

KEABSAHAN ALAT BUKTI ELEKTRONIK DALAM UNDANG-UNDANG NO. 11 TAHUN 2008

Bunadi Hidayat *

Abstract

Transactions in cyber crime and activities of illegal business, such as ; fraud, piracy, interception, cyber porn, cyber sex, face books, traffickings, gambling etc, hve been phenomenon and threatening the people in overseas. Facing these cyber crimes, the Government has implemented Constitution Number 11 the year 2008, concerning Information and Electrical Transaction. Based on the judicial considerations of this constitution, some of electrical media are legal evidences by off which values are correspondent to traditional evidences. This statement can be found in : Article 1 point (2), Article 31 point (1) ITE Constitution ; Juncto Article 12 verse (1 and 2), Article 15 verse (1) Constitution Number 8 the year 1997, concerning on Document of Company ; Juncto Article 184 Criminal Justice System ; Article 1320 Civil Code or Burgerlijk Wetboek (B.W) ; Juncto Article 164 Rechtsreglement Voor De Buitengewesten (R.Bg) ; Juncto Article 45 Herzienne Indonesische Reglement (H.I.R). Hence, any documents and information using electrical media, can be classified as the legal evidences in trial court.

Kata kunci : Alat Bukti- Transaksi Elektronik- Undang-Undang

Kemajuan teknologi informasi yang ditandai dengan perkembangan piranti pengolahan informasi komputer, telah memberikan kemudahan kepada dunia. Sistem Jaringan Komunikasi berhasil menjadi infrastruktur dalam teknologi informasi. Hubungan bisnis melalui komunikasi konvensional *via* telepon, sudah tidak lagi dapat memenuhi kebutuhan bisnis yang bersifat global, khususnya dalam bidang perbankan. Internet banyak digunakan sebagai perpaduan antara telekomunikasi dan informatika yang kemudian menghasilkan sebuah media baru yang oleh penggunaanya disebut sebagai *Cyber space*, yaitu : suatu dunia maya yang bergerak tanpa batas. Semua informasi hasil ekspresi pikiran dan gagasan manusia tertuang di dalamnya seolah setiap orang dapat menuangkan ide atau gagasannya secara bebas.

Bertalian dengan istilah cyber space tersebut, Barda Nawawi Arief, mengatakan :

Cyber space / virtual space, memiliki dimensi baru dari high tech crime, dimensi baru dari transnational crime dan dimensi baru dari white collar crime¹

Selanjutnya, Barda Nawawi Arief, menambahkan :

Cyber crime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional²

Barda Nawawi Arief, juga mensitasi pendapat Volodymyr Golubev :

Cyber crime adalah the new form of anti-social behavior³

Lebih lanjut, Barda Nawawi Arief, menjelaskan :

Perkembangan *cyber crime* / tindak pidana mayantara, sering dibahas di berbagai forum internasional. Kongres PBB mengenai "*The Prevention of Crime and the Treatment of Offenders*" yang sejak Kongres XI/2005, berubah menjadi *Congress on Crime Prevention and Criminal Justice*, telah membahas masalah ini sampai tiga kali, yaitu pada Kongres VIII / 1990 di Havana, Kongres X / 2000 di Wina, dan terakhir pada Kongres XI / 2005 di Bangkok (tanggal 18-25 April). Di samping itu, telah ada pula Konvensi *Cyber Crime* Dewan Eropa (*Council of Europe Cyber Crime Convention*) yang ditandatangani di Budapest pada tanggal 23 Nopember 2001 oleh berbagai negara termasuk

* Bunadi Hidayat adalah Dosen Fakultas Hukum Universitas Sunan Giri (Unsuri) Surabaya

¹ Barda Nawawi Arief, *Tindak Pidana Mayantara (Perkembangan Kajian Cyber Crime Di Indonesia)*, PT Raya Grafindo Persada, Jakarta, 2006, h 1

² Ibid

³ Ibid

Kanada, Jepang, Amerika dan Afrika Selatan⁴

Kemajuan ilmu pengetahuan dan teknologi global ini, di satu sisi memang tidak dapat dihindari untuk kebutuhan masyarakat dunia, tetapi di sisi yang lain ketenangan hidup seseorang (*privacy*) juga harus diproteksi dengan piranti hukum yang tegas.

Shinta Dewi, mensitasi pendapat Thomas Cooley, bahwa :

*Jenis hak hidup yang harus dilindungi dalam tort law adalah : (a). hak perorangan (personal right) ; (b) hak hidup (right to life) ; (c) hak kekebalan (the right of personal immunity) yaitu hak seseorang untuk tidak diganggu kehidupan pribadinya atau (to be let alone) ; (d). hak untuk memperoleh reputasi (the right of reputation)*⁵

Privacy seseorang untuk menikmati hak hidup agar tidak diganggu oleh orang lain atau Pemerintah. Hal ini sejalan dengan pendapat Shinta Dewi yang mensitasi pendapat Shinta Dewi, bahwa :

*Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition*⁶

Konvergensi telematika berwujud sebagai penyelenggaraan sistem elektronik yang berbasis teknologi digital dikenal dengan *the net internet*,⁷ merupakan jaringan komputer yang berhubungan satu sama lain melalui media komunikasi, seperti : telepon, serat optik, satelit, atau gelombang frekuensi.⁸ *Internet (interconnected network)* memiliki potensi luar biasa bagi perkembangan bisnis *e-Commerce*, sarana informasi, transaksi valuta asing, proses industri, dan lain sebagainya.⁹

Era globalisasi telah menempatkan peranan teknologi informasi dan komunikasi ke dalam tempat yang sangat strategis, karena menghadirkan suatu dunia tanpa batas, jarak, ruang dan waktu, dan diharapkan dapat meningkatkan produktivitas dan efisiensi yang pada akhirnya akan meningkatkan kesejahteraan masyarakat. Namun selain dampak positif, juga disadari memberikan peluang terjadinya

kejahatan-kejahatan baru (*cyber crime*) yang bahkan lebih canggih dibandingkan kejahatan konvensional.¹⁰

Cyber crime adalah kejahatan yang dilakukan oleh seseorang atau kelompok dengan menggunakan sarana komputer dan alat telekomunikasi lainnya.¹¹ *Cyber crime* juga dapat disebut sebagai *Computer crime*. *The US Department of Justice* memberikan pengertian ... *any illegal act requiring knowledge of computer*.¹²

Menurut *Organization of European Community Development*, *Cyber crime : any illegal, unethical or unauthorized behavior relating to the automatic processing and / or the transmission of data*.¹³ Merujuk pada dokumen Kongres PBB, *The Prevention of Crime and the treatment of offenders* di Havana, Cuba 1999, Wina Austria 2000, mengenal 2 istilah, yaitu :

*Cyber crime in narrow sense (dalam arti sempit) disebut computer crime : any illegal behavior directed by means of electronic operation that target the security of computer system and the data processed by them. Cyber crime in a broader sense (dalam arti luas), disebutkan computer related crime : any illegal behavior directed by means on relation to a computer systems offering or system, or network, including such crime as illegal possession in offering or distributing information by means of computer system or network*¹⁴

Secara sederhana, menurut Sutanto dkk :

*Cyber crime adalah suatu aktivitas yang dilakukan dengan sebuah alat (PC, Laptop, notebook, handphone) yang terhubung dengan jaringan internet dan aktivitas tersebut melanggar undang-undang*¹⁵

Secara umum, *cyber crime* dibagi menjadi 3 karakter, yaitu : (a) *Spam*, yaitu penyebaran *e-mail* secara *illegal* dan biasanya isinya ditumpangangi dengan program *virus* ; (b) *Abuse*, yaitu : penyalagunaan ; dan (c) *Fraud*, yaitu : penipuan¹⁶

4 Ibid

5 Shinta Dewi, *Cyber Law, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Inter nasional*, Widya Pendjadjaran, 2009, h 10

6 Shinta Dewi, Loc Cit

7 Edmon Makarim, *Pengantar Hukum Telematika Suatu Kompilasi Kajian*, (Jakarta, Badan Penerbit FHUI, 2005) , 4. Periksa pula Asril Sitompul, *Hukum Internet*, (Bandung, Citra Aditya Bakti, 2004), X

8 Agus Rahardjo, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, 2002, h 59

9 Sutanto Hermawan Sulisty, dan Tjuk Sugiarto (ed), *Cyber Crime, Mutif dan Penindakan*, (Jakarta, : Pencil 321), 1

10 Didit MArief Mansur dan Elisatris Gultom, *Cyber Law*, Refika Aditama, Bandung, 2005, h 24

11 Sutatman, *Cyber Crime, Modus Operandi dan Penanggulangannya*, Laksbang Press Sindo, Jogjakarta, 2007, h 4

12 Sutatman Op Cit 33

13 Ibid

14 Ibid

15 Sutanto, et all, Op Cit

16 Ibid

Jenis kejahatan *cyber*, meliputi : *cyber Terrorism*, *cyber pornograpy*, *cyber harrasment (pelecehan sexual)*, *Haking* (penggunaan *programming abilities* secara melawan hukum dan *carding (credit card* secara melawan hukum)¹⁷

Berdasarkan uraian di atas, dapat dirumuskan permasalahan sebagai berikut :

1. Apakah setiap perbuatan melawan hukum yang menggunakan media elektronik dapat digunakan sebagai alat bukti yang sah dalam persidangan ?
2. Bagaimana implementasi Undang-Undang No 11 tahun 2008, tentang Informatika dan Transaksi Elektronik dalam Kejahatan Mayantara di Indonesia ?

Alat Bukti Elektronik

Teknologi Informatika dan Komunikasi telah mampu mengubah pola hidup masyarakat secara *global* dan mengakibatkan perubahan sosial, budaya, pendidikan, ekonomi, dan pola penegakan hukum yang kecepataannya berlangsung secara signifikan. Teknologi Informasi dan Komunikasi dewasa ini tidak saja terbukti memberikan kontribusi bagi peningkatan kesejahteraan, tetapi juga menjadi sarana efektif untuk melakukan kejahatan. Kejahatan menggunakan media Teknologi Informasi dan Komunikasi merupakan fenomena yang sangat mengkhawatirkan, misalnya : *banking crime*, *credit card*, *hacking*, *cracking*, *face books*, *dating*, *cyber porn*, *cyber sex*, *interception*, etc

Bidang bisnis merupakan salah satu bidang yang memiliki korelasi dan tingkat interdependensi yang tinggi terhadap perkembangan teknologi informasi dan komunikasi, yaitu : menggunakan jaringan *internet*. Teknologi Informasi dan Komunikasi dimanfaatkan untuk berkomunikasi, penyebaran, dan pencarian data, kegiatan belajar mengajar, pelayanan dan transaksi bisnis perbankan, *e-commerce*. Perdagangan berbasis teknologi canggih (*e-Commerce*) telah mereformasi perdagangan konvensional, interaksi secara langsung menjadi interaksi secara *virtual*. Transaksi *e-Commerce* diciptakan transaksi bisnis lebih praktis, tanpa perlu memakai kertas (*paperless*), para pihak tidak perlu bertemu langsung secara *face to face*, dan dapat bertandatangan secara elektronik.

Transaksi elektronik di satu sisi memang menguntungkan, tetapi di pihak yang lain,

menimbulkan penyelewengan dan masalah hukum, khususnya mengenai sahnya suatu perjanjian dengan menggunakan media elektronik. Menurut ketentuan Pasal 1313 KUH Perdata : Perjanjian adalah perbuatan dengan mana satu orang atau lebih mengikatkan dirinya terhadap satu orang atau lebih. Subekti berpendapat, perjanjian adalah suatu peristiwa dimana seorang berjanji kepada orang lain atau dimana orang itu saling berjanji untuk melaksanakan suatu hal. Berdasarkan ketentuan Pasal 1320 KUH Perdata, ditegaskan syarat sahnya perjanjian : sepakat saling mengikat diri, kecakapan untuk membuat suatu perjanjian dan suatu sebab yang halal.

Keabsahan Transaksi Elektronik dengan mendasarkan pada ketentuan Pasal 1320 KUH Perdata, sebenarnya tidak menjadi masalah jika dihubungkan dengan media yang digunakan dalam transaksi yang lain, karena ketentuan Pasal 1320 KUH Perdata tidak mensyaratkan bentuk dan jenis media yang digunakan dalam bertransaksi. Asas kebebasan berkontrak yang dianut KUH Perdata, dimana para pihak dapat bebas menentukan dan membuat suatu perikatan atau perjanjian dalam bertransaksi yang dilakukan berdasarkan itikat baik (*Vide* Pasal 1338 KUH Perdata). Jadi apapun bentuk dan media dari kesepakatan tersebut, tetap berlaku dan mengikat para pihak karena perikatan tersebut merupakan undang-undang bagi yang membuatnya.

Permasalahan yang akan timbul dari suatu transaksi apabila salah satu pihak ingkar janji (*wanprestasi*). Penyelesaian permasalahan yang terjadi tersebut, selalu berkait dengan apa yang menjadi barang bukti dalam bertransaksi terlebih apabila transaksi yang menggunakan sarana elektronik. Hal ini karena menggunakan dokumen atau data elektronik sebagai akibat transaksi melalui media elektronik, belum diatur secara khusus dalam hukum acara yang berlaku, baik dalam Hukum Acara Perdata maupun dalam Hukum Acara Pidana.

Sebelum lahirnya Undang-Undang Nomor 11 tahun 2008, tentang Informasi dan Transaksi Elektronik (UU ITE), Mahkamah Agung menyadari adanya perkembangan teknologi informatika dalam menyikapi penggunaan *microfilm* atau *microfiche* untuk menyimpan suatu dokumen. Mahkamah Agung dengan suratnya tanggal 14 Januari 1988 yang ditujukan kepada Menteri Kehakiman menyatakan

17 Ibid

bahwa *microfilm* atau *microfiche* dapat dipergunakan sebagai alat bukti surat sebagaimana tersebut dalam Pasal 184 ayat (1) huruf c Kitab Undang-Undang Hukum Acara Pidana (KUHAP), dengan catatan bahwa baik *microfilm* maupun *microfiche* itu, yang sebelumnya dijamin otentiknya, dapat ditelusuri kembali dari registrasi dan berita acaranya.

Demikian pula dengan diundangkannya Undang-Undang No 8 tahun 1997, tanggal 24 Mei 1997, tentang Dokumen Perusahaan yang dalam Pasal 15 ayat (1) ditegaskan bahwa : Dokumen Perusahaan yang telah dimuat dalam *microfilm* atau media lainnya dan atau hasil cetaknya merupakan alat bukti yang sah.

Selanjutnya, apabila memperhatikan ketentuan Pasal 1 angka 2, mengenai pengertian dokumen dan dikaitkan dengan ketentuan Pasal 12 ayat (1) dan ayat (2) Undang-Undang No 8 tahun 1997 Jo Pasal 1320 KUH Perdata, transaksi melalui media elektronik adalah sah menurut hukum.

Secara konvensional, setiap orang melakukan perjanjian selalu berhadapan antara yang satu dengan yang lain. Mereka saling mengenal dan saling membubuhkan tanda tangan pada draf perjanjian dengan tinta di atas kertas. Sedangkan dalam transaksi elektronik, prinsip-prinsip perjanjian dilakukan secara *virtual*, mereka tidak saling mengenal secara personal, tidak pernah bertatap muka, bahkan tidak membubuhkan tanda tangan secara *manual*.

Dalam kondisi riil, transaksi elektronik tidak dapat dihindari, bahkan tidak terasa masyarakat terbiasa melakukan transaksi tersebut, misalnya : melakukan pembayaran melalui mesin pembayaran (*Automatic Teller Machine / ATM*, atau Anjungan Tunai Mandiri). Sebenarnya tanpa disadari bahwa transaksi dengan menggunakan *credit* berpotensi merugikan orang lain. Segala transaksi elektronik yang telah dilakukan, tidak dapat dikembalikan, meskipun ada unsur perjanjian yang tidak terpenuhi atau salah input di mesin *ATM* dan pembobolan *credit card* sehingga justru pihak lain yang menerima keuntungan.

Eksistensi Undang-Undang Informasi Dan Transaksi Elektronik

Segala perbuatan hukum baik dalam bidang hukum pidana maupun dalam hukum perdata di era informasi ini senantiasa menggunakan alat teknologi, yaitu sistem komputer dan *internet* (dalam arti sempit) dan sistem informasi elektronik lainnya (dalam arti

luas), seperti : *radio*, *televisi*, *handphone*, *handy talky* dan sebagainya. Setiap kemampuan dan keahlian yang menggunakan *internet* ternyata mampu memecahkan dari sistem kode masuk (*security password program*) ke *computer security program*. Eksistensi *internet* sebagai infra struktur *modern*, acapkali menimbulkan masalah baru baik secara teknis (sebagai media) maupun non-teknis berupa aplikasi teknologi elektronik tersebut.

Permasalahan yang timbul secara substantif adalah subyek atau pelaku tindak pidana *cyber crime*. Sebagaimana sifat *cyber crime* adalah *transnational crime* yang bersifat maya, maka pelaku tindak pidana *cyber crime* bisa dilakukan oleh orang, korporasi, lembaga dan negara. Jika *cyber crime* itu dilakukan di luar negeri yang dampaknya terjadi dan dirasakan di Indonesia, maka yang menjadi acuan adalah hukum positif yang berlaku di kedua negara tersebut. Di samping itu harus ada perjanjian ekstradisi yang disepakati oleh kedua negara itu. Selain kendala subyek atau pelaku tindak pidana, permasalahan perangkat hukum juga harus jelas, karena bisa jadi ketentuan normatif *cyber crime* di negara tertentu secara tegas dilarang, tetapi di negara tertentu bukan merupakan tindak pidana *cyber crime*. Selanjutnya yang menyangkut validitas dan keaslian data *message (availability)*, secara yuridis menyangkut kekuatan hukum yang mengikat para pihak. Apabila data tersebut digunakan sebagai alat bukti, maka permasalahan lain yang timbul adalah sistem hukum yang berlaku, khususnya hukum acara pidana dan hukum acara perdata, disamping juga ketentuan hukum materiel dari kedua hukum acara tersebut. Demikian pula terhadap teritorial dimana terjadinya tindak pidana *cyber crime*, juga menjadi permasalahan hukum, misalnya asas hukum pidana di Indonesia yang menganut asas *locus delictie*, bisa saja terjadi : Tempat Kejadian Perkara (TKP) *cyber crime* di Amerika yang belum memiliki perjanjian ekstradisi dengan Indonesia, tetapi dampak atau imbasnya dirasakan di Indonesia. Hal ini juga menjadi permasalahan hukum yang rumit untuk diselesaikan.

Jika *cyber crime* itu dilakukan warga negara Indonesia, dan terjadi di Indonesia, maka penyelesaiannya akan berbeda dengan yang diuraikan di atas. Dengan diundangkannya Undang-Undang No 11 tahun 2008, tentang Informasi dan Transaksi Elektronik atau yang lazim disebut Undang-Undang ITE, maka segala perbuatan *cyber crime* memperoleh pengaturan yang jelas. Kedudukan

Indonesia sebenarnya sudah setara dengan negara tetangga yang lebih dahulu mengatur tentang transaksi elektronik, seperti : Malaysia telah mempunyai *Computer Crime Act 1997*, *Digital Signature Act* tahun 1997, *Communication and Multimedia Act 1998*. Singapura telah memiliki undang-undang yang mengatur tentang transaksi elektronik, yaitu : *The Electronic Act 1998*, *The Electronic Communication and Privacy Act*, *The Singapore Evidence Act 1996*.

Menurut ketentuan Pasal 1 angka 2, Undang-Undang ITE, ditegaskan : Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, Jaringan Komputer, dan / atau media elektronik lainnya. Berdasarkan ketentuan Pasal 1 angka 4, Undang-Undang ITE, ditegaskan Dokumen Elektronik adalah :

Setiap informasi elektronik yang dibuat, diteruskan, dikirim, diterima, atau disimpan dalam bentuk analogi, digital, elektronik genetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan dan / atau didengar melalui Komputer atau Sistem Elektronik, tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Undang-Undang No 11 tahun 2008, merupakan hukum baru dalam khasanah peraturan perundangan di Indonesia. Karena itu, dengan menganut asas yurisdiksi ekstrateritorial dan alat bukti elektronik, sudah seperti alat bukti lain yang diatur dalam KUHAP (Pasal 184) atau *H.I.R / R. Bg.* (Pasal 45, 164). Jika dikaitkan dengan ketentuan Pasal 11 Undang-Undang ITE, tanda tangan elektronik diakui memiliki kekuatan hukum yang sama dengan tanda tangan konvensional yang menggunakan tinta basah dan bermaterai. Keadaan itu diharapkan akan memberikan kepastian hukum bagi pemanfaatan teknologi informasi dan komunikasi yang telah berkembang pesat dan memasuki berbagai segi kehidupan berbangsa dan bernegara.

Ketika terjadi sengketa keperdataan atau terjadi *cyber crime*, hukum mulai muncul ke permukaan karena dibutuhkan sebagai indikator keabsahan perjanjian, keabsahan transaksi, pembuktian, keabsahan alat bukti, penyitaan dan seterusnya. Dengan demikian, kendala yang dihadapi dalam pembuktian di persidangan adalah keabsahan dokumen-dokumen transaksi yang dapat diajukan

sebagai alat bukti. Misalnya dalam perkara pidana dilakukan penyitaan alat bukti yang dilakukan oleh penyidik. Penyidik hanya mampu menyita beberapa perangkat komputer, sedangkan *file* yang berisi program yang berada di dalamnya sulit untuk disita. Apabila data yang berada dalam komputer tersebut di-*print out* menjadi *hard copy*, maka pertanyaannya adalah menyangkut validitas / keabsahan *hard copy* tersebut yang diajukan sebagai alat bukti.

Otorisasi keabsahan hukum transaksi elektronik di bursa, telah diratifikasi seiring dengan diterimanya sistem *order* melalui *digital signature* kode *broker* di sistem bursa (*JATS, e Clears, dan c Best*) serta nomor rekening di sistem perbankan. Bahkan dapat dikatakan, Indonesia tidak terlihat terbelakang dari sisi yuriprudensi ketika diterimanya alur rekening dana sebagai alat bukti hukum di pengadilan. Catatan rekening bank (yang berbasis elektronik) dan pembicaraan (penyadapan) telepon sudah menjadi alat bukti di pengadilan. Hal ini sebagaimana terurai dalam Pasal 31 angka (1) Undang-Undang ITE yang selengkapnya berbunyi :

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan / atau Dokumen Elektronik dalam suatu Komputer dan / atau Sistem Elektronik tertentu milik orang lain

Selanjutnya dalam Pasal 31 ayat (2) ditambahkan:

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan / atau Dokumen Elektronik yang 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 dan / atau Dokumen Elektronik yang sedang ditransmisikan.

Kemudian di dalam Pasal 47 Undang-Undang ITE ditegaskan :

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan / atau denda paling banyak Rp 800. 000. 000, 00 (delapan ratus juta rupiah)

Keabsahan alat bukti intersepsi ini juga terlihat

dalam pemberantasan tindak pidana korupsi. Komisi Pemberantasan Korupsi (KPK) melalui peradilan tindak pidana korupsi (Tipikor) kerap kali melakukan terobosan hukum tersebut. Tindak pidana pencucian uang (*Money Laundry*) sebagaimana diatur dalam Undang-Undang No 15 tahun 2002 sebagaimana diperbarui dengan Undang-Undang No 25 tahun 2003, tentang Pencucian Uang, telah menunjukkan verifikasi alat bukti transaksi keuangan antar yurisdiksi lembaga negara yang semuanya berbasis elektronik, dapat dilakukan melalui kewenangan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK).

Alat bukti dalam perkara perdata dapat dilihat secara tegas dalam Pasal 164 *H.I.R / R.Bg* dan Pasal 1866 KUH Perdata, bahwa alat bukti adalah : tulisan, saksi-saksi, persangkaan, pengakuan dan sumpah. Sedangkan dalam ranah hukum pidana alat bukti adalah (a) keterangan saksi ; (b) keterangan ahli ; (c) surat ; (d) petunjuk ; dan (e) keterangan terdakwa ; Selanjutnya dalam ayat (2) ditegaskan : Hal yang secara umum sudah jelas, tidak perlu dibuktikan. Patut diketahui, baik dalam *H.I.R / R.Bg* maupun KUHAP **belum mengatur** masalah alat bukti elektronik, namun di **berbagai undang-undang yang baru, telah mengatur** dokumen elektronik **menjadi alat bukti yang sah**, termasuk alat bukti surat, *microfilm* dan media lainnya (*CD ROM* atau *WORM*).

Menurut ketentuan Pasal 1 ayat (4) Undang-Undang ITE, ditegaskan : Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirim, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditayangkan, dan / atau didengar melalui Komputer atau Sistem Elektronik, tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahami.

Berdasarkan ketentuan di atas, maka sebenarnya yang dimaksud dengan dokumen elektronik adalah setiap informasi yang menggunakan media elektronik. Dokumen tersebut harus dalam keadaan dibuat, diteruskan, dikirim, diterima dan disimpan secara elektronik. Dokumen tersebut tidak dapat diraba atau disentuh atau dilihat tanpa menggunakan media elektronik. Penyimpangan dokumen elektronik dilakukan secara digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan dan / atau didengar melalui

komputer.

Informasi lain termasuk dokumen / informasi elektronik berupa suara, gambar, peta, rancangan, foto, atau sejenisnya, huruf, tanda, angka, kode akses (*password*), simbol atau perforasi makna atau sejenisnya yang dapat dipahami oleh orang yang mampu memahami. Orang yang mampu memahami dalam dokumen atau informasi elektronik adalah orang yang ahli dalam bidang elektronik. Bagi orang yang ahli dalam semua bidang informasi elektronik dapat memberikan dan mengungkapkan berbagai misteri dan memiliki makna khusus dalam bidang tersebut.

Hampir di segala bidang kehidupan tidak terlepas dari kebutuhan dokumen dan informasi elektronik. Misalnya dalam dunia medis, hampir semua jenis pemeriksaan bahkan tindakan dan keputusan tim medis untuk melakukan tindakan operasi menggunakan komputer. Aktivitas gunung berapi, rahasia dunia di bawah laut, dasar bumi, ruang angkasa, rekayasa genetik, logika kuantitatif, dunia industri dan perbankan, semua itu dilakukan dengan menggunakan media komputer.

Berdasarkan ketentuan Pasal 5 ayat (1), Undang-Undang ITE, ditegaskan : *print out* yang dihasilkan dari media elektronik dapat digunakan sebagai alat bukti yang sah di persidangan. Selanjutnya dalam Pasal 5 ayat (2) Undang-Undang ITE tersebut, selengkapnya berbunyi : Informasi Elektronik dan / atau Dokumen Elektronik dan / atau hasil cetaknya sebagaimana yang dimaksud dalam ayat (1) di atas, merupakan perluasan dari alat bukti yang sah sesuai dengan ketentuan Hukum Acara yang berlaku di Indonesia. Kemudian Pasal 5 ayat (3) Undang-Undang ITE, menegaskan : Informasi Elektronik dan / atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

Dalam hal terjadi kecelakaan pesawat terbang, penyelidik dan penyidik tidak hanya memperhatikan keadaan korban, tetapi juga keadaan kotak hitam (*black box*) pesawat tersebut. Meskipun *black box* itu tidak berwarna hitam, melainkan *orange*. Sebenarnya yang dimaksud hitam itu, bukanlah warna kotaknya, tetapi kotak tersebut dapat menyimpan misteri penyebab kecelakaan pesawat yang masih gelap (hitam) yang harus diungkap oleh penyidik dengan menggunakan ilmu pengetahuan khusus. Kotak hitam itu mampu mengungkapkan semua misteri yang

menjadi penyebab kecelakaan dalam pesawat terbang. Setelah semua data / informasi / dokumen berhasil diungkapkan dalam *black box* tersebut, maka semua data, informasi, dokumen dalam *black box* itu dapat dikatakan sebagai alat bukti yang sah dalam persidangan.

Ketentuan Pasal 5 ayat (1) Undang-Undang ITE, memberikan batasan terhadap dokumen tertentu, terhadap berbagai dokumen hukum yang menurut ketentuan undang-undang harus dibuat dan dituangkan dalam akta notariil oleh Pejabat yang berwenang. Akta tersebut berdasarkan sifat dan bentuknya harus dibuat dengan bentuk tertulis berdasarkan formalitas / tata cara dan bentuk yang telah ditentukan oleh peraturan perundangan. Akta sebagaimana dimaksud, seperti : sertifikat hak atas tanah, akta jual beli, akta ikatan jual beli, akta perkawinan, akta pendirian berbagai lembaga baik untuk bisnis maupun kepentingan sosial. Meskipun datanya juga disimpan dalam Komputer, dan dapat dicetak / di-*print out* dalam bentuk *hard copy*, namun kalau digunakan sebagai alat bukti di pengadilan menjadi tidak sah. Dokumen yang harus diajukan di Pengadilan sebagai alat bukti tetap harus dapat menunjukkan dokumen aslinya. Meskipun *print out* dari berbagai dokumen hukum dibuat oleh Pejabat yang sama, diperoleh dari Komputer yang sama dan datanya sama, tetap tidak dapat dinilai sebagai alat bukti yang sah di Pengadilan. Kekuatan pembuktian dari *print out* dokumen hukum tersebut, hanya merupakan petunjuk.

Uraian tersebut dikuatkan dengan ketentuan Pasal 5 ayat (4) huruf (a dan b) Undang-Undang ITE yang menegaskan :

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 notariil atau akta yang dibuat oleh Pejabat Pembuat Akta

Kesimpulan

Dengan diundangkannya Undang-Undang No 11 tahun 2008, tentang Informasi dan Transaksi Elektronik, maka alat bukti elektronik diakui seperti : alat bukti lainnya yang diatur di dalam KUHAP. Konsekuensi yuridis terhadap keabsahan alat bukti

elektronik dinyatakan sah secara hukum, maka menjadi sah pula diajukan sebagai alat bukti di Pengadilan. Demikian pula terhadap tanda tangan elektronik diakui memiliki kekuatan hukum yang sama dengan tanda tangan konvensional (dengan tinta basah dan bermaterai). Namun demikian rasa keadilan substantif dalam *cyber crime* masih terasa sulit dirasakan karena *cyber crime* mempunyai sifat yang maya baik ditinjau dari perangkat hukum yang digunakan, subyek hukum yang harus diminta pertanggungjawaban maupun dilihat dari wilayah atau teritorial hukum yang dipakai sebagai tempat yang untuk mengadili *cyber crime* tersebut.

DAFTAR PUSTAKA

- Arief Barda Nawawi, *Tindak Pidana Mayantara , Perkembangan Kajian Cyber Crime di Indonesia*, PT Raja Grafindo Persada, Jakarta, 2006
- Dewi Shinta, *Cyber Law, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Mien AZ. Widya, Padjadjaran, 2009
- Makarin Edmon, *Pengantar Hukum Telematika, Suatu Kompilasi*, FH.Ul, Jakarta, 2005.
- Mansur Didik M Arif dan Elisatris Gultom, *Cyber Law*, Refika Aditama, Bandung, 2005
- Rahardjo Agus, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, 2002
- Sitompul Asril, *Hukum Internet*, Citra Aditya Bakti, Bandung, 2004
- Sulistyo dan Tjuk Sugiarti, Sutanto Hermawan, *Cyber Crime, Mutif dan Penindakan*, Pensil 324, Jakarta
- Sutarman, *Cyber Crime, Modus Operandi dan Penanggulangannya*, LaksBang PRESSindo, Jogjakarta, 2007