PEMBUKTIAN DALAM PENEGAKAN HUKUM TINDAK PIDANA TEKNOLOGI INFORMASI[1]

Oleh : F. Yerusalem R. Taidi[2]

ABSTRAK

Tujuan dilakukan penelitian ini adalah untuk mengetahui aspek-aspek apa yang berhubungan dengan tindak pidana teknologi informasi dan bagaimana pembuktian dalam penegakan hukum tindak pidana teknologi informasi. Metode penelitian dalam penulisan skripsi ini menggunakan metode penelitian juridis normatif dan dapat disimpulkan: 1. Dalam menjamin keamanan, keadilan dan kepastian hukum dalam penegakan hukum 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 tentang Informasi dan Transaksi 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. 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: Pembuktian, tehnologi informasi.

PENDAHULUAN

A. LATAR BELAKANG MASALAH

Sehubungan dengan tindak pidana di dunia maya yang terus berkembang, pemerintah telah melakukan kebijakan dengan terbitnya Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diundangkan pada tanggal 21 Apri 2008.[3] Undang-undang ITE merupakan payung hukum pertama yang mengatur khusus terhadap dunia maya *(cyber law)* di Indonesia.

Substansi/materi yang diatur dalam UU ITE ialah menyangkut masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara *e-comerce,* azas persaingan usaha-usaha tidak sehat dan perlindungan konsumen, azas-azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional serta azas *Cybercrime.* Undang-undang tersebut mengkaji *cyber case* dalam beberapa sudut pandang secara komprehensif dan spesifik, fokusnya adalah semua aktivitas yang dilakukan dalam *cyberspace* seperti perjudian, pornografi, pengancaman, penghinaan dan pencemaran nama baik melalui media *internet* serta akses komputer tanpa ijin

[1] Artikel Skripsi
[2] NIM 090711092
[3] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Diundangakan tanggal 28 April 2008, Lembaran Negara No.58.

oleh pihak lain *(cracking)* dan menjadikan seolah dokumen otentik *(phising) .*

Kebijakan penanggulangan *cybercrime* secara teknologi, diungkapkan 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. Aspek-Aspek apakah yang berhubungan dengan tindak pidana teknologi informasi ?
2. Bagaimanakah pembuktian dalam penegakan hukum tindak pidana teknologi informasi ?

C. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang merupakan salah satu jenis penelitian yang dikenal umum dalam kajian ilmu hukum. Pendekatan hukum normatif dipergunakan dalam usaha menganalisis bahan hukum dengan mengacu kepada norma-norma hukum yang dituangkan dalam peraturan perundang-undangan dan putusan pengadilan.

D. 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 terjadi *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. Penegakkan hukum *cybercrime* 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.

[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.

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 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.

Agar suatu perkara pidana dapat sampai pada tingkat penuntutan dan pemeriksaan di sidang pengadilan, maka sebelumnya harus melewati beberapa tindakan-tindakan pada tingkat penyidik. Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan, dalam Pasal 1 sub-13 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia penyelidikan didefinisikan sebagai:"

> "serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya".[5]

Penyidikan terhadap tindak pidana teknologi informasi sebagaimana dimaksud dalam UU ITE Pasal 42, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam UU ITE. Pasal 43 UU ITE menjabarkan bahwa selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintahan yang lingkup tugas dan tanggungjawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik.

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.

Untuk meningkatkan upaya penanggulangan kejahatan *cyber* yang semakin meningkat Polri dalam hal ini Bareskrim Mabes Polri telah berupaya melakukan sosialisasi mengenai kejahatan *cyber* dan cara penanganannya kepada satuan di kewilayahan (Polda). Sosialisasi tersebut dilalatkan dengan cara melakukan pelatihan (pendidikan kejuruan) dan peningkatan kemampuan penyidikan anggota Polri dengan mengirimkan personel-nya ke berbagai macam kursus yang berkaitan dengan *cybercrime.* Pelatihan, kursus dan ceramah kepada aparat penegak hukum lain (jaksa dan hakim) mengenai *cybercrirne* juga hendaknya dilaksanakan, dikarenakan jaksa dan hakim belum memiliki satuan unit khusus yang menangani kejahatan dunia maya sehingga diperlukan sosialisasi terutama setelah disyahkannya UU ITE agar memiliki kesamaan persepsi daft pengertian yang sama dalam melakukan penanganan terhadap kejahatan *cyber.*

[5] Pasal 1 Sub 13 Undang-Undang Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia.

Jaksa dan Hakim *cyber* sangat dibutuhkan seiring dengan perkembangan tindak pidana teknologi yang semakin banyak terjadi di masyarakat yang akibatnya dapat dirasakan di satu daerah, di luar daerah perbuatan yang dilakukan bahkan di luar negeri. Sarana atau fasilitas komputer hampir dimiliki oleh semua kesatuan aparat penegak hukum, namun masih sebatas untuk keperluan mengetik. Alat ini akan sangat membantu manakala dilengkapi dengan akses internet. Kurangnya sarana dan prasarana dalam penegakan hukum *cybercrime* sangat berpengaruh terhadap kinerja aparat penegak hukum dalam menghadapi *high-tech crimes.* Aparat penegak hukum perlu informasi yang dapat diakses melalui jaringan internet.

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.

Dilibatkannya masyarakat dalam strategi pencegahan kejahatan mempunyai 2 (dua) tujuan pokok, menurut Mohammad Kemal Dertuawan, adalah untuk:[6]

1. Mengeliminir faktor-faktor kriminogen yang ada dalam masyarakat.
2. Menggerakkan potensi masyarakat dalam hal mencegah dan mengurangi kejahatan.

Sampai saat ini, kesadaran hukum masyarakat untuk melakukan pengamanan dan merespon aktivitas *cybererime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahatan *cybercrime* yang menyebabkan upaya penanggulangan *cybercrime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cybercrime.*

Melalui pemahaman yang komprehensif mengenai *cybercrime,* peran masyarakat menjadi sangat penting dalam upaya pengawasan.

B. PEMBUKTIAN DALAM PENEGAKAN HUKUM TINDAK PIDANA TEKNOLOGI INFORMASI DAN YURISDIKSI HUKUM PIDANA DALAM PENANGGULANGANNYA

1. Pembuktian Dalam Penegakan Hukum Tindak Pidana Teknologi Informasi

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,[7] 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).

a. Alat Bukti Informasi dan Data Elektronik

Undang-Undang No.8 Tahun 1997 Tentang Dokumen Perusahaan telah mulai mengatur ke arah pembuktian data

[6] Mohammed Kemal Dermawan, *Strategi Pencegahan Kejahatan,* Citra Aditya Bhakti, Bandung 1994,hal.10.

[7] Ibid, ***hal.107.***

elektronik.[8] 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 1 Alat Bukti Informasi dan Data Elektronik dalam Undang-Undang

No	Undang-Undang	Pasal	Keterangan
1	UU No.8 tahun 1997 ttg Dokumen Perusahaan	Pasa112	Pengakuan atas Mikro film dan media penyimpan yang lain seperti *Compact Disk-Read Only Memory* (CD-ROM), dan *Write-Once-Read-Many* (WORM),
2	UU No. 20/2001 tentang Perubahan atas UU No. 31/1999 ttg Pemberantasan 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 yang diucapkan, dikirim, diterima, atau disimpan secara elektronik
3	UU No. 15/2002 tentang Tindak Pidana Pencucian Uang	Pasal 38 (huruf b)	alat bukti elektronik atau *digital evidence* adalah alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elelctronik dengan alat optik atau yang serupa dengan itu.
4	UU No. 16/2003 jo UU No. 15/2003 ttg Pemberantasan Tindak Pidana Terorisme,	Pasal 27 huruf (b) dan (c)	Alat bukti berupa informasi yang disimpan secara elektronik dengan alat optik. Data, rekaman atau informasi yang terekam secara elektronik
5	UU No.11 tahun 2008 ttg Informasi Dan Tran saksi Elektronik	Pasal 5	Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum sah. Serta merupakan perluasan dari alat yang bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Penerapan alat bukti 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.

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.[9]

[8] ***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.***

[9] 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.

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.[10]

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 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 :[11]

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).*[12] 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).*[13]

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

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

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

[12] 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.

[13] *Ibid*.

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.[14]

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 secara 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:[15]

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 :[16]

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 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

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

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

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

mudah dimengerti karena tidak ada tanda tangan elektronik tanpa data.

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.

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 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 KUH 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.

2. 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.[17]

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.[18]

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 melalui interpol ke Mabes Polri atau yang disalurkan ke Kepolisian Daerah mengalami jalan buntu.

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:[19]

1. Yurisdiksi Legislatif *(legislatif jurisdiction atau jurisdiction to prescribe);*

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

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

[19] 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.

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 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 tentang Informasi dan Transaksi 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. 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 hukum

mengingat 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

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

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

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

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

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

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 Oktober 1993.

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.

Lain-Lain:

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

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

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

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

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

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

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