KEBIJAKAN PENEGAKAN HUKUM DALAM UPAYA PENANGGULANGAN TINDAK PIDANA TEKNOLOGI INFORMASI[1]

Oleh: Ahmad S. Daud[2]

ABSTRAK

Tujuan dilakukannya penelitian ini adalah untuk mengetahui bagaimana kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini, bagaimana kebijakan aplikatif yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi, dan bagaimana sebaiknya kebijakan formulasi dan kebijakan aplikatif hukum pidana dalam penanggulangan tindak pidana teknologi informasi di masa yang akan datang. Dengan menggunakan metode penelitian kepustakaan dapast disimpulkan bahwa: 1. Dalam menjamin keamanan, keadilan dan kepastian hukum dalam penegakan hukum *(law enforcement)* di dunia *cyber* dapat terlaksana dengan baik maka harus dipenuhi 4 (empat) syarat yaitu: (1) Adanya aturan perundang-undangan khusus yang mengatur dunia *cyber.* (2) Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus menangani *cybercrime* . (3) Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu. (4) Kesadaran hukum dari masyarakat yang terkena peraturan. Selain ke 4 (empat) syarat tersebut penegakan hukum di dunia maya juga sangat tergantung dari pembuktian dan yuridiksi yang ditentukan oleh undang-undang. 2. Kebijakan pemerintah Indonesia dengan diundangkannya Undang-Undang No. 11 tahun 2008 tentarig Informasi dan Trarisaksi Elektroriik (UU ITE) merupakan payung hukum pertama yang mengatur dunia siber *(cyberlaw),* sebab muatan dan cakupannya yang luas dalam membahas pengaturan di dunia maya seperti perluasan alat bukti elektronik sama dengan alat bukti yang sudah dikenal selama ini, diakuinya tanda tangan elektronik sebagai alat verifikasi, dan autentikasi yang sah suatu dokumen elektronik, serta pengaturan perbuatan-perbuatan yang dilakukan dalam *cyberspace* sebagai suatu tindak pidana. 3. Peraturan mengenai *cyberlaw* harus dapat mencakup perbuatan yang dilakukan di luar wilayah Indonesia tapi merugikan kepentingan orang atau negara dalam wilayah Indonesia. Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur masalah yurisdiksi yang di dalamnya sudah menerapkan asas universal.

Kata kunci: tindak pidana, teknologi informasi

PENDAHULUAN

A. LATAR BELAKANG MASALAH

Menurut Barda Nawawi Arief kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakekatnya, kebijakan kriminalisasi terhadap tindak pidana teknologi informasi merupakan bagian dari kebijakan kriminal *(criminal policy*) dengan menggunakan sarana hukum pidana *(penal),* dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" *(penal policy),* khususnya kebijakan formulasinya. Selanjutnya menurut Barda Nawawi Arief kebijakan kriminalisasi bukan sekedar kebijakan menetapkan/ merumuskan/ memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan formulasi/legislasi itu disusun dalam satu

[1] Artikel skripsi.
[2] NIM: 0707712074.

kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu.[3]

Kebijakan penanggulangan *cybercrime* secara teknologi, diungkapkan juga dalam IIIC *(Internatonal Information Industry Congress)* yang rnenyatakan :[4]

> *The IIIC recognizes that goverment action and international traties to harmonize laws and coordinate legal procedures are key in the fight against cybercrime, but warns that these should not be relied upon as the only instuments. Cybercrime is enabled by technology and requires* a *healty reliance on technology for* its *solution.*

Bertolak dari pengertian di atas maka upaya atau kebijakan untuk melakukan penanggulangan tindak pidana di bidang teknologi informasi yang dilakukan dengan menggunakan sarana *"penal"* (hukum pidana) maka dibutuhkan kajian terhadap materi/substansi *(legal subtance reform)* tindak pidana teknologi informasi saat ini. Dalam penanggulangan melalui hukum pidana *(penal policy)* perlu diperhatikan bagaimana memformulasikan (kebijakan legislatif) suatu peraturan perundang-undangan yang tepat untuk menanggulangi tindak pidana di bidang teknologi informasi pada masa yang akan datang, serta bagaimana mengaplikasikan kebijakan legislatif (kebijakan yudikatif/yudisial atau penegakan hukum pidana *in conereto)* tersebut oleh aparat penegak hukum atau pengadilan.

B. PERUMUSAN MASALAH

1. Bagaimana kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini ?
2. Bagaimana kebijakan aplikatif yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi ?
3. Bagaimana sebaiknya kebijakan formulasi dan kebijakan aplikatif hukum pidana dalam penanggulangan tindak pidana teknologi informasi di masa yang akan datang?

C. **METODE PENELITIAN**

Pendekatan hukum normatif dipergunakan dalam usaha menganalisis bahan hukum dengan mengacu kepada norma-norma hukum yang dituangkan dalam peraturan perundang-undangan dan putusan pengadilan.

TINJAUAN PUSTAKA

A. PENGERTIAN KEBIJAKAN HUKUM PIDANA

Pengertian kebijakan hukum dan hukum pidana di atas memberikan definisi kebijakan hukum pidana (*penal policy/criminal law policy/ strafrechts politiek*) sebagai, bagaimana mengusahakan atau membuatan merumuskan suatu perundang-undangan pidana yang baik.[5] Pengertian demikian terlihat pula dalam definisi "*penal policy*" yang dikemukakan oleh Marc Ance1,[6] bahwa *penal policy* adalah suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak hanya kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada para

[3] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana,* PT.Citra Aditya Bakti, Bandung, 2003, ha1.259.

[4] ITAC, "*IIIC Common Views Paper On: Cybercrime ", IIIC* 2000 Millenium Congress, September 19th, 2000, ha1.5. Lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* Kencana Prenada Media Group, Jakarta, 2007, ha1.240.

[5] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana,* PT.Citra Aditya Bakti, Bandung, 2003, ha1.25.

[6] Marc Ancel, *Social Defence, A Modern Approach to Criminal Problem* (London, Routledge & Kegan Pau1,1965,ha1.4-5), lihat dalam Barda Nawawi Arief, *Ibid.,*ha1.21.

penyelenggara atau pelaksana putusan pengadilan.

B. TEKNOLOGI INFORMASI DAN PERKEMBANGANNYA

Perkembangan teknologi informasi yang terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara *(borderless).* Negara yang sudah mempunyai infrastruktur jaringan informasi yang lebih memadai tentu telah menikmati hasil pengembangan teknologi informasinya, negara yang sedang berkembang dalam pengembangannya akan merasakan kecenderungan timbulnya neo-kolonialisme.[7] Hal tersebut menunjukan adanya pergeseran paradigma dimana jaringan informasi merupakan infrastruktur bagi perkembangan suatu negara.

Jaringan informasi melalui komputer *(interconnected computer networks)* dapat digolongkan dalam tiga istilah yaitu *ekstranet, intranet* dan *internet. Intranet* adalah *"a private network belonging to an organization, usually a corporation, accessible only by the organization's members, employes, or others with authorization* [8] dan *ekstranet* adalah "*a fancy way of saying that a corporation has opened up portions of its intranet to authorized users outside the corporation.*[9]

PEMBAHASAN

A. ASPEK-ASPEK YANG BERHUBUNGAN DENGAN TINDAK PIDANA TEKNOLOGI INFORMASI

1. Aspek Perundang-undangan yang Berhubungan dengan Tindak Pidana Teknologi Informasi

Saat ini Indonesia telah memiliki *cyber law* untuk mengatur dunia maya berikut sanksi bila terkaji *cybercrime* baik di wilayah Indonesia maupun di luar wilayah hukum Indonesia yang akibatnya dirasakan di Indonesia. *Cybercrime* terus berkembang seiring dengan revolusi teknologi informasi yang membalikkan paradigma lama terhadap kejahatan konvensional ke arah kejahatan virtual dengan memanfaatkan instrumen elektronik tetapi akibatnya dapat dirasakan secara nyata.

Penanggulangan *cybercrime* oleh aparat penegak hukum sangat dipengaruhi oleh adanya peraturan perundang-undangan.Terdapat beberapa perundang-undangan yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan Internet sebelum disahkannya UU ITE.

Penegakkan hukum *cybercrime* sebagaimana telah dilakukan Mabes Polri pada tahun 2007 di atas dilakukan dengan menafsirkan *cybercrime* ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi seperti:

1. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
2. Undang-Undang No.19 tahun 2002 tentang Hak cipta.
3. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang.
4. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme.

2. Aspek Aparatur Penegak Hukum

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrime.* Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet), di samping itu aparat penegak hukum di daerah pun belum siap dalam

---

[7] Lihat di www.ristek.go.id, Perlunya Studi Perbandingan dalam Pengembangan Teknologi Informasi di Indonesia.2001di akses pada tangga1 29 Agustus 2008.

[8] Lihat di http://netforbeginners.mining;s.com diakses pada tangga130 Agustus 2008.

[9] *Ibid*

mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi "gaptek" hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan Internet.

Berdasarkan data Polri, kasus kejahatan dunia maya yang terjadi selama kurun waktu 4 (empat) tahun dari tahun 2002 sampai dengan tahun 2005 terdapat 48 (empat puluh delapan) kasus. Dari 48 (empat puluh delapan) kasus yang dilaporkan tersebut, 25 (dua puluh lima) kasus telah dinyatakan P-21 oleh Jaksa Penuntut Umum.[10]

3. Sarana dan Fasilitas dalam Penanggulangan *Cybercrime*

Tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan trampil, organism' yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Kalau hal-hal itu tidak terpenuhi, maka mustahil penegakan hukum akan mencapai tujuannya.

4. Kesadaran Hukum Masyarakat

Dalam konsep keamanan masyarakat modern, sistem keamanan bukan lagi tanggung jawab penegak hukum semata, namun menjadi tanggung jawab bersama seluruh elemen masyarakat. Dalam pandangan konsep in masyarakat di samping sebagai objek juga sebagai subjek. Sebagai subjek, masyarakat adalah pelaku aktivitas komunikasi antara yang satu dengan yang lain, serta pengguna jasa kegiatan internet dan media lainnya. Sebagai objek, masyarakat dijadikan sasaran dan korban kejahatan bagi segenap aktivitas kriminalisasi Internet.

B. PEMBUKTIAN DALAM PENEGAKAN HUKUM TINDAK PIDANA TEKNOLOGI INFORMASI

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

Menurut M.Yahya Harahap, pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-carayang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa.[11] Menurut Pitlo, "pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya".[12] Menurut Subekti, yang dimaksudkan dengan "membuktikan" adalah meyakinkan hakim tentang kebenaran dalil ataupun dalil-dalil yang dikemukakan oleh para pihak dalam suatu persengketaan.[13] "Pembuktian tentang

[10] Petrus Reinhard Golose, *Penegakan Hukum Cybercrime dalam Sistem Hukum Indonesia* dalam *Handout* Seminar Nasional tentang "Penanganan Masalah *Cybercrime* di Indonesia dan Pengembangan Kebijakan Nasional Yang Menyeluruh Terpadu, diselenggarakan oleh Deplu, BI, dan Depkominfo, Jakarta, 10 Agustus 2006, hal.6

[11] M.Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan , Banding, Kasasi, dan Peninjauan Kembali* Edisi Kedua, Sinar Grafika, Bandung, 2000, hal.273.

[12] Edmon Makaritn, *Kompilasi Hukum Telematika,* Rajagrafindo Persada, Jakarta, 2003,hal. 417.

[13] Subekti, *Hukum Pembuktian,* Pradnya Paramita, Jakarta, 1995, hal. 1.

benar tidaknya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting dalam hukum acara pidana".[14]

Dalam hukum pembuktian dikenal istilah *notoire feiten notorious (generally known)* yang berarti setiap hal yang "sudah umum diketahui" tidak lagi perlu dibuktikan dalam pemeriksaan sidang pengadilan".[15] Hal ini tercantum dalam Pasal 184 ayat (2) KUHAP yang berbunyi, "hal yang secara umum diketahui tidak perlu dibuktikan. "Menurut Yahya Harahap, mengenai pengertian "hal yang secara umum sudah diketahui" ditinjau dari segi hukum, tiada lain daripada "perihal" atau "keadaan tertentu" atau *omstandigheiden* atau *circumstances,* yang sudah sedemikian mestinya atau kesitnpulan atau resultan yang menimbulkan akibat yang pasti demikian".[16]

Berkaitan dengan membuktikan sebagaimana diuraikan di atas, dalam hukum acara pidana (KUHAP) secara tegas disebutkan beberapa alat-alat bukti yang dapat diajukan oleh para pihak yang berperkara di muka persidangan. Berdasarkan Pasal 184 KUHAP,[17] alat-alat bukti ialah: Keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Dalam perkembangannya, keberadaan informasi dan data elektronik diakui sebagai "alat bukti lain" selain yang diatur dalam Pasal 184 KUHAP, Pasal 164 *Herzien Inlancls Reglements* (HIR) dart 1903 Kitab Undang-Undang Hukum Perdata (bukti tulisan, bukti dengan saksi, persangkaan-persangkaan, pengakuan dan sumpah).

1. Alat Bukti Informasi dan Data Elektronik

Undang-Undang No.8 Tahun 1997 Tentang Dokumen Perusahaan telah mulai mengatur ke arah pembuktian data elektronik.[18] Melalui undang-undang ini pemerintah berusaha mengatur pengakuan atas *microfilm* dan media lainnya seperti alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan, misalnya *Compact Disk-Read Only Memory* (CD-ROM) dan *Write-One-Read-Many* (WORM) sebagai alat bukti yang sah, diatur dalam Pasal 12 Undang-Undang Dokumen Perusahaan.

Pengaturan informasi dan data elektronik tercantum di dalam beberapa undang-undang khusus yang lain yaitu Pasal 38 UU No. 15/2002 tentang Tindak Pidana Pencucian Uang, Pasal 27 UU No. 16/2003 jo UU No. 15/2003 tentang Pemberantasan Tindak Pidana Terorisme, dan Pasal 26 (a) UU No. 20/2001 tentang Perubahan atas UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi. Pengaturan terhadap alat bukti dalam perundang-undangan di Indonesia dapat dilihat dalam tabel di bawah

Tabel.3 Mat Bukti Informasi dan Data Elektronik dalam Undang-Undang

No	Undang-Undang	Pasal	Keterangan
1	UU No.8 tahun 1997 ttg Dokumen Perusahaan	Pasa11 2	Pengakuan atas Mikrofilm dan media penyimpan yang lain seperti *Compact Disk-Read Only Memory* (CD-
2	UU No 20/2001 Tentang Perubahan atas UU No. 31/ 1999 ttg Pembera Tindak Pidana Korupsi	Pasal 26 huruf (a)	Pengakuan bukti petunjuk sebagai alat bukti yang sah. Bukti petunjuk juga dapat diperoleh dari alat bukti lain yang berupa informasi

[14] Andi Hamzah, *Hukum Acara Pidana Indonesia,* Sinar Graftka, Jakarta, 2005, hal. 245.

[15] M.Yahya Harahap, "Pembahasan Permasalahan….", *Op. Cit*.,hal.276

[16] *Ibid.* ,hal.276.

[17] *Ibid,* hal.107.

[18] Isis Ikhwansyah*,* Prinsip-Prinsip Universal Bagi Kontak Melalui E-Commerce dan Sistem Hukum Pembuktian Perdata dalam Teknologi Informasi, dalam *Cyberlaw: Suatu Pengantar*, ELIPS, Bandung, 2002, hal.36.

3	UU No. 1 tentang Pidana Pe Uang	Pasal 38 (huruf b)	alat bukti elektronik atau *digital evidence* adalah alat bukti lain berupa informasi yang diucapkan,
4	UU No. 16/2003 jo UU No. 15/2003 ttg Pemberantasan Tindak Terorisme,	Pasal 27 huruf (b) dan (c)	Alat bukti berupa informasi yang disimpan secara elektronik dengan alat optik. Data,
5	UU No.11 tahun 20	Pasal 5	Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum sah. Serta merupakan

Dalam UU No. 15/2002 tentang Tindak Pidana Pencucian Uang, Pasal 27 UU No. 16/2003 jo UU No. 15/2003 tentang Pemberantasan Tindak Pidana Terorisme, dan Pasal 26 (a) UU No. 20/2001 tentang Perubahan atas UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi menyatakan informasi dan bukti elektronik dikatakan sebagai alat bukti baru yang merupakan pelengkap dari alat-alat bukti yang telah dikenal dalam Pasal 184 KUHAP.

Penerapan alat bujkti informasi dan data elektronik dalam perundang-undangan sering mengakibatkan multitatsir diantara aparat penegak hukum terutama path saat pemeriksaan pengadilan. Hal tersebut dikarenakan belum adanya rambu yang jelas terhadap pengakuan alat bukti tersebut.

Konsep Rancangan Undang-Undang KUHP 2000, di mana konsep ini mengalami perubahan sampai dengan 2008 telah mengatur alat bukti elektronik yaitu:[19] Dalam Buku I (Ketentuan Umum) Dibuat Ketentuan mengenai alat bukti:

1. Pengertian "barang" (Pasal 174/178) yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon atau telekomunikasi atau jasa komputer.
2. Pengertian "anak kunci" (Pasal 178/182) yang di dalamnya termasuk kode rahasia, kunci masuk komputer, kartu *magnetic,* silly & yang telah deprogram untuk membuka sesuatu. Menurut Agus Raharjo,[20] maksud dari anak kunci ini kemungkinannya adalah *password* atau kode-kode tertentu seperti privat atau *public key infrastructure.*
3. Pengertian "surat" (Pasal 188/192) termasuk data tertulis atau tersimpan dalam disket, pita *magnetic,* media penyimpanan komputer atau penyimpanan data elektronik lainnya.
4. Pengertian "ruang" (Pasal 189/193) termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu. Maksud dari ruang ini kemungkinan termasuk pula dunia maya atau maya atau antara *cyberspace* atau *virtual reality.*
5. Pengertian "masuk" (Pasal 190/194) termasuk mengakses komputer atau masuk ke dalam sistem komputer. Pengertian masuk menurut Agus Raharjo di sini adalah masuk ke dalam sistem jaringan informasi global yang disebut internet dan kemudian baru masuk ke sebuah situs atau *website* yang di dalamnya berupa *server* dan komputer yang termasuk dalam pengelolaan situs. Jadi ada 2 pengertian masuk, yaitu masuk ke internet dan masuk ke situs.
6. Pengertian jaringan telepon" (Pasal 191/195) termasuk jaringan

[19] Barda Nawawi Arief, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan,* PT. Citra Aditya Bakti, Bandung, 2005, hal.131-133.

[20] Agus Raharjo, *CyberCrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* PTCitra Aditya Bakti, Bandung, 2002, hal. 236

komputer atau sistem komunikasi komputer.

Dengan meningkatnya aktivitas elektronik, maka alat pembuktian yang dapat digunakan secara hukum harus juga meliputi informasi atau dokumen elektronik untuk memudahkan pelaksanaan hukumnya. Selain itu hasil cetak dari dokumen atau Informasi tersebut juga harus dapat dijadikan bukti yang sah secara hukum. Untuk memudahkan pelaksanaan penggunaan bukti elektronik (baik dalam bentuk elektronik atau hasil cetak), maka bukti elektronik dapat disebut sebagai perluasan alat bukti yang sah, sesuai dengan hukum acara yang berlaku di Indonesia, sebagaimana tertulis dalam Pasal 5 UU ITE:

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.[21]

Namun bukti elektronik tidak dapat digunakan dalam hal-hal spesifik sebagaimana yang tertulis dalam Pasal 5 ayat (4) UU ITE menyatakan Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

a. surat yang menurut Undang-Undang harus dibuat &lam 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.[22]

Surat yang menurut undang-undang harus dibuat tertulis seperti dalam pembuatan dan pelaksanaan surat-surat terjadinya perkawinan dan putusnya perkawinan, surat-surat yang menurut undang-undang harus dibuat dalam bentuk tertulis, perjanjian yang berkaitan dengan transaksi barang tidak bergerak, dokumen yang berkaitan dengan hak kepemilikan dan juga dokumen lainnya yang menurut peraturan perundang-undangan mengharuskan adanya pengesahan notaris atau pejabat yang berwenang.

Bukti elektronik baru dapat dinyatakan sah apabila menggunakan sistem elektronik yang sesuai dengan peraturan yang berlaku di Indonesia. Suatu bukti elektronik dapat memiliki kekuatan hukum apabila informasinya dapat dijamin keutuhannya, dapat dipertanggungjawablcan, dapat diakses dan dapat ditampilkan, sehingga menerangkan suatu keadaan orang yang mengajukan suatu bukti elektronik harus dapat menunjukkan bahwa informasi yang dimilikinya berasal dari sistem elektronik yang terpercaya.

Berdasarkan Pasal 5 ayat (1) UU ITE, informasi elektronik memiliki kekuatan hukum sebagai alat bukti yang sah, bila informasi elektronik ini dibuat dengan menggunakan sistem elektronik yang dapat dipertanggungjawabkan sesuai dengan perkembangan teknologi informasi. Bahkan secara tegas, Pasal 6 UU ITE menentukan bahwa "Terhadap semua ketentuan hukum

[21] Pasal 5 ayat (1),(2) dan (3) Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[22] Pasal 5 ayat (4) Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli selain yang diatur dalam Pasal 5 ayat (4), persyaratan tersebut telah terpenuhi berdasarkan undang-undang ini jika informasi elektronik tersebut terjamin keutuhannya dan dapat dipertanggungjawabkan, dapat diakses, dapat ditampilkan sehingga menerangkan suatu keadaan".

Penegasan terhadap informasi elektronik dan dokumen elektronik dapat dijadikan menjadi alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan tertulis di dalam Pasal 44 UU ITE yang isinya sebagai berikut :[23]

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).

Sesungguhnya pandangan yang mengatakan alat bukti elektronik tidak dapat menjadi alat bukti tertulis tidaklah mutlak, karena sangat tidak relevan di jaman teknologi tetap memandang alat bukti tertulis hanya yang berbentuk konvensional. Disinilah Hakim dituntut untuk berani melakukan tembosan hukum karena dia yang paling berkuasa dalam memutuskan suatu perkara dan karena dia juga yang dapat memberi suatu *vonnis van de rechter* (keputusan hakim) yang tidak langsung dapat didasarkan atas suatu peraturan hukum tertulis atau tidak tertulis. Dalam hal ini, Hakim harus membuat suatu peraturan sendiri *(eigen regeling).*[24] Tindakan seperti ini, menurut Pasal 14 Undang-Undang Nomor 14 Tahun 1970 tentang kekuasaan kehakiman, dibenarkan karena seorang Hakim tidak boleh menolak untuk memeriksa, mengadili dan memutuskan suatu perkara dengan alasan peraturan perundang-undangan yang tidak menyebutkan, tidak jelas, atau tidak lengkap (asas *ius curia novit).* Bila keputusan Hakim yang memuat *eigen regeling* ini dianggap tepat dan dipakai berulang-ulang oleh Hakim-hakim lainnya, maka keputusan ini akan menjadi sebuah sumber hukum bagi peradilan *(rechtspraak).*[25]

Dengan dasar-dasar di atas, seorang Hakim diberikan keleluasan untuk menemukan hukum *(eeditsvinding),* baik dengan cara Melakukan interpretasi hukum *(wetinteepeetatie),* maupun dengan menggali, mengikuti dan memahami nilai-nilai hukum yang hidup dalam masyarakat. Metoda interpretasi yang dapat digunakan claim pencarian kekuatan hukum dari akta elektronik dan tanda tangan elektronik khususnya adalah interpretasi analogi, interpretasi ekstensif dan interpretasi sosiologis.[26]

Metoda interpretasi analogis dilakukan dengan memberi ibarat terhadap suatu kata-kata sesuai dengan asas hukumnya, sehingga suatu peristiwa yang pada awalnya tidak dapat dimaksudkan, lalu dianggap sesuai dengan ketentuan peraturan tersebut, misalnya menyambung aliran listrik dianggap mencuri/mengambil aliran listrik sebagaimana yang ditegaskan dalam yurisprudensi tetap *Hoge Raad der Nederlanden* (pengadilan tertinggi di Belanda). Berdasarkan asas konkordansi, pengadilan Indonesia menggunakan yurisprudensi ini untuk menjawab

[23] Pasal 44 ayat (4) Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[24] E. Utrecht dan Moh. Saleh Djindang, *Pengantar Dalam Hukum Indonesia,* cetakan kesebelas, penerbit P.T. Ichtiar Baru dan Penerbit Sinar Harapan, Jakarta, 1989, hal.121.

[25] *Ibid*.

[26] *Ibid,* hal.203.

kebingungan Hakim dalam menyelesaikan kasus penyalahgunaan/ pencurian listrik.[27]

Di Indonesia sendiri terdapat putusan pengadilan yaitu putusan MARI.Nomor.9/KN/1999, yang dalam putusannya hakim meneritna hasil *print Out* sebagai alat bukti surat. Kemudian kasus pidana yang diputus di Pengadilan Negeri Jakarta Timur mengetengahkan bukti *e-mail (electronic mail)* sebagai salah satu alat bukti. Setelah mendengar keterangan ahli bahwa dalam transfer data melalui *e-mail* tersebut tidak terjadi tindakan manipulatif, hakim memvonis terdakwa dengan hukuman satu tahun penjara karena terbukti telah melakukan tindakan cabul berupa penyebaran tulisan dan gambar.[28]

2. Tanda Tangan Elektronik

Salah satu alat yang dapat digunakan untuk menentukan keaslian atau keabsahan suatu bukti elektronik adalah tanda tangan elektronik. Tanda tangan elektronik harus dapat diakui seem hukum karena penggunaan tanda tangan elektronik lebih cocok untuk suatu dokumen elektronik.

Agar suatu tanda tangan elektronik dapat diakui kekuatan hukumnya, maka syarat-syarat yang harus dipenuhi sesuai Pasal 11 ayat (1) UU 11 E adalah:[29]

a. Data pembuatan tanda tangan elektronik hanya terkait kepada penanda tangan saja;
b. Data pembuatan tanda tangan elektronik hanya berada dalam kuasa penandatangan pada saat penandatanganan;
c. Perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
d. Perubahan terhadap informasi elektronik yang berhubungan dengan tanda tangan elektronik dapat diketahui setelah waktu penandatanganan;
e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangannya;
f. Terdapat cara tertentu untuk menunjukkan bahwa penandatangan telah memberikan persetujuan terhadap informasi elektronik yang ditandatangani.

Orang yang menggunakan tanda tangan elektronik atau terlibat dalamnya mempunyai kewajiban untuk mengamankan tanda tangan agar tanda tersebut tidak dapat dapat disalahgunakan oleh orang yang tidak berhak. Pengamanan tanda tangan elektronik sesuai Pasal 12 (2) UU ITE meliputi syarat :[30]

a. Sistem tidak dapat diakses oleh orang lain yang tidak berhak;
b. Penandatangan harus waspada terhadap penggunaan tidak sah dari data pembuatan tanda tangan oleh orang lain;
c. Penandatangan harus menggunakan cara atau instruksi yang dianjurkan oleh penyelenggara tanda tangan elektronik. Penandatangan harus memberitahukan kepada orang yang mempercayai tanda tangan tersebut atau kepada pihak pendukung layanan tanda tangan elektronik apabila ia percaya bahwa:
   1. Data pembuatan tanda tangan telah dibobol; atau
   2. Tanda tangan dapat menitnbulkan risiko, sehingga ada

[27] *Ibid,* ,hal.127.

[28] Di akses dari http://www.hukumonline.comiartikel_detail dengan judul "Data Elektronik sebagai Alat Bukti Masih Dipertanyakan" pada tanggal 30 Agustus 2008.

[29] Pasal 11 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[30] Pasal 12 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58 .

kemungkinan bobolnya data pembuatan tanda tangan elektronik tersebut.

d. Dalam hal sertifikat Elektronik digunakan untuk mendukung tanda tangan elektronik, penanda tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan sertifikat elektronik tersebut.

Menurut Penulis, penggunaan kata "data pembuatan tanda tangan elektronik" hendaklah disederhanakan menjadi "tanda tangan elektronik", agar lebih jelas dan mudah dimengerti karena tidak ada tanda tangan elektronik tanpa data. Tanda tangan elektronik yang diatur di Peraturan Pemerintah sesuai dengan wewenang yang akan diberikan Pasal 11 ayat (2) UU ITE harus memberikan perbedaan antara tanda tangan elektronik *simple* (sederhana) dan tanda tangan elektronik *securisee* (diamankan/terkualifikasi).[31]

Ketentuan-ketentuan Pasal 11 merupakan syarat-syarat minimal (yang harus diintegrasikan dengan pasal 12) untuk dipenuhi agar sebuah tanda tangan elektronik menikmati "asas praduga kehandalan" *(presomption de fiabilite)* yang memberikan kekuatan hukum dan akibat hukum yang sama dengan tanda tangan manuskrip. Tanda tangan elektronik *securisee* (diamankan/terkualifikasi) seharusnya yang diatur dalam Peraturan Pemerintah nantinya dan berhak untuk menikmati *presomption de fiabilite.* Kecuali dibuktikan lain, keuntungan dari asas ini adalah jaminan praduga kehandalan identitas dari pengguna dan integritasnya dengan akta yang dilekatinya. Ketidakmampuan pengguna untuk menikmati asas ini, menciptakan kesulitan kepada mereka dalam membuktikan kehandalan prosedur yang digunakannya. Dari sudut kekuatan hukum dan akibat hukum, jelaslah tipe *securisie* yang akan mendapatkan nilai pembuktian lebih unggul daripada tanda tangan elektronik sederhana.

Selain itu, menurut Penulis, butir (f) pada Pasal 11 ayat (1) sebaiknya dihapus karena dari sudut pandang teknis, butir (e) sudah cukup untuk membuktikan bahwa Penandatangan telah memberikan persetujuamiya dengan menandatangani akta elektronik tersebut dengan tanda tangan elektronik miliknya. Munn, tintuk membuktikan apakah persetjjuan Penandatangan tersebut datang tanpa unsur paksaan, digunakanlah fakta-fakta hukum dalam proses peradilanlah, bukan piranti lunak yang digunakan.

Berkaitan dengan pembuktian R. Subekti. mengatakan bahwa, "beban pembuktian harus dilakukan dengan adil dan tidak berat sebelah, karena suatu pembagian beban pembuktian yang berat sebelah berarti *a priori* menjerumuskan pihak yang mendapat beban terlalu berat kedalam jurang kekalahan".[32] Berkaitan dengan beban pembuktian terhadap tanda tangan elektronik, hendaknya dibebankan kepada pihak yang mempunyai alat-alat yang memadai untuk membuktikan bahwa tanda tangan elektronik tersebut dibuat dengan prosedur yang handal daft dapat dipertanggungjawabkan.

Sistem beban pembuktian terhadap tanda tangan elektronik hendaknya diserahkan kepada penyelenggara sertifikasi tanda tangan elektronik. Dengan demikian, kesulitan hakim dalam hal membuktikan unsur-unsur tersebut terutama dengan menggunakan alat bukti elektronik dapat diringankan oleh saksi ahli karena penyelenggara sertifikasi tanda tangan elektroniklah yang mempunyai kemampuan teknis dan peralatan teknik

[31] Julius Singara, *Alemoire : la cryptologie et la preuve electronique de la France a l'Indonesie,* D.E.A. *Informatique et Droit, Universite Montpellier I, armee universitaire,* Montpellier, 2003-2004, hal.80

[32] R. Soesilo , *RIB/HIR Dengan Penjelasan,* Politeia, Bogor, 1995, hal. 113.

untuk membuktikan kehandalan dan keamanan prosedur yang mereka gunakan.

Pengaturan data elektronik sebagai alat bukti walau bagaimanapun telah melakukan pembaharuan mengenai substansi hukum, yang ada dalam hukum acara pidana (KUHAP) Indonesia, HIR dan KU!-! Perdata. Tetapi perluasan alat bukti tersebut akan terasa sia-sia jika aparat penegak hukumnya belum siap atau belum mampu untuk itu dibutuhkan pengetahuan dari kemampuan aparat penegak hukum dalam teknologi informasi serta keyakinan dan pandangan yang luas hakim dalam menafsirkan hukum sebagai upaya penegakan hukum dunia mayantara di Indonesia.

C. YURISDIKSI HUKUM PIDANA DALAM PENANGGULANGAN *CYBERCRIME*

Pengaturan teknologi informasi yang diterapkan oleh suatu negara berlaku untuk setiap orang yang melakukan perbuatannya baik yang berada di wilayah negara tersebut maupun di luar negara apabila perbuatan tersebut memiliki akibat di Indonesia. Butuhnya pengaturan yurisdiksi ekstrateritorial dikarenakan suatu tindakan yang merugikan kepentingan orang atau negara dapat dilakukan di wilayah negara lain. Oleh karena itu, peraturan mengenai *cyberlaw* harus dapat mencakup perbuatan yang dilakukan di luar wilayah Indonesia tapi merugikan kepentingan orang atau negara dalam wilayah Indonesia.

Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 11E) telah mengatur masalah yurisdiksi yang di dalamnya sudah menerapkan asas universal. Hal ini dapat dilihat dari Pasal 2 UU ITE:

> Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.[33]

Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal. Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada menigikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.[34]

Perluasan pengaturan yurisdiksi ekstrateritorial dalam tindak pidana teknologi informasi dimaksudkan untuk melindungi jaringan komunikasi/informasi yang saat ini telah menjadi kepentingan intemasional/global. Pengaturan yurisdiksi ekstrateritorial sama dengan prinsip atau azas *ubikuitas* sehingga sangat beralasan dalam menghadapi tindak pidana mayantara. Sebagaimana ditulis oleh Barda

[33] Pasal 2 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[34] Penjelasan Pasal 2 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

Nawawi Arief,[35] mengusulkan untuk memberlakukan prinsip *ubikuitas (the principle of ubiquity)* atas tindak pidana mayantara. Alasannya saat ini semakin marak terjadi *cybercrime* seiring dengan pertumbuhan penggunaan internet. Yang dimaksud dengan prinsip atau azas *ubikuitas* adalah prinsip yang mengatakan bahwa delik-delik yang dilakukan atau terjadi di sebagian wilayah teritorial negara sebagian di luar wilayah teritorial suatu negara (ekstrateritorial) harus dapat dibawa ke dalam yurisdikgi setiap negara yang terkait.

Berdasarkan Pasal 2 dan penjelasan UUITE path dasarnya tetap dianut asas-asas ruang berlakunya hukum pidana dalam KUHP yaitu didasarkan path asas teritorial (pasal 2-5 KUHP), asas personal/nasional aktif (pasal 7 KUHP), dan asas universal (pasal 8 KUHP), hanya ada perubahan dan perkembangan formulasinya yaitu:

- Memuat ketentuan tentang lingkup yurisdiksi yang bersifat transnasional dan internasional serta memuat ketentuan khusus terhadap tindak pidana teknologi informasi.
- Subjek hukum tidak hanya terhadap perorangan baik warga negara Indonesia ataupun warga negara asing yang memiliki akibat hukum di Indonesia tetapi juga 'terhadap badan hukum asing (koorporasi)

Berlakunya asas-asas ruang hukum pidana dalam KUHP sebenarnya tidak perlu lagi diatur di dalam UU ITE, maka lebih aman dan lebih luas jangkauannya apabila UU ITE menegaskan berlakunya asas-asas ruang berlakunya hukum pidana menurut KUHP dengan menambah/memperluas hal-hal yang belum ditegaskan dalam KUHP.

Problema dalam penerapan pengaturan yurisdiksi ekstrateritorial adalah dalam hal penegakan hukumnya. Beberapa komplain sering dilakukan oleh beberapa kedutaan besar, yang disalurkan nielalui interpol ke Mabes Polri atau yang disalurkan ke Kepolisian Daerah mengalami jalan buntu. Hal tersebut dapat terlihat dari data korespondensi kasus *cybercrime* Interpol Indonesia dari tahun 2006 sampai dengan tahun 2008 di bawah ini :

Tabel.7
Data Korespondensi Kasus *Cybercrime* Interpol 2006-2008[36]

NO	TAHUN	JUMLAH KASUS	HASIL PENYELIDKAN	
			Selesai	Proses Penyidikan
1	2006	28	7	21
2	2007	31	-	31
3	2008	38	-	38
TOTAL			7	90

Penyelidikan dan penyidikan atas komplain yang tidak tuntas tersebut dikarenakan berbagai faktor seperti faktor keterbatasan sumber daya manusia yang dimiliki aparat penegak hukum, faktor biaya, sarana atau fasilitas, sulitnya menghadirkan korban juga dikarenakan faktor prinsip kedaulatan wilayah dan kedaulatan hukum masing-masing Negara. Menurut Masaki Hamano sebagaimana dikutip oleh Barda Nawawi Arief Ada tiga lingkup yurisdiksi di ruang maya *(cyberspace),* yang dimiliki suatu negara berkenaan dengan penetapan dan pelaksariaan pengawasan terhadap setiap peristiwa, setiap orang dan setiap benda. Ketiga katagori yurisdiksi tersebut, yaitu:[37]

[35] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana,* PT. Citra Aditya Bakti, Bandung, 2003, hal.253.

[36] Sumber dari situs Interpol Indonesia http://vvvvw.interpol.go.id di akses pada tanggal 28 September 2008.

[37] Masaki Hamano,"Comparative Study in the Approach to Jurisdiction in Cyberspace" Chapter: The Principle of Jurisdiction,,hal.l. lihat dalam Barda Nawawi Arief, *Tindak Pidana Mayantara*, Raja Grafindo Persada, Jakarta, 2006.,ha1.27-28.

1. Yurisdiksi Legislatif *(legislatif jurisdiction atau jurisdiction to prescribe);*
2. Yurisdiksi Yudisial *(judicial jurisdiction atau jurisdiction to adjudicate*); dan
3. Yurisdiksi Eksekutif *(executive jurisdiction* atau *jurisdiction to enforce).*

Berdasarkan ketiga katagori yurisdiksi menurut Masakl Hamano di atas perbuatan yang dapat menimbulkan masalah dalarn UU ITE ketika warga negara Indonesia melakukan tindak pidana di luar Indonesia (asas persona/nasionalitas aktif) tanpa akibatnya dirasakan di Indonesia. Hal tersebut sangat terkait dengan masalah yurisdiksi judisial (kewenangan mengadili atau menerapkan hukum) dan yuriisdiksi eksekutif (kewenangan melaksanakan putusan) karena masalah yurisdiksi judisial/adjudikasi dan yurisdiksi eksekutif sangat terkait dengan kedaulatan wilayah dan kedaulatan hukum masing-masing Negara, karena konstitusi suatu negara tidak dapat dipaksakan kepada negara lain karena dapat bertentangan dengan kedaulatan dan konstitusi negara lain, oleh karena itu hanya berlaku di negara yang bersangkutan saja, sehingga dibutuhkan kesepakatan Internasional dan kerjasama dengan negara-negara lain dalam menanggulangi tindak pidana teknologi informasi.

PENUTUP

A. KESIMPULAN

1. Dalam menjamin keamanan, keadilan dan kepastian hukum dalam penegakan hukum *(law enforcement)* di dunia *cyber* dapat terlaksana dengan baik maka harus dipenuhi 4 (empat) syarat yaitu: (1) Adanya aturan perundang-undangan khusus yang mengatur dunia *cyber.* (2) Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus menangani *cybercrime* . (3) Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu. (4) Kesadaran hukum dari masyarakat yang terkena peraturan. Selain ke 4 (empat) syarat tersebut penegakan hukum di dunia maya juga sangat tergantung dari pembuktian dan yuridiksi yang ditentukan oleh undang-undang.
2. Kebijakan pemerintah Indonesia dengan diundangkannya Undang-Undang No. 11 tahun 2008 tentarig Informasi dan Trarisaksi Elektroriik (UU ITE) merupakan payung hukum pertama yang mengatur dunia siber *(cyberlaw),* sebab muatan dan cakupannya yang luas dalam membahas pengaturan di dunia maya seperti perluasan alat bukti elektronik sama dengan alat bukti yang sudah dikenal selama ini, diakuinya tanda tangan elektronik sebagai alat verifikasi, dan autentikasi yang sah suatu dokumen elektronik, serta pengaturan perbuatan-perbuatan yang dilakukan dalam *cyberspace* sebagai suatu tindak pidana.
3. Peraturan mengenai *cyberlaw* harus dapat mencakup perbuatan yang dilakukan di luar wilayah Indonesia tapi merugikan kepentingan orang atau negara dalam wilayah Indonesia. Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur masalah yurisdiksi yang di dalamnya sudah menerapkan asas universal.

B. SARAN

1. Diaturnya alat pembuktian inforinasi, dokumen elektronik dan tanda tangan. elektronik yang dapat digunakan secara hukum diharapkan dapat memudahkan pelaksanaan penegakan hukum terhadap tindak pidana

teknologi informasi di Indonesia, tetapi hal tersebut haras didukung dengan pengetahuan dan keterampilan, serta kerja sama antara aparat penegak hukum balk lingkup regional maupun internasional mengingat tindak pidana *cybercrime* yang *borderless.*

2. Yurisdiksi *cyberspace* sangat berpengaruh dalam penegakan hukummengingat jarak, biaya dan kedaulatan masing-masing negara. Oleh karena itu dibutuhkan kerjasama Internasional baik *mutual assistance,* perjanjian ekstradisi dan kesepakatan atau kerjasama dengan negara-negara lain terkait kejahatan *cybercrime* dalam upaya penegakan hukum dalam menanggulangi tindak pidana teknologi informasi.

DAFTAR PUSTAKA

Abdul Mu'in M., Teknologi Informasi Dalam Sistem Jaringan Perpustakaan Perguruan Tinggi. www.yahoo.com. Diakses pada tanggal 1 September 2008.

Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime),* Refika Aditama, Bandung, 2005.

Abadinsky, Howard., *Prohobition and Parole : Theory and Practice*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1977.

Agus Raharjdo, *Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi, Op.Cit.*

Andi Hamzah, Aspek-Aspek Pidana di Bidang Komputer, 1998.

Anton M. Moelijono, (et.al)., *Kamus Besar Bahasa Indonesia*, Balai Pustaka, Jakarta,1998.

A. Mulder ,*"Strafrechtspolitiek" Delikt en Delinkwent* Mei 1980,ha1.333*,* lihat dalam Barda Nawawi Arief,

Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana,* PT.Citra Aditya Bakti, Bandung, 2003.

Caldwell, Kave. "*Applying Old Law to New Technology",* The Commercenet Newsletter The Public Policy Report. Vol. 2 No. 7 Agustus 2000.

Chandra, Fransisca Haryanti., *Internet* : *Information Superhighway*. Makalah pada Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi Melalui Media Komputer bagi Dosen PTS Kopertis Wilayah VI di Semarang, 4-8 September 1995.

Didik J.Rachbini, "*Mitos dan Implikasi Globalisasi " :* Catatan Untuk Bidang Ekonomi dan Keuangan, Pengantar edisi Indonesia dalam Hirst, Paul dan Grahame Thompson, *Globalisasi adalah Mitos*, Jakarta, Yayasan Obor, 2001.

Freddy Haris, *Cybercrime dari Persfektif Akademis,* Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia.

Hanny Kamarga, *Belajar Sejarah Melalui E-Learning : Alternatif Mengakses Sumber Informasi Kesejarahan,* PT Intimedia, Jakarta, 2002.

Hoefnagels, G. Peter., *The Other Side of Criminology, An Inversion of the Concept of Crime*, 972.

Horton, Paul B dan Chester L.Hunt, *Sosiologi*, Erlangga, Jakarta, 1984, ha1.237.

Ibrahim. Johannes., *Kartu Kredit Dilematis Antara Kontrak dan Kejahatan*. Bandung: Refika Aditama, 2004.

Jeff Zalesky, *Spritualitas Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia,* Mizan, Bandung, 1999.

Marc Ancel, *Social Defence, A Modern Approach to Criminal Problem* (London, Routledge & Kegan Pau1,1965,ha1.4-5).

Meliala. Adrianus., *Menyingkap Kejahatan Krah Putih*. Jakarta: Pustaka Sinar Harapan,1993.

M.Arief Mansur dan Alistaris Gultom, *CyberLaw; Aspek Hukum Teknologi Informasi, Op. Cit.*

Muladi, *Demokratisasi,HakAsasi Manusia dan Reformasi Hukum di Indonesia,* The Habibie Center, Jakarta, 2002, hal.269.

Moeljatno. *Perbuatan Pidana dan Pertanggungjawaban Dalam Hukum Pidana*. Yogyakarta: 1969.

Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantom Roes Setiyadi.

----------., *Asas-Asas Hukum Pidana*. Jakarta, Bina Aksara, 1983

Nitibaskara, Tubagus Ronny Rahman., *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi,*Peradaban, Jakarta, 2001.

Onno W Purbo, *Kebangkitan Nasional Ke-2 Berbasis Teknologi Informasi, Computer Network Research* Group, ITB,2007. Lihat dalam yclday@garuda.drn.go.id. Pada tanggal 5 Agustus 2008.

Pattiradjawane, Rene L., "*Globalisasi dan Teknologi Menuju Keseimbangan Baru,*" Harian *Kompas,* Tanggal 28 April 2000.

Pontier, J.A. (Penerjemah: B. Arief Sidharta). *Penemuan Hukum*. Bandung: Jendela Mas Pustaka, 2008.

Rahardjo. Agus., *Cybercrime. Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citta Aditya Bakti, 2002.

Reksodiputro, Mardjono., *Sistem Peradilan Pidana Indonesia (Melihat Pada Kejahatan dan Penegakan Hukum Dalam Batas-Batas Toleransi)*, Pidato Pengukuhan Jabatan Guru Besar dalam bidang Ilmu Hukum pada Fakultas Hukum Universitas Indonesia, Jakarta, 30

Romli Atmasasmita, *Ruang Lingkup Berlakunya Hukum Pidana terhadap Kejahatan Transnasional Terorganisasi,* artikel dalam Padjajaran Jilid XXIV No.2 tahun 1996.

Sahetapy, J.E., *Teori Kriminologi Suatu Pengantar*, Citra Aditya Bakti, Bandung, 1992.

----------., dan Mardjono Reksodiputro, *Paradoks Dalam Kriminologi*, Rajawali Press, Jakarta, 1989.

Sapardjaja. Komariah Emong., *Ajaran Sifat Melawan Hukum Materiel Dalam Hukum Pidana Indonesia*. Bandung: Alumni, 2002.

Silalahi, Darwin. "*Banyak Negara Bersiap dengan Ekononmi Berbasis Internet,*" Harian Kompas,. Tanggal 10 April 2000.

Soemadipradja. R Achmad S., *Hukum Pidana dalam Yurisprudensi*. Bandung: Armico, 1990.

Sudarto, *Hukum dan Hukum Pidana,* Alumni, Bandung, 1977, hal. 100.

Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, *Cybercrime-Motif* dan Penindakan, Pensil 324, Jakarta

Undang-Undang:

Undang-Undang Nomor I 1 Tahun 2008 Tentang Informasi dan Tmnsaksi Elektronik.

Undang-Undang Nomor 7 Tahun 1992 tentang Perbanbankan junto Undang-Undaag Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan

Lain-Lain:

Abidin M Asyek www.groups. google.mm/group/imssumatra

Majalah Warta Ekonomi No. 9, 5 Maret 2001

Majalah *CyberTECH* , dengan judul "Steven Haryanto" ,6 November 2002.

Majalah Gatra No.23 Tahun XIV17-23 April 2008.

www.bankgaransi blogspot.com. Modus Kejahatan Kartu ATM dan Kartu Kredit.

www.idsirtii.or.id. Mewaspadai Kejahatan Layanan Perbankan Elektronik. 2010