undang-Undang ITE yang menyatakan adanya beban pembuktian oleh PSE

terhadap Sistem Elektroniknya yang menyebabkan PSE juga ikut berperan menemukan alat bukti elektronik.

3. keterangan PSE begitu penting dalam memperkuat alat bukti elektronik, dimana bukanlah hanya sekedar penambah. Hal ini disebabkan alat bukti elektronik tidak dapat berdiri sendiri sehingga memerlukan unsur-unsur lain untuk memperkuat alat bukti tersebut sehingga sah di depan hukum. Unsur-unsur lain tersebut haruslah dapat dipercaya karena ini berhubungan dengan keabsahan alat bukti elektronik dan PSE-lah yang dapat melakukan itu. Sebagai contoh pentingnya keterangan PSE adalah diperlukannya keterangan PSE dalam surat berita acara pengalihan dokumen elektronik di persidangan, karena PSE memiliki tanggung jawab terhadap Sistem Elektroniknya yang diakui oleh Undang-Undang ITE sebagai syarat diakuinya sebuah alat bukti elektronik dalam suatu Sistem Elektronik.⁷³

B. Saran

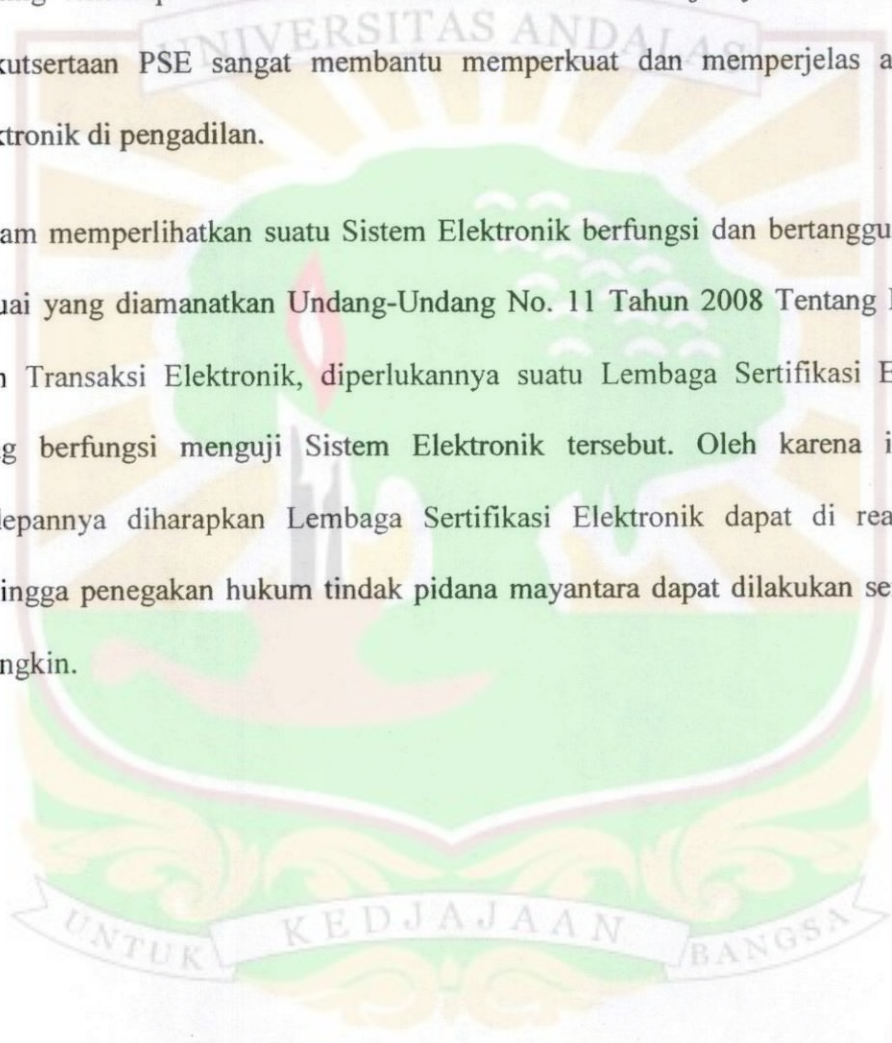
Dari kesimpulan diatas, maka diajukan beberapa saran sebagai berikut:

1. Kedudukan hukum PSE dalam Undang-Undang ITE telah memperlihatkan andil besarnya terhadap terjadinya tindak pidana mayantara dalam Sistem Elektronik, sehingga PSE memiliki peranan besar dalam penemuan alat bukti elektronik.

⁷³ Pasal 6 Undang-Undang Nomor 11 Tahun 2008 yang berbunyi:

“Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan”

2. Peranan PSE sangat membantu dalam penegakan hukum di Indonesia agar suatu tindak pidana mayantara dapat dibuktikan secara jelas dan terang, sehingga dapat ditemukan pelaku tindak pidana yang sebenarnya.
3. Dengan adanya peran PSE tersebut, memperlihatkan keterangan PSE juga begitu penting terhadap keabsahan alat bukti elektronik selanjutnya. Oleh karena itu keikutsertaan PSE sangat membantu memperkuat dan memperjelas alat bukti elektronik di pengadilan.
4. Dalam memperlihatkan suatu Sistem Elektronik berfungsi dan bertanggung jawab sesuai yang diamanatkan Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, diperlukannya suatu Lembaga Sertifikasi Elektronik yang berfungsi menguji Sistem Elektronik tersebut. Oleh karena itu untuk kedepannya diharapkan Lembaga Sertifikasi Elektronik dapat di realisasikan, sehingga penegakan hukum tindak pidana mayantara dapat dilakukan semaksimal mungkin.



DAFTAR PUSTAKA

A. Buku

- Arief, Barda Nawawi, 2006. *Tindak Pidana Mayantara (Perkembangan Kajian Cyber Crime Di Indonesia)*. Jakarta: PT. Raja Grafindo Persada.
- Djaja, Ermansjah, 2010. *Penyelesaian Sengketa Hukum Teknologi Informasi Dan Transaksi Elektronik*. Yogyakarta: Pustaka Timur.
- Fakhriah, Efa Laela, 2009. *Bukti Elektronik Dalam Sistem Pembuktian Perdata*. Bandung: Alumni.
- Makarim, Edmon, 2005. *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*. Jakarta: PT Raja Grafindo Persada.
- Mansyur, Dikdik M. Arief Dan Elisatris Gultom, 2006. *Cyber Law (Aspek Hukum Teknologi Informasi)*. Bandung: Refika Aditama.
- Hamzah, Andi, 1996. *Hukum Pidana Yang Berkaitan Dengan Komputer (edisi kedua)*. Jakarta: Sinar Grafika.
- Harahap, M. Yahya, 2000. *"Pembahasan Permasalahan Dan Penerapan KUHP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali"*, Edisi Kedua. Jakarta: Sinar Grafika.
- Moeljatmo, 1985. *Azas-Azas Hukum Pidana*. Jakarta: Bina Aksara.

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

Purnomo, Vita Prihatoni, 2005. *Cara mudah membuat website sengan dreamweaver mx*. Jakarta: Dian Rakyat.

Raharjo, Agus, 2002. *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya Bakti.

Subekti, 1983. *Hukum Pembuktian*. Jakarta: Pradnya Paramita.

Widodo, 2009. *Sistem Pemidanaan Cyber Crime*. Yogyakarta: Laksbang Mediatama.

Waluyo, Bambang, 1996. *Dalam Peradilan Indonesia*. Jakarta: Sinar Grafika.

B. Jurnal Dan Makalah

Golose, Petrus Reinhard, Agustus 2006. *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri*. Jakarta: Buliten Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, hal. 29-30.

Santoso, Agus dan Dyah Pratiwi, Desember 2008. *Tanggung Jawab Penyelenggara Sistem Elektronik Perbankan Dalam Kegiatan Transaksi Elektronik pasca Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik*, Jakarta: Jurnal Legislasi Indonesia Vol 5 No 4.

Setiawan, Deris. *Bagaimana Menjadi Hacker (Talk Show Computer Easy di Radio SONORA FM)*. Kerjasama Radio SONORA FM dan PT. Elex Media Komputindo, 30 Agustus 2003.

Makarim, Edmon, 22 Januari 2010. *Pembobolan Sistem Elektronik Dari Segi Hukum*. Koran Seputar Indonesia.

D. Internet:

Berita Acara Pengalihan Dokumen Elektronik Perlu, <http://www.hukumonline.com>, Senin, 9 Pebruari 2009, diakses tanggal 12 maret.

Haris, Freddy, *Cyber Crime Dari Prespektif Akademis*, Lembaga Kajian Hukum Dan Teknologi Fakultas Hukum Universitas Indonesia, hal. 15-16, dalam (<http://www.gipi.or.id>), diakses tanggal 30 mei 2004.

<http://www.rakyatmerdeka.co.id>, 24 Agustus 2006, *Teroris Semarang Terlibat Anshar.Net*, diakses tanggal 30 Desember 2009.

<http://www.suaramerdeka.com/harian/0207/24/nas13.htm>, *Kegelisahan Dunia Oleh Cyber Crime*, diakses 24 Juli 2002.

Penyelenggara Sistem Elektronik Gunakan Prinsip Praduga Bersalah, www.hukumonline.com, Selasa, 21 Juli 2009, diakses tanggal 13 Februari 2010.

Syailendra Wisnu, *Alat Bukti Elektronik dalam Undang-Undang Informasi dan Transaksi Elektronik*, www.google.com, de_rechter_2007@blog.uns.ac.id, 28 juli 2009, diakses tanggal 23 Pebruari 2010.

Suhartono, *Penanggulangan Kejahatan Hacking Di Indonesia (Suatu Kajian dalam Perspektif Kebijakan Hukum Pidana Saat ini dan Wacana Kebijakan Hukum Pidana Akan Datang)*, <http://www.google.com> dari suhartono_71@yahoo.com, diakses tanggal 29 September 2009.

Lumy, Gildas Deograt, CISSP (*Information Security Senior Consultant*), 17 Maret 2009.

Risiko Dan Tanggung Jawab Pemilik Website. www.CHIP.co.id/kolom-oplini.

Saputro, Hendra W, Senin 9 Maret 2009. *Perjanjian Kontrak Website*. Diakses di google (Bali orange communication.yahoo.com) tanggal 23 Mei 2010.

<http://www.depkominfo.go.id>, 26 Pebruari 2009. *Undang-Undang Informasi Dan Transaksi Elektronik Bantu Beri Pedoman Bagi Hakim*. Diakses tanggal 25 maret 2010.

<http://www.hukumonline.com>, Senin, 09 Pebruari 2009. Berita Acara Pengalihan Dokumen Elektronik Perlu. Diakses 11 juni 2010.

E. Undang-Undang

KUHP dan KUHP.

Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan.

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

Undang-Undang Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-Undang No. 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi.

Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.

Undang-Undang Nomor 25 Tahun 2003 Tentang Pencucian Uang.

Undang-Undang Nomor 21 Tahun 2007 Tentang Pemberantasan Tindak Pidana Perdagangan Orang.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 88 Tahun 1999 Tentang Tata Cara Pengalihan Dokumen Perusahaan Ke Dalam Mikrofilm Atau Media Lainnya Dan Legalisasi.

PBI No. 7/52/PBI/2005 tanggal 28 Desember 2005 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu (PBI APMK).

PBI No. 9/PBI/2007 tanggal 30 November 2007 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Oleh Bank Umum (PBI TSI).

Peraturan Menteri Komunikasi Dan Informatika Nomor:
41/PER/MEN.KOMINFO/11/2007 Tentang Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional.



DEPARTEMEN PENDIDIKAN NASIONAL

Fakultas Hukum Universitas Andalas

Kampus Jl. Pancasila No. 10 Padang - 25117

Telp. (0751) 27404

Nomor : 180/H.16.4/KM-RM/2010

29 April 2010

Lamp : -

Hal : Tugas Survey/Penelitian/KKN/Studi Pustaka
Co-Schap/Praktek Lapangan/KKN/Wawancara/dll

Kepada Yth,
Sdr, Kejaksaan Negeri Padang
di
Padang

Dengan ini disampaikan kepada saudara , bahwa kami menugaskan seorang mahasiswa :

Nama : Arisman
Nomor BP : 06 940 055
Program Kekhususan : Hukum Pidana
Fakultas : **Hukum Reguler Mandiri**
Alamat : Komp. Jondul Rawang Barat Blok. GG No. 15 Padang

Untuk melaksanakan Survey / Penelitian Lapangan / Studi Pustaka / Pengumpulan Data terhitung mulai tanggal 01 Mei 2010 s/d 01 Agustus 2010, guna mendapatkan bahan / data dalam rangka menyusun Skripsi dengan judul : “ **Peranan Penyelenggara sistem Elektronik dalam Menemukan Alat Bukti Elektronik Tindak Pidana Mayantara di Indonesia** ” pada kantor yang saudara pimpin.

Sehubungan dengan maksud diatas , kami mohon bantuan saudara agar kepada yang Bersangkutan dapat diberi kemudahan-kemudahan guna terlaksananya penelitian tersebut Disamping itu kami mengharapkan surat keterangan dari kantor saudara apabila yang bersangkutan telah selesai melaksanakan tugas dimaksud.

Demikianlah disampaikan kepada saudara, atas bantuan dan kerjasamanya diucapkan terima kasih.

Ang Dekan

Pembantu Dekan I

YOSERWAN, SH.MH.LLM
NIP. 196212311989011002

Tembusan disampaikan kepada Yth,

1. Sdr. Dekan Fakultas Hukum Universitas Andalas.
2. Sdr. Ketua Bagian Hukum Pidana.
3. Sdr Pembimbing I dan II.
4. Sdr Yang Bersangkutan .
5. Peringgal.