UNIVERSITAS INDONESIA

KEABSAHAN TANDA TANGAN ELEKTRONIK SEBAGAI ALAT BUKTI YANG SAH DITINJAU DALAM HUKUM ACARA PERDATA

T E S I S

JOAN VENZKA TAHAPARY

0906582665

FAKULTAS HUKUM
PROGRAM STUDI MAGISTER KENOTARIATAN
DEPOK
JULI 2011

UNIVERSITAS INDONESIA

KEABSAHAN TANDA TANGAN ELEKTRONIK SEBAGAI ALAT BUKTI YANG SAH DITINJAU DALAM HUKUM ACARA PERDATA

T E S I S

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Kenotariatan

JOAN VENZKA TAHAPARY

0906582665

FAKULTAS HUKUM
PROGRAM STUDI MAGISTER KENOTARIATAN
DEPOK
JULI 2011

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

HALAMAN PENGESAHAN

Tesis ini diajukan oleh

Nama	:	Joan Venzka Tahapary, SH
NPM	:	0906 582665
Program Studi	:	Magister Kenotariatan
Judul Tesis	:	Keabsahan Tanda Tangan Elektronik Sebagai Alat Bukti Yang Sah Ditinjau Dalam Hukum Acara Perdata.

Telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Kenotariatan pada Program Studi Magister Kenotariatan, Fakultas Hukum, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Pieter Latumeten, S.H., M.H. (.....)

Penguji : Dr. Drs. Widodo Suryandono, S.H., M.H. (.....)

Penguji : Wenny Setiawaty, S.H, M.Li (.....)

Ditetapkan di : Depok

Tanggal : 15 – 07 - 2011

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	:	**Joan Venzka Tahapary, SH**
NPM	:	**0906 582665**
Tanda Tangan	:	
Tanggal	:	**15 – 07 - 2011**

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan dibawah ini :

Nama	: Joan Venzka Tahapary, SH
NPM	: 0906 582665
Program Studi	: Magister Kenotariatan
Fakultas	: Hukum
Jenis Karya	: Tesis

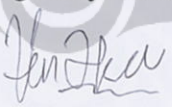
Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Non-eksklusif** (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul :

KEABSAHAN TANDA TANGAN ELEKTRONIK SEBAGAI ALAT BUKTI YANG SAH DITINJAU DALAM HUKUM ACARA PERDATA

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-eksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/ formatkan, mengelola dalam bentuk pangkalan data *(database)*, merawat, dan mempublikasikan tugas akhir saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 15 – 07 - 2011
Yang menyatakan,



(Joan Venzka Tahapary, SH)

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

KATA PENGANTAR

Dengan mengucapkan segala puji dan syukur atas segala limpahan berkat kepada Tuhan Yesus, karena atas kasih, tuntunan dan izin-Nya saja sehingga penulis berhasil menyusun dan dapat menyelesaikan penulisan tesis yang berjudul "**Keabsahan Tanda Tangan Elektronik Sebagai Alat Bukti Yang Sah Ditinjau Dalam Hukum Acara Perdata**", sebagai suatu syarat untuk mendapatkan derajat sarjana S-2 pada Program Studi Magister Kenotariatan Universitas Indonesia.

Selama proses penulisan tesis ini sejak penyusunan rancangan penelitian, studi kepustakaan, pengumpulan data serta pengolahan hasil penelitian sampai terselesaikannya penulisan tesis ini, penulis telah banyak mendapatkan bantuan baik sumbangan pemikiran maupun tenaga yang tak ternilai harganya dari berbagai pihak. Untuk itu pada kesempatan ini perkenankanlah penulis dengan segala kerendahan hati dan penuh keikhlasan untuk menyampaikan rasa terima kasih yang tulus kepada :

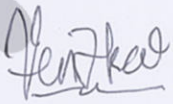
1. Bapak Dr. Drs. Widodo Suryandono, S.H., M.H., selaku Ketua Program Studi Magister Kenotariatan Universitas Indonesia.
2. Bapak Pieter Latumeten, S.H., M.H., selaku Dosen Pembimbing Utama yang telah meluangkan waktu untuk memberikan bimbingan dan arahan dalam penulisan tesis ini hingga mencapai hasil yang maksimal. Merupakan suatu kebanggaan tersendiri bagi penulis mendapatkan bimbingannya.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

3. Papa dan Mama tersayang Joppy Tahapary dan Jeanne Tahapary, yang selalu setia membantu dan membimbing Penulis dalam setiap harinya sampai tesis ini terselesaikan.
4. Rekan-rekan Program Studi Magister Kenotariatan Universitas Indonesia 2009 khususnya olin, cici, bayu, juned, tulang, kiki, aileen, ritson, ricky, rajul.
5. Seluruh staf pengajar dan tata usaha pada Program Studi Magister Kenotariatan, Universitas Indonesia atas segala ilmu yang telah diberikan dan yang telah membantu penulis dalam menyelesaikan pendidikan di Program Studi Magister Kenotariatan, Universitas Indonesia.
6. Semua pihak yang tidak dapat disebutkan satu persatu yang telah banyak membantu penulis dalam melakukan penelitian sejak awal sampai akhir penulisan tesis ini.

Akhirnya semoga tesis ini dapat memberikan sumbangan dan pikiran serta bermanfaat bagi semua pihak yang membacanya.

Depok, Juli 2011



Joan Venzka Tahapary

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

ABSTRAK

Nama : Joan Venzka Tahapary, SH
Program Studi : Magister Kenotariatan
Judul : **Keabsahan Tanda Tangan Elektronik Sebagai Alat Bukti Yang Sah Ditinjau Dalam Hukum Acara Perdata**

Penggunaan tanda tangan elektronik pada suatu dokumen elektronik, dapat menjamin keamanan suatu pesan informasi elektronik, yang menggunakan jaringan publik, karena tanda tangan elektronik dibuat berdasarkan teknologi kriptografi asimetris. Dari penelitian, terdapat perbedaan pendapat mengenai kekuatan pembuktian dokumen elektronik, yang ditandatangani dengan tanda tangan elektronik yang digunakan sebagai alat bukti dipersidangan. Pemerintah hendaknya segera mengesahkan Peraturan Pemerintah mengenai Tanda Tangan Elektronik dan Peraturan Pemerintah mengenai Sertifikasi Elektronik, sehingga ada aturan hukum lebih lanjut dari Undang-Undang Nomor 11 Tahun 2008. Dokumen elektronik yang telah ditandatangani dengan tanda tangan elektronik, mempunyai daya pembuktian yang sama dengan akta otentik yang dibuat oleh pejabat yang berwenang, setelah dikeluarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sedangkan para notaris berpendapat dokumen elektronik yang ditandatangani dengan tanda tangan elektronik, hanya mempunyai kekuatan pembuktian dibawahtangan, karena tidak memenuhi syarat sebagai akta otentik, yaitu tidak menghadap kepada pejabat yang berwenang.

Kata kunci:
Alat Bukti, Tanda Tangan, Tanda Tangan Elektronik.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

ABSTRACT

Nama : Joan Venzka Tahapary
Program Studi : Magister Kenotariatan
Judul : **Electronic Signature Validity Evidence As Seen In The Legal Civil Procedure**

The use of electronic signatures on an electronic document, can guarantee the security of an electronic information message, which uses a public network, because an electronic signature based on asymmetric cryptography technology. From research, there is a difference of opinion regarding the strength of proof electronic documents, signed by electronic signature that is used as evidence dipersidangan. The government should immediately ratify the Government Regulation on Electronic Signatures and Certification Regulations on Electronic Government, so there is further legal rules of Law Number 11 Year 2008. Electronic documents signed with electronic signatures, have the same evidentiary power of the authentic deed made by the competent authority, having issued Law Number 11 Year 2008 on Information and Electronic Transaction, whereas the electronic document notary public opinion that was signed with the sign electronic hand, only has the power of proof , because it does not qualify as an authentic deed, that is not facing to the authorities.

Key words: Evidence, Signature, Electronic Signatures.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

DAFTAR ISI

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan jaman saat ini sangatlah pesat bila dibandingkan sepuluh tahun yang lalu. Saat ini perkembangan ilmu pengetahuan yang ada sudah cukup berkembang apalagi dengan hadirnya era internet. Kebutuhan akan dunia yang serba praktis ini mendukung semakin berkembanganya dunia maya. Semua orang saat ini butuh sesuatu yang serba cepat. Untuk mencari sesuatu didalam jaringan Internet semua orang bisa mengakses dan mendapatkan informasi dengan mudah.

Informasi sangat mudah didapat pada saat era internet seperti saat ini. Mulai dari anak kecil sampai orang tua sering menggunakan layanan jaringan internet. Setiap infomasi yang mereka butuhkan sangat cepat dan mudah didapat. Hanya menggunakan tombol Klik saja maka informasi yang mereka inginkan bisa didapat di dalam jaringan Internet. Dunia maya memastikan untuk kita berhubungan dengan banyak orang. Informasi yang kita peroleh pun juga bertambah banyak. Cara kita memperoleh informasi inilah sekarang dilindungi melalui suatu peratutan perundangann yang ada di UU no. 11 Tahun 2008. Begitu banyak cara kita memperoleh informasi di dalam dunia maya. Informasi mengenai apa saja dapat dicari di Jaringan Internet Dunia Maya. Banyak orang yang sering menyalah gunakan penggunaan Informasi secara elektonik ini olek karena itu dibutuhkan sesuatu aturan perundang – undangan untuk melindunginya.

Selain untuk mencari informasi maka kita dapat juga melakukan trasaksi melalui jaringan Internet. Transaksi elektronik saat ini sudah sering dilakukan karena orang begitu ingin praktisnya.Ditengah globalisasi komunikasi yang semakin terpadu (*global communication network*) dengan semakin populernya Internet seakan telah membuat dunia semakin menciut (*shrinking the world*) dan semakin memudarkan batas-batas negara berikut kedaulatan dan tatananan masyarakatnya. Ironisnya, dinamika masyarakat Indonesia yang masih baru tumbuh dan berkembang

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

sebagai masyarakat industri dan masyarakat Informasi, seolah masih tampak prematur untuk mengiringi perkembangan teknologi tersebut. Pola dinamika masyarakat Indonesia seakan masih bergerak tak beraturan ditengah keinginan untuk mereformasi semua bidang kehidupannya ketimbang suatu pemikiran yang handal untuk merumuskan suatu kebijakan ataupun pengaturan yang tepat untuk itu. Meskipun masyarakat telah banyak menggunakan produk-produk teknologi informasi dan jasa telekomunikasi dalam kehidupannya, namun bangsa Indonesia secara garis besar masih meraba-raba dalam mencari suatu kebijakan publik dalam membangun suatu infrastruktur yang handal (*National Information Infrastructure*) dalam menghadapi infrastruktur informasi global (*Global Information Infrastructure*).[1]

Indonesia yang berada dalam era globalisasi ditandai dengan era teknologi informatika yang memperkenalkan dunia maya (cyberspace, virtual world) melalui jaringan internet, komunikasi dengan media elektronik tanpa kertas. Melalui media elektronik ini maka seseorang akan mememasuki dunia maya yang bersifat abstrak, universal, lepas dari keadaan tempat dan waktu.[2] Masyarakat Indonesia yakin bahwa peran informasi berperan untuk memberi kontribusi terhadap pembangunan ekonomi, sosial dan budaya. Selain itu kemajuan teknologi informasi juga mempengaruhi kondisi sosial pada masa yang kan datang, seperti sistem pelayanan medis, sistem pelayanan pendidikan, sistem pelayanan administrasi pemerintahan dan berbagai aspek kehidupan lainnya.[3] Setiap orang dapat memberikan informasi tentang segala hal, termasuk juga pemberian informasi terhadap penjualan suatu barang atau jasa dengan menggunakan teknologi informasi ini, dari informasi tersebut, apabila seseorang tertarik untuk memiliki suatu produk barang atau jasa yang ditawarkan tersebut, maka akan terjadi suatu transaksi elektronik. Kedudukan sederajat antara perlindungan hukum, kehandalan dan

---

[1] Maria Farida Indrati Soepapto, *Ilmu perundang-Undangan, Dasar-Dasar dan Pembentukan*, Kanisius, Jakarta, 1998, hal. 25.

[2] Mariam Darus Badrulzaman, *Mendambakan Kelahiran Hukum Saiber (Cyber Law) di Indonesia*, Pidato Purna Bhakti, Medan, 13 Nopember 2001, hal. 3.

[3] *Ibid*, hal. 6.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

keamanan teknologi informasi akan menciptakan suatu "kepercayaan" kepada para penggunanya, tanpa kepercayaan ini perdagangan elektronik dan pemerintahan elektronik yang saat ini digalakkan oleh pemerintah Indonesia tidak akan berkembang. Kepercayaan ini dapat diperoleh dengan memberikan pengakuan hukum terhadap tulisan elektronik. Hingga hari ini hukum positif Indonesia menentukan bahwa hanya satu cara untuk memberikan kekuatan hukum dan akibat hukum terhadap suatu akta, yaitu dengan tanda tangan manuskrip. Namun, dalam praktek perdagangan khususnya, tanda tangan manuskrip sudah kian tergeser dengan penggunaan tanda tangan elektronik yang melekat pada akta terdematerialisasi atau dengan kata lain "akta elektronik", sehingga timbul perdebatan tentang pengakuan, kekuatan hukum dan akibat hukum dari sebuah tanda tangan elektronik.

Transaksi elektronik bersifat *non face* (tanpa bertatap muka), *non sign* (tidak memakai tanda tangan asli) dan tanpa batas wilayah (seseorang dapat melakukan Transaksi elektronik dengan pihak lain walaupun mereka berada di Negara yang berbeda) dengan menggunakan teknologi informasi.[4] Dalam, perkembangannya, aspek keamanan dalam informasi sudah mulai diperhatikan. Ketika informasi ini menjadi rusak atau maka akan terdapat resiko-resiko yang harus ditanggung oleh orang-orang baik yang mengirim, membutuhkan, ataupun sekedar melihatnya, dikarenakan penggunaan informasi elektronik ini, menggunakan jaringan publik, dimana setiap orang dapat mengetahui informasi elektronik tersebut , atau apabila salah satu pihak tidak melaksanakan prestasi dari transaksi elektronik yang telah disepakati dengan pihak yang lain, hal ini merugikan pihak yang berkepentingan yang menggunakan teknologi informasi untuk penjualan suatu barang atau jasa.

Oleh karena itu, sangat dibutuhkan produk hukum yang bertujuan untuk meningkatkan keamanan dari transaksi-transaksi elektronik melalui jaringan elektronik, serta untuk memberikan pengakuan terhadap kekuatan hukum dari alat bukti elektronik dan tanda tangan elektronik. Sejak tahun

[4] *Penjelasan Undang-undang nomor 11 Tahun 2008Tentang Informasi dan Transaksi Elektronik.*

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

1999 Rancangan Undang-Undang ini dibahas oleh Badan Legislatif yang berwenang, akhirnya Indonesia mempunyai aturan hukum untuk mengatur masalah tersebut dengan dikeluarkannya Undang-Undang Nomor 11 tahun 2008, tentang "Informasi dan Transaksi Elektronik" yang disahkan pada tanggal 21 April 2008. Berdasarkan pada Pasal 18 juncto Pasal 7 juncto Pasal 11 Undang-Undang Nomor 11 Tahun 2008 maka kekuatan pembuktian dokumen elektronik tersebut yang ditandatangani dengan *digital signature* sama dengan kekuatan pembuktian akta otentik yang dibuat oleh pejabat umum yang berwenang.

Aturan tersebut diatas bertentangan dengan Pasal 1 ayat (7) Undang-Undang Nomor 30 tahun 2004 yang dimaksud akta notaris adalah akta otentik yang dibuat oleh atau dihadapan Notaris menurut bentuk dan tata cara yang ditetapkan dalam Undang-Undang ini. Sedangkan pengertian akta otentik berdasarkan Pasal 1868 KUH Perdata adalah suatu akta yang didalam bentuk yang ditentukan oleh Undang-Undang, dibuat oleh atau di hadapan pegawai-pegawai umum yang berkuasa untuk itu di tempat di mana akta dibuatnya . Akibat terjadi suatu pertentangan aturan tersebut, maka apabila salah satu pihak mengajukan gugatan dengan alat bukti dokumen elektronik yang ditandatangani dengan tanda tangan elektronik sebagai alat bukti[5], maka di dalam menyelesaikan sengketa dipengadilan, hakim dituntut untuk berani melakukan terobosan hukum, karena dia yang paling berkuasa dalam memutuskan suatu perkara dan karena dia juga yang dapat memberi suatu *vonnis van de rechter*, yang tidak langsung dapat didasarkan atas suatu peraturan hukum tertulis atau tidak tertulis. Sesuai dengan penjelasan umum UU no. 11 Tahun 2008 Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang

[5] Arrianto Mukti Wibowo,1999, *Kerangka Hukum Digital Signature Dalam Electronic Commerce*, 1999, amwibowo@caplin.cs.ui.ac.id, Hlm. 3

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual.

Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Yang dimaksud dengan sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input, process, output, storage,* dan *communication*. Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelanjaan di Internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit.

Permasalahan yang lebih luas terjadi pada bidang keperdataan karena transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik *(electronic commerce)* telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru di bidang teknologi informasi, media, dan komunikasi.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Kegiatan melalui media sistem elektronik, yang disebut juga *cyber space* atau ruang siber, meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai Orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* antara lain dikenal adanya dokumen elektronik yang kedudukannya disetarakan dengan dokumen yang dibuat di atas kertas. Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan di *cyber space*, yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

Analisis tentang dasar pemikiran informasi elektronik sebagai alat bukti dalam pembuktian keperdataan dan keabsahan *electronic signature* dalam perdagangan dengan menggunakan *electronic commerce* menunjukkan suatu gambaran yang rumit dan holistik. Hal demikian terjadi karena sifat virtual dari transaksi elektronik sehingga sistem jaringan tersebut tidak mengenal batas daerah atau negara dan tanpa kertas serta global. Disisi lain, hukum pembuktian keperdataan di Indonesia memberikan pembatasan terhadap alat-alat bukti yaitu bukti tertulis, saksi, persangkaan, pengakuan dan sumpah di muka hakim.

Alat bukti utama dalam hukum pembuktian keperdataan adalah bukti tertulis yang bagi perdagangan melalui *electronic commerce* menjadi masalah aktual karena *electronic commerce* menggunakan alat yaitu

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

informasi elektronik dan *electronic signature*. Oleh karena itu maka penelitian ini dilakukan dengan menginventarisir, mensistematisasi, menganalisis dan mengevaluasi peraturan perundangan yang menyangkut masalah pembuktian perdata di Indonesia dengan pengembanan hukum atas informasi elektronik dan *electronic signature*. Nampak bahwa ternyata melalui analisis pasal-pasal alat bukti tertulis yang digunakan untuk menjadi dasar keabsahan informasi elektronik dan electronic signature tidaklah mudah karena terdapat multi tafsir. Maka satu-satunya cara yang dilakukan adalah melalui penemuan hukum (*rechtsvinding*) atas bukti tertulis itu dengan pendekatan statute, *comparative*, filosofis.

Dokumen elektronik yang ditandatangani dengan sebuah *digital signature*, dapat dikategorikan sebagai bukti tertulis. Tetapi, terdapat suatu prinsip hukum yang menyebabkan sulitnya pengembangan penggunaan dan dokumen elektronik atau *digital signature*, yakni adanya syarat bahwa dokumen tersebut harus dapat dilihat, dikirim dan disimpan dalam bentuk kertas. Permasalahan akan muncul ketika seseorang hendak melakukan transaksi misalnya saja pembelian barang, maka para pihak sudah mulai dihadapkan pada berbagai permasalahan hukum seperti keabsahan dokumen yang dibuat, tanda tangan digital (*digital signature*) yang dibuat saat orang tersebut menyatakan sepakat untuk bertransaksi, kekuatan mengikat dari kontrak tersebut serta pembatalan transaksi dan sebagainya. Salah satu isu yang *crucial* dalam transaksi *E-commerce* adalah yang menyangkut keamanan dalam mekanisme pembayaran (*payment mechanism*) dan jaminan keamanan dalam bertransaksi *(security risk*) seperti Informasi mengenai transfer data kartu kredit dan identitas pribadi konsumen, yang dalam hal ini ada dua permasalahan utama yaitu:*pertama* mengenai *Identification Integrity* yang menyangkut identitas pengirim yang di kuatkan lewat tanda tangan digital *(digital signature*), *kedua* mengenai *message integrity* yang menyangkut apakah pesan yang dikirimkan oleh pengirim benar-benar diterima oleh penerima yang dikehendaki (*Intended Recipient)*.[6]

[6] Abdul Halim dan Barkatullah Teguh Prasetyo, *Bisnis E-commerce Study System*

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Perjanjian *e-comerce* yang dibuat oleh para pihak yang berkepentingan dalam bentuk dokumen elektronik, bila salah satu pihak melanggar kesepakatan tersebut atau wanprestasi dari salah satu pihak, maka pihak yang dirugikan dapat mengugat ke Pengadilan dengan alat bukti dokumen elektronik. Pada kasus perdata, dalam tahap pembuktian ini para pihak diberikan kesempatan untuk menunjukkan kebenaran terhadap fakta-fakta hukum yang merupakan titik pokok sengketa. Sehingga, hakim yang memeriksa dan memutus perkara akan mendasarkan pada alat bukti yang diajukan oleh para pihak yang bersengketa. Membuktikan adalah upaya untuk mengumpulkan fakta-fakta yang dapat dianalisis dari segi hukum dan berkaitan dengan suatu kasus yang digunakan untuk memberikan keyakinan hakim dalam mengambil keputusan, sedangkan pembuktian adalah proses untuk membuktikan suatu kasus yang disertai dengan fakta-fakta yang dapat dianalisis dari segi hukum untuk memberikan keyakinan hakim dalam mengambil keputusan.

Pada pasal 11 UU.ITE dibahas mengenai Tandatangan elektronik dimana Undang-Undang ini memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, Tanda Tangan Elektronik memiliki kedudukan yang sama dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum. Persyaratan sebagaimana dimaksud dalam Pasal ini merupakan persyaratan minimum yang harus dipenuhi dalam setiap Tanda Tangan Elektronik.

Ketentuan ini membuka kesempatan seluas–luasnya kepada siapa pun untuk mengembangkan metode, teknik, atau proses pembuatan Tanda Tangan Elektronik. Peraturan Pemerintah dimaksud, antara lain, mengatur tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik. Pada Pasal 12 UU.ITE dibahas mengenai siapa yang berhak dan dapat menggunakan tanda tangan elektronik ini. Batasan – batasan untuk keamanan juga diperlukan dalam tanda tangan elektonik ini. Pasal 11 ayat 1 bagian c dan d UU.ITE, mewajibkan adanya metode untuk mengetahui segala perubahan terhadap Tanda Tangan Elektronik yang

---

Keamanan dan Hukum di Indonesia, Pustaka Pelajar, Yogyakarta, 2006, Hlm. 2.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

terjadi setelah waktu penandatanganan dan mengetahui segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan. Perubahan itu dapat diketahui hanya apabila informasi elektronik menjadi data pembuatan tanda tangan elektronik.

Mengenai keabsahan transaksi dan kekuatan pembuktian, transaksi elektronik tidak memerlukan *hard copy* atau *warkat* kertas, namun demikian setiap transaksi yang melibatkan eksekusi diberikan tanda bukti berupa nomor atau kode yang dapat disimpan atau direkam di komputer atau dicetak. Pembuktian isi berkas atau dokumen itu juga dapat dibuktikan, sifat yang ingin dibuktikan adalah sifat *integrity,* sifat ini dapat terjaga dan dibuktikan jika digunakan tandatangan digital *(digital signature*) untuk mengesahkan berkas tersebut, sebab dengan *digital signature*, perubahan satu huruf saja dalam isi berkas akan dapat menunjukan bahwa berkas sudah berubah meskipun tidak ditunjukan bagian mana yang berubah. Dengan pengertian informasi elektronik yang mencakup spektrum luas menjadi hal yang essensial dalam kegiatan virtual terutama kegiatan *E- commerce*. Maka informasi elektronik sebagai alat bukti dalam hukum pembuktian keperdataan menjadi penting karena menyangkut identitas subyek, substansi informasi, metodologi fiksasi dan media penyimpanan yang membuat informasi menjadi jelas untuk diketahui. Bagaimana dengan tanda tangan asli serta informasi yang ditanda tangani di kertas diubah ke data elektronik dengan peralatan scanner, apakah memiliki kekuatan hukum dan akibat hukum yang sah? Tentu tidak memiliki kekuatan hukum dan akibat hukum yang sah, karena tanda tangan itu tidak dibuat berdasarkan informasi yang disepakati atau dengan kata lain informasi yang disepakati tidak menjadi data pembuatan tangan tangan, sehingga perubahan tanda tangan elektronik dan/atau informasi elektronik setelah waktu penandatanganan tidak dapat diketahui. Berdasarkan latar belakang masalah tersebut, maka penulis ingin meneliti dan menyusun tesis yang berjudul : "**KEABSAHAN TANDA TANGAN ELEKTRONIK SEBAGAI ALAT BUKTI YANG SAH DITINJAU**

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

DALAM HUKUM ACARA PERDATA".

1.2. Pokok Permasalahan

Berdasarkan latar belakang permasalahan yang telah diuraikan di atas, maka terdapat beberapa pokok permasalahan yang dapat dirumuskan, yakni:

a. Bagaimanakah kedudukan dan kekuatan hukum dari tanda tangan elektronik sebagai alat bukti?

b. Bagaimanakah tanggapan yang timbul mengenai keabsahan tanda tangan elektronik sebagai bukti?

1.3. Metode Penelitian

Setiap kegiatan ilmiah untuk lebih terarah, akurat dan rasional sehingga sesuai dengan kriteria keilmuan dan dapat dipertanggung jawabkan keobyektifannya, diperlukan suatu metode yang sesuai dengan obyek yang dibicarakan. Karena penelitian hukum bertujuan untuk memberikan kemampuan dan ketrampilan untuk mengungkapkan kebenaran, melalui kegiatan-kegiatan yang sistematis, metodelogis dan konsisten.[7]

Dalam penulisan ini, bentuk penelitian hukum yang digunakan adalah dengan penelitian hukum normatif atau penelitian hukum kepustakaan.

Penelitian kepustakaan yaitu, penelitian yang menekankan pada penggunaan data sekunder atau berupa norma hukum tertulis dan atau wawancara dengan informan serta narasumber.[8]

Dengan metode-metode pengumpulan data tersebut di atas, diharapkan dapat memberikan titik terang untuk sedikit megetahui dan

---

[7] Soerjono Soekanto, *Pengantar Penelitian Hukum*, (Jakarta : Penerbit Universitas Indonesia, 2007), hlm. 46.

[8] Dian Puji N. Simatupang, "*Proposal Penelitian (Thesis), Bahan Perkuliahan Metode Penelitian Hukum Universitas Indonesia Fakultas Hukum Program Magister Kenotariatan,*" (makalah disampaikan pada perkuliahan, Depok, 13 Maret 2009), hlm. 8.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

memecahkan permasalahan yang ada. Dari hasil penelitian itu dipilah-pilah dan akhirnya menjadi suatu kesimpulan yang teratur, lengkap dan sistematis dalam bentuk laporan penelitian data primer dan data sekunder. Data primer diperoleh langsung dari sumber pertama di lapangan melalui penelitian, yaitu dari mencakup dokumen-dokumen resmi, buku-buku, hasil-hasil penelitian yang bewujud laporan, buku harian dan seterusnya.[9]

Sedangkan metode analisis data yang dipergunakan dalam penelitian ini adalah studi dokumen kualitatif, yaitu tidak mementingkan kuantitas tetapi kualitas dari data-data yang dipergunakan. Studi dokumen kualitatif tersebut, mempergunakan data sekunder yang berasal dari kepustakaan.

Ronny Hanitijo Soemitro membagi jenis dan sumber data atas data primer dan data sekunder. Data primer adalah data yang diperoleh langsung dari masyarakat. Sedangkan data sekunder yaitu data yang diperoleh dari bahan kepustakaan dengan membaca dan mengkaji bahan-bahan-bahan kepustakaan. Data sekunder dalam penelitian hukum terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tertier.

Bahan hukum primer berupa : norma dasar Pancasila, UUD 1945, Undang-undang, Yuriprudensi dan Traktat dan berbagai peraturan perundang-perundangan sebagai peraturan organiknya. Bahan hukum sekunder berupa : Rancangan peraturan perundang-undangan, buku-buku hasil karya para sarjana dan hasil-hasil penelitian sebelumnya yang berkaitan dengan masalah yang diteliti. Dan bahan hukum tertier berupa bibliolografi dan indeks komulatif.[10]

1.3.1 Bahan-bahan hukum primer yaitu bahan hukum yang bersifat mengikat yang terdiri dari :

1. Kitab Undang-undang Hukum Perdata.
2. Kitab Undang-Undang Hukum Pidana.
3. Kitab Undang-Undang Hukum Acara Pidana.

---

[9] Soeryono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Raja Grafindo, Jakarta, 1998, hlm 12.

[10] Ronny Hanitijo Soemitro, *Metode Penelitian Hukum*, Ghalia Indonesia, Jakarta, 1982, hlm. 52 - 53.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

4. Undang-Undang Nomor 1 Tahun 1995 tentang Perseroan Terbatas.
5. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.
6. Undang-Undang Nomor 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa
7. Undang-Undang Nomor 30 tahun 2004 tentang Jabatan Notaris.
8. Undang-Undang Nomor 30 Tahun 2009 tentang Perlindungan Konsumen.
9. Peraturan Pemerintah Nomor 26 Tahun 1998 tentang Pemakaian Nama Perseroan Terbatas.
10. Undang-Undang Nomor 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik.

1.3.2 Bahan hukum sekunder yaitu bahan hukum yang memberikan penjelasan mengenai bahan hukum primer yang terdiri dari :

1. Rancangan Undang-Undang Perseroan Terbatas.
2. Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik (ITE).
3. Buku pedoman penggunaan Sisminbakum.
4. Website Sisminbakum.
5. Hasil-hasil penelitian, hasil seminar, hakis karya dari kalangan hukum dan lain- lain.

1.3.3 Bahan hukum tersier

Bahan yang memberikan petunjuk dan penjelasan terhadap bahan hukum primer dalam bentuk ensiklopedia, majalah, artikel-artikel, surat kabar dan jurnal-jurnal hukum.

Dengan metode-metode pengumpulan data tersebut di atas, diharapkan dapat memberikan titik terang untuk sedikit megetahui dan memecahkan permasalahan yang ada. Dari hasil penelitian itu dipilah-pilah dan akhirnya menjadi suatu kesimpulan yang teratur, lengkap dan sistematis dalam bentuk laporan penelitian.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

1.4 Sistematika Penulisan

Judul tesis ini adalah **Keabsahan Tanda Tangan Elektronik Sebagai Alat Bukti Yang Sah Ditinjau Dalam Hukum Acara Perdata**.

Sistematika penulisan dalam tesis ini terdiri dari tiga bab dan tiap bab dibagi menjadi beberapa sub bab. Adapun sistematika setiap bab adalah sebagai berikut:

Bab I Pendahuluan

Dalam bab ini berisikan antara lain mengenai latar belakang masalah, pokok permasalahan, metode penelitian dan sistematika penulisan.

Bab II Tinjauan Pustaka, Analisa dan Pembahasan

Dalam bab ini berisikan antara lain mengenai Tinjauan Teori Mengenai Keabsahan Tanda Tangan Elektronik, Kekuatan hukum dan keabsahan tanda tangan elektronik sebagai alat bukti, Pembuktian hukum perdata di Indonesia, Penggunaan dan pelaksanaan dan kekuataan bukti elektronik dalam perkara perdata di Indonesia.

BAB III Penutup

Pada bab terakhir ini, penulis akan menyajikan suatu kesimpulan dan saran dari segala penguraian dan pembahasan dari seluruh isi judul tesis tersebut.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

B A B II
TINJAUAN PUSTAKA
KEABSAHAN TANDA TANGAN ELEKTRONIK SEBAGAI ALAT BUKTI YANG SAH DITINJAU DALAM HUKUM ACARA PERDATA

2.1 Tinjauan Teori Mengenai Keabsahan Tanda Tangan Elektronik.

2.1.1. Pengertian Tanda Tangan.

Penggunaan tanda tangan adalah suatu kebiasaan formil yang digunakan untuk menyatakan persetujuan seseorang sekaligus memastikan identitas (*authentification*) orang tersebut yang bertanda tangan untuk sesuatu baik yang berimplikasi hukum maupun yang tidak.

Menurut Tan Thong Kie, tanda tangan adalah suatu pernyataan kemauan pembuat tanda tangan (penanda tanganan), bahwa ia dengan membubuhkan tanda tangannya di bawah suatu tulisan menghendaki agar tulisan itu dalam hukum dianggap sebagai tulisanya sendiri.[11] Pengertian tanda tangan dalam arti umum, adalah tanda tangan yang dapat didefinisikan sebagai suatu susunan (huruf) tanda berupa tulisan dari yang menandatangani, dengan mana orang yang membuat pernyataan atau keterangan tersebut dapat di individualisasikan.[12]

Definisi tersebut mencakup suatu anggapan, bahwa pada pernyataan yang dibuat secara tertulis harus dibubuhkan tanda tangan dari yang bersangkutan. Menurut American Bar Association (ABA), pengertian tanda tangan dapat berupa tanda apapun yang dibuat dengan tujuan untuk memberikan persetujuan dan otentifikasi terhadap suatu dokumen tersebut.[13]

---

[11] Tan Thong Kie, *Studi Notariat dan Serba-Serbi Praktek Notaris*, PT. Ichtiar Baru Van Hoeve, Jakarta, 2007, Hlm. 473

[12] Herlien Budiono, *Kumpulan Tulisan Hukum Perdata Di Bidang Kenotariatan*, PT.Citra Aditya Bakti, Bandung, 2007, Hlm. 220

[13] Information Security Committee, Section of Science & Technology – American Bar Association, Digital Signature Guideliness (United States, American Bar Association: 1996), hlm. 4. Pengertian dari otentifikasi menurut ABA adalah "*authentication is generally the process used to confirm the identity of a person or to prove the integrity of xpecific information. More specifically, in the case of a message, authentication involves determining its source and providing assurance that the message has not been modified or replaced in transit. The historical legal concept of signature is broader. It recognizes any mark made with the intention of authenticating the marked document*".

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Pengertian dari tanda tangan sekarang ini merujuk kepada tanda tangan tertulis seseorang di atas kertas atau yg dapat disamakan dengan itu. Inti dari tanda tangan difokuskan pada pengertian dasar tersebut. Menurut Kamus Besar Bahasa Indonesia, pengertian tanda tangan itu sendiri adalah tanda sebagai lambing nama yang dituliskan dengan tangan oleh orang itu sendiri sebagai penanda pribadi (telah menerima). Jika dilihat daripengertian tersebut, pengertian tanda tangan belum tentu merujuk kepada suatu tanda tangan secara "tertulis" tetapi justru terhadap suatu penandaan, dimana tanda tersebut dapat merujuk kepada bertanda tangan itu. Penggunaan tanda tangan adalah suatu kebiasaan formil yang digunakan untuk menyatakan persetujuan seseorang sekaligus memastikan identitas (*authentification*) orang tersebut yang bertanda tangan untuk sesuatu yang baik yang berimplikasi hukum maupun yang tidak.

2.1.2. Pengertian Tanda Tangan Elektronik.

Pengertian tanda tangan elektronik, berdasarkan pada Pasal 1 ayat (12) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah sebagai berikut : "Tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi". Penanda tangan adalah subjek hukum yang terasosiasi atau terkait dengan tanda tangan elektronik. Definisi tersebut mencakup suatu anggapan, bahwa pada pernyataan yang dibuat secara tertulis harus dibubuhkan tanda tangan dari yang bersangkutan. *Digital signature,* adalah sebuah pengaman pada data digital yang dibuat dengan kunci tanda tangan pribadi (*private signature key*), yang penggunaannya tergantung pada kunci publik (*public key*) yang menjadi pasangannya.[14] Menurut Julius Indra Dwiparyo, tanda tangan elektronik, adalah sebuah identitas elektronik yang berfungsi sebagai tanda persetujuan terhadap kewajiban-kewajiban yang melekat pada sebuah akta elektronik.[15]

[14] Din Mudiardjo, 2008, *Telekomunikasi Dan Teknologi Hukum E-commerce (grattan),* www.google.com

[15] Julius Indra Dwipayono, 2005, *Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia,* www.legalitas.org.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Informasi elektronik yang menggunakan jaringan publik, bisa saja seseorang berniat jahat mengganti informasi elektronik yang telah ditandatangani oleh para pihak dengan informasi elektronik lain tetapi tanda tangan tidak berubah. Pada data elektronik perubahan ini mudah terjadi dan tidak mudah dikenali. Oleh karena itu, tanda tangan elektronik harus terasosiasi dengan informasi elektronik. Terasosiasi adalah informasi elektronik yang ingin ditandatangani menjadi data pembuatan tanda tangan elektronik, dengan demikian, antara tanda tangan elektronik dan informasi elektronik yang ditandatangani menjadi erat hubungannya seperti fungsi kertas. Keuntungannya adalah jika terjadi perubahan informasi elektronik yang sudah ditandatangani maka tentu tanda tangan elektronik juga berubah.[16]

Tanda tangan elektronik bukan tanda tangan yang dibubuhkan di atas kertas sebagaimana lazimnya suatu tanda tangan, tanda tangan elektronik diperoleh dengan terlebih dahulu meciptakan suatu *message digest* atau *hast*, yaitu mathematical summary dokumen yang dikirimkan melalui *cyberspace*.[17] Tanda tangan elektronik pada prinsipnya berkenaan dengan jaminan untuk message integrity yang menjamin bahwa si pengirim pesan (sender) adalah benar-benar orang yang berhak dan bertanggung jawab untuk itu. Hal ini berbeda dari tanda tangan biasa yang berfungsi sebagai pengakuan dan penerimaan atas isi pesan atau dokumen. Tanda tangan elektronik adalah sebuah item data yang berhubungan dengan sebuah pengkodean pesan digital yang dimaksudkan untuk memberikan kepastian tentang keaslian data dan memastikan bahwa data tidak termodifikasi.[18] Persoalan hukum yang muncul sekitar hal ini antara lain berkenaan dengan fungsi dan kekuatan hukum tanda tangan elektronik. Di USA saat ini telah ditetapkan satu undang-undang yang secara formal mengakui keabsahan tanda tangan elektronik. Pengaturan di

[16] Ronny, *Sembilan Peraturan Pemerintah Dan Dua Lembaga Yang Baru Undang-Undang Informasi Transaksi Elektronik*, www.ronny-hukum.blogspot.com, 2008, Hlm. 3

[17] Soemarno Partodihardjo, *Tanya Jawab Sekitar Undang-Undang No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*, PT Gramedia Pustaka Utama, Jakarta, 2009, Hlm. 20.

[18] *Ibid.*, Hlm. 21.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

tingkat internasional diatur dalam Pasal 7 UNICITRAL Model Law (The United Nations Commissions on International Trade Law) merupakan salah satu organisasi internasional yang pertama kali mulai membahas mengenai perkembangan telematika informatika dan dampaknya terhadap perkembangan elektronik.

Tujuan Tanda Tangan Digital, tujuan dari suatu tanda tangan dalam suatu dokumen elektronik adalah sebagai berikut :

1. Untuk memastikan otensitas dari dokumen tersebut;
2. Untuk menerima atau menyetujui secara menyakinkan isi dari sebuah tulisan.

Sifat persyaratan *digital signature* atau tanda tangan elektronik, yaitu :[19]

1. Autentik.
2. Aman.
3. Interoperabilitas dari perangkat lunak maupun jaringan dari penyedia jasa.
4. Konfidensialitas.
5. Hanya sah untuk dokumen itu saja atau kopinya yang sama persis.
6. Dapat diperiksa dengan mudah.
7. Divisibilitas, berkaitan dengan spesifikasi praktis transaksi baik untuk volume besar atau skala kecil.

Sedangkan Manfaat Tanda Tangan Digital (*Digital Signature*) adalah suatu tanda tangan digital (*digital Signature*) akan menyebabkan data elektronik yang dikirimkan melalui *open network* tersebut menjadi terjamin, sehingga mempunyai manfaat dari *digital signature* adalah sebagai berikut:[20]

1. *Authenticity*

Dengan memberikan *digital signature* pada data elektronik yang dikirimkan, maka akan dapat atau bisa ditunjukkan darimana data-data elektronik tersebut sesungguhnya berasal. Terjaminnya integritas pesan

[19] *Loc.cit*, Hlm. 91-92.
[20] Arrianto Mukti Wibowo, dkk, *Op.Cit*., Hlm. 5.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

tersebut bisa terjadi, karena keberadaan dari *digital certificate*. *Digital Certificate* diperoleh, atas dasar aplikasi kepada *Certification Authority oleh user atau subscriber*. *Digital Certificate* berisi informasi mengenai pengguna antara lain:

1. Identitas
2. Kewenangan
3. Kedudukan hukum
4. Status dari *user* atau pengguna

Digital certificate ini memiliki berbagai tingkatan atau *level*, tingkatan dari *digital certificate* ini menentukan berapa besar kewenangan yang dimiliki oleh pengguna. Contoh dari kewenangan atau kwalifikasi ini adalah apabila suatu perusahan hendak melakukan perbuatan hukum, maka pihak yang berwenang mewakili perusahaan tersebut adalah direksi. Jadi apabila suatu perusahaan hendak melakukan suatu perbuatan hukum maka *digital certificate* yang dipergunakan adalah *digital certificate* yang dipunyai oleh direksi perusahaan tersebut.

Dengan keberadaan dari *digital certificate* ini maka pihak ketiga yang berhubungan dengan pemegang *digital certificate* tersebut dapat merasa yakin bahwa suatu pesan adalah benar berasal dari pengguna tersebut.

2. *Integrity*

Penggunaan *digital signature* yang diaplikasikan pada pesan atau data elektronik yang dikirimkan, dapat menjamin bahwa pesan atau data elektronik tersebut tidak mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang.

Integritas atau *integrity* berhubungan dengan masalah keutuhan dari suatu data yang dikirimkan. Seorang penerima pesan atau data dapat merasa yakin apakah pesan yang diterimanya sama dengan pesan yang dikirimkan. Ia dapat merasa yakin bahwa data tersebut pernah dimodifikasi atau diubah selama proses pengiriman atau penyimpanan. Jaminan *authenticity* ini dapat dilihat dari adanya *hash function* dalam sistem *digital signature*, dimana penerima data (*recipient*) dapat

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

melakukan pembandingan *hash value*. Apabila *hash value*-nya sama dan sesuai, maka data tersebut benar-benar otentik, tidak pernah terjadi suatu tindakan yang sifatnya merubah (*modify*) dari data tersebut pada saat proses pengiriman, sehingga terjamin *authenticity*-nya. Sebaliknya apabila *hash value*-nya berbeda, maka patut dicurigai dan langsung dapat disimpulkan bahwa recipient menerima data yang telah dimodifikasi.

3. *Non-Repudiation* (Tidak Dapat Disangkal Keberadaannya)

Non-Repudiation (Tidak Dapat Disangkal Keberadaannya), timbul dari keberadaan *digital signature* yang menggunakan enkripsi asimetris (*asymmetric encryption*). *Enskripsi asimetris* ini melibatkan keberadaan dari kunci privat dan kunci publik. Suatu pesan yang telah dienkripsi dengan menggunakan kunci privat, maka ia hanya dapat dibuka/dekripsi dengan menggunakan kunci publik dari pengirim. Jadi apabila terdapat suatu pesan yang telah dienkripsi oleh pengirim dengan menggunakan kunci privatnya, maka ia tidak dapat menyangkal keberadaan pesan tersebut, karena terbukti bahwa pesan tersebut didekripsi dengan kunci publik pengirim. Keutuhan dari pesan tersebut dapat dilihat dari keberadaan *hash function* dari pesan tersebut, dengan catatan bahwa data yang telah di-sign akan dimasukkan ke dalam digital *envelope*.

Non-repudiation (Tidak dapat disangkalnya keberadaan) suatu pesan berhubungan dengan orang yang mengirimkan pesan tersebut. Pengirim pesan tidak dapat menyangkal bahwa ia telah mengirimkan suatu pesan apabila ia sudah mengirimkan suatu pesan. Ia juga tidak dapat menyangkal isi dari suatu pesan bebeda dengan apa yang ia kirimkan apabila ia telah mengirim pesan tersebut. Non repudiation adalah hal yang sangat penting bagi *e-commerce* apabila suatu transaksi dilakukan melalui suatu jaringan internet, kontrak elektronik (*electronic contracts*), ataupun transaksi pembayaran.

4. *Confidentiality*

Pesan dalam bentuk data elektronik yang dikirimkan tersebut bersifat rahasia atau *confidental*, sehingga tidak semua orang dapat mengetahui isi data elektronik yang telah *disign* dan dimasukkan dalam

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

digital envolve. Keberadaan *digital envolve* yang termasuk bagian yang integral dari *digital signature*, menyebabkan suatu pesan yang telah dienkripsi hanya dapat dibuka oleh orang yang berhak. Tingkat kerahasiaan dari suatu pesan yang telah dienkripsi ini, tergantung dari panjang kunci atau *key* yang dipakai untuk melakukan enkripsi.

Pengamanan data dalam *e-commerce* dengan metode kriptografi melalui skema digital signature tersebut secara teknis sudah dapat diterima dan diterapkan, namun apabila kita bahas dari sudut pandang ilmu hukum ternyata masih kurang mendapatkan perhatian. Kurangnya perhatian dari ilmu hukum dapat dimengerti karena, khususnya di Indonesia, penggunaan komputer sebagai alat komunikasi melalui jaringan internet baru dikenal semenjak tahun 1994. Dengan demikian pengamanan jaringan internet dengan metode digital signature di Indonesia tentu masih merupakan hal yang baru bagi kalangan pengguna komputer.

2.1.3. Klasifikasi Tanda Tangan Elektronik

1. Tanda Tangan Elektronik (Biasa)

Tanda tangan elektronik biasa, sesuai dengan pengertian mengenai tanda tangan elektronik diatas adalah tanda tangan yang ditujukan merujuk kepada si penanda tangan, yang dilakukan dengan media elektronik. Contoh paling mudah adalah suatu tanda tangan konvensional (tertulis) yang kemudian di-*scan*. Kemudian hasil *scan* tersebut akan menjadi suatu informasi elektronik, biasanya berupa suatu file gambar, ditempelkan (paste) pada suatu dokumen elektronik. Hal tersebut sudah termasuk dalam ruang lingkup tanda tangan elektronik (biasa).

2. Tanda Tangan Elektronik yang Aman (*Secure* atau *Reliable*)

Tanda tangan elektronik yang aman atau Electronic Signature, merupakan suatu tanda tangan elektronik yang harus memenuhi persyaratan-persyaratan tertentu, sehingga dapat dalam konteks kesamaanya, dapat dipersamakan dengan tanda tangan konvensional. Tanda tangan elektronik yang aman ini diperuntukkan untuk menampung semua jenis kemajuan teknologi yang mungkin berkembang dalam bidang

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

keamanan terhadap informasi elektronik yang aman ditujukan untuk tidak hanya dapat merujuk kepada si penanda tangan, tetapi juga untuk menjaga keutuhan dan keamanan daripada suatu informasi elektronik yang dilekatkan. Tanda tangan digital termasuk di dalam kategori tanda tangan elektronik yang aman.

2.1.4. Dokumen Elektronik

Dokumen elektronik berdasarkan pada pasal 1 ayat 4 Undang-Undang Nomor 11 Tahun 2008 adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, atau sejenisnya, huruf, tanda, angka, kode akses, symbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu memahaminya. Dokumen elektronik dapat dijadikan alat bukti yang sah, menurut Undang-undang Informasi dan Transaksi Elektronik, suatu dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan sistem elektronik yang andal dan aman, serta memenuhi persyaratan minimum sebagai berikut :

a. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;
b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan system elektronik tersebut;
c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggung-jawaban prosedur atau petunjuk.

Dokumen elektronik merupakan dokumen yang terjadi akibat suatu transaksi komersial elektronik (e-*commerce*). Untuk menentukan kapan terjadinya kesepakatan dalam suatu transaksi komersial elektonik (*e-commrce*). Hasil print out dari sebuah dokumen elektronik yang dihasilkan dalam pertukaran informasi, selayaknya memiliki nilai pembuktian yang sama seperti bukti tulisan lainnya. Dalam memutus suatu perkara, tentu saja hakim harus mendasarkan ketentuan hukum acara yang mengatur masalah pembuktian.

2.1.5. Transaksi Komersial Elektronik (*E-Commerce*)

1. Pengertian Transaksi Komersial Elektronik (*E-Commerce*)

Transaksi komersial elektronik (*e-Commerce*), merupakan salah satu bentuk bisnis modern yang bersifat non-face dan non-sign (tanpa bertatap muka dan tanpa tanda tangan). Transaksi komersial elektronik (*e-commerce*) memiliki beberapa ciri khusus, diantaranya bahwa transaksi ini bersifat paperless (tanpa dokumen tertulis), *borderless* (tanpa batas geografis) dan para pihak yang melakukan transaksi tidak perlu bertatap muka. Transaksi komersial elektronik (*e-commerce*), mengacu kepada semua bentuk transaksi komersial yang didasarkan pada proses elektronis dan transmisi data melalui media elektronik. Karena itu, tidak ada definisi konsep transaksi komersial elektronik yang berlaku Internasional.

Hal serupa juga dikemukakan oleh UNCITRAL yang mendefinisikan *e-commerce* sebagai berikut : "*Electronic commerce*. Which involves the use of alternatives to paper-based of communication and storage of information".[21] Vladimir Zwass, mendefinisikan transaksi komersial elektronik (*e-commerce*) sebagai pertukaran informasi bisnis, mempertahankan hubungan bisnis dan melalukan transaksi bisnis melalui

[21] Ridwan Khairandy, 2001, *Pembaharuan Hukum Kontrak Sebagai Antisipasi Transaksi Elektronic Commerce "become a popular prefixs for other terms associated with electronic Transaction"* , Jurnal Hukum Bisnis, vol.16, Hlm. 57.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

jaringan komunikasi.[22] Mengamati hal tersebut, transaksi komersial elektronik (*e-commerce*) adalah transaksi perdagangan jual beli barang dan jasa yang dilakukan dengan cara pertukaran informasi atau data menggunakan alternatif selain media tertulis, yang dimaksud media transaksi di sini adalah media elektronik, khususnya internet.

Transaksi Elektronik berdasarkan pada Pasal 1 ayat (9) Undang-Undang Nomor 11 tahun 2008 tentang Informasi Transaksi Elektronik menyebutkan : Transaksi elektronik, adalah hubungan hukum yang dilakukan melalui komputer, atau media elektronik lainnya. Berdasarkan berbagai definisi tersebut, terdapat beberapa kesamaan yaitu :

1. Terdapat transaksi antara dua pihak atau lebih;
2. Ada pertukaran barang dan jasa;
3. Menggunakan internet sebagai medium utama untuk melakukan transaksi.

Transaksi komersial elektronik (*e-commerce*), pada prinsipnya merupakan hubungan hukum berupa pertukaran barang dan jasa antara penjual dan pembeli yang memiliki prinsip dasar sama dengan transaksi konvensional, namun dilaksanakan dengan pertukaran data melalui media yang tidak berwujud (internet), di mana para pihak tidak perlu bertatap muka secara fisik.

2. Jenis Transaksi Komersial Elektronik (*E-commerce*)

Secara garis besar jenis transaksi komersial elektronik (*e-commerce*) dibagi menjadi 5, yaitu:[23]

a. *Business to Business* (B2B)

Transaksi B2B merupakan transaksi, di mana kedua belah pihak yang melakukan transaksi adalah suatu perusahaan.

b. *Busines to Consumer* (B2C)

Transaksi B2C, merupakan transaksi antara perusahaan dengan konsumen atau individu. Transaksi B2C meliputi pembelian

[22] *Ibid*, Hlm. 65.
[23] Roberto Aaron, 1999, *Electronic commerce :Enablers and Implications*, IEEE Communication Magazine, Hlm. 47.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

produk secara langsung oleh konsumen melalui internet.

c. *Customer to Customer* (C2C)

Transaksi C2C merupakan transaksi, di mana individu saling menjual barang satu sama lain.

d. *Costumer to Business* (C2B)

Transaksi C2B, merupakan transaksi yang memungkinkan individu menjual barang pada perusahaan.

e. *Customer to Government* (C2G)

Transaksi C2G merupakan transaksi, di mana individu dapat melakukan transaksi dengan pemerintah.

2.1.6 Sertifikat Elektronik

Sertifikat elektronik menduduki peran layaknya "paspor elektronik", ia tidak dapat dipisahkan dari praktek tanda tangan elektronik, ia membawa kekuatan hukum yang kuat karena dapat meyakinkan identitas Penandatangan.[24] Sertifikat elektronik mempunyai sebuah struktur internal, artinya ada beberapa bagian yang diwajibkan untuk diinformasikan atau dilekatkan pada sertifikat tersebut untuk memberikan kekuatan hukum pada sertifikat tersebut.

Penyelenggaraan Sertifikasi Elektronik menurut Pasal 13 dan 14 UU.ITE, yaitu :

1. Setiap orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan tanda tangan elektronik.
2. Penyelenggara Sertifikasi Elektronik harus memastikan suatu tanda tangan elektronik dengan pemiliknya.
3. Penyelenggara Sertifikasi Elektronik terdiri atas Penyelenggara Sertifikasi Elektronik Indonesia dan Penyelenggara Sertifikat Elektronik Asing.
4. Penyelenggara Sertifikasi Indonesia berbadan hukum Indonesia

[24] Julien ESNAULT, *Memoire : la signature électronique, D.E.S.S. du droit du Multimédia et de l'Informatique, Université de Paris II Pantheon-Assas*, Paris, Année universitaire 2002-2003, h. 11. www.legalitas.org

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

dan berdomisili di Indonesia.

5. Penyelenggara Sertifikasi Elektronik Asing yang beroperasi di Indonesia harus terdaftar di Indonesia.
6. Ketentuan lenih lanjut mengenai Penyelenggara Sertifikasi Elektronik diatur dengan Peraturan Pemerintah (PP).

Penyelenggara Sertifikasi Elektronik harus menyediakan informasi yang akurat jelas, dan pasti kepada setiap pengguna jasa, yang meliputi :

1. Metode yang digunakan untuk mengidentifikasikan Penanda Tangan.
2. Hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik.
3. Hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

Penjelasannya adalah informasi yang minimum harus dipenuhi oleh setiap penyelenggara Tanda Tangan Elektronik.

2.1.7 *Certification Authority (CA)*

C.A berkedudukan sebagai pihak ketiga yang dipercaya untuk memberikan kepastian atau pengesahan terhadap identitas dari seseorang atau pelanggan (klien C.A. tersebut). Selain itu C.A. juga mengesahkan pasangan kunci publik dan kunci privat milik orang tersebut. Proses sertifikasi untuk mendapatkan pengesahan dari C.A. dapat dibagi menjadi 3 tahap :

1. Pelanggan atau subscriber membuat sendiri pasangan kunci privat dan kunci publiknya dengan menggunakan software yang ada di dalam komputernya
2. Menunjukan bukti-bukti identitas dirinya sesuai dengan yang disyaratkan C.A.
3. Membuktikan bahwa dia mempunyai kunci privat yang dapat dipasangkan dengan kunci publik tanpa harus memperlihatkan kunci privatnya.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Tahapan-tahapan tersebut tidak mutlak harus seperti di atas, akan tetapi tergantung pada ketentuan-ketentuan yang telah ditetapkan oleh C.A. itu sendiri. Hal ini berkaitan dengan level atau tingkatan dari sertifikat yang diterbitkannya dan level atau tingkatan ini berkaitan juga dengan besarnya kewenangan yang diperoleh pelanggan "Subscriber" berdasarkan sertifikat yang didapatkannya. Semakin besar kewenangannya yang diperoleh dari suatu Digital Certificate yang diterbitkan oleh C.A. semakin tinggi pula level sertifikat yang diperoleh serta semakin ketat pula persyaratan yang ditetapkan oleh C.A. Sebagai contoh; untuk mendapatkan suatu sertifikat yang mempunyai level kewenangan yang cukup tinggi, terkadang C.A. bahkan memerlukan kehadiran secara fisik si "subscriber" sehingga C.A. dapat memperoleh kepastian pihak yang akan memperoleh sertifikat tersebut.

Setelah persyaratan-persyaratan tersebut diuji keabsahannya maka C.A. menerbitkan sertifikat pengesahan (dapat berbentuk hard-copy maupun soft-copy). Sebelum diumumkan secara luas "subscriber" terlebih dahulu mempunyai hak untuk melihat apakah informasi-informasi yang ada pada sertifikat tersebut telah sesuai atau belum. Apabila informasi-informasi tersebut telah sesuai maka subscriber dapat mengumumkan sertifikat tersebut secara luas atau tindakan tersebut dapat diwakilkan kepada C.A. atau suatu badan lain yang berwenang untuk itu (suatu lembaga notariat). Selain untuk memenuhi sifat integrity dan authenticity dari sertifikat tersebut, C.A. akan membubuhkan digital signature miliknya pada sertifikat tersebut.[25]

Informasi-informasi yang terdapat di dalam sertifikat tersebut diantaranya dapat berupa :

1. Identitas C.A. yang menerbitkannya.
2. Pemegang atau pemilik atau subscriber dari sertifikat tersebut.
3. Batas waktu keberlakuan sertifikat tersebut.
4. Kunci publik dari pemilik sertifikat.

Setelah sertifikat tersebut diumumkan maka pihak-pihak lain dapat

[25] *http://en.wikipedia.org/wiki/Public_key_infrastructure*, diakses tanggal 20 Juli 2006

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

melakukan transaksi, transfer pesan dan berbagai kegiatan dengan media internet secara aman dengan pihak pemilik sertifikat.

Fungsi C.A.

Fungsi-fungsi C.A yang telah kita bicarakan di atas dapat kita golongkan sebagai berikut :

1. Membentuk hierarki bagi penandatanganan digital.
2. Mengumumkan peraturan-peraturan mengenai penerbitan sertifikat.
3. Menerima dan memeriksa pendaftaran yang diajukan.

Selain itu, pihak-pihak yang terlibat dalam e-commerce tidak hanya dilihat pada statusnya sebagai pihak, melainkan juga dengan melihat kedudukannya dalam perikatan, yaitu sebagai berikut:

1. Penjual (merchant)
2. Pembeli (buyer)
3. Certification Authority (CA)
4. Account Issuer (penerbit rekening contoh: kartu kredit)
5. Jaringan pembayaran (contohnya Visa dan Mastercard dalam *scheme* SET)
6. Internet Service Provider (ISP)
7. Internet Backbones
8. Aspek Kontrak Perdagangan Internasional

2.1.8. Keabsahan Tanda Tangan Elektronik

Konsep “tanda tangan digital” (*digital signature*) yang dikenal pada dunia keamanan komputer adalah hasil dari penerapan teknik-teknik komputer pada suatu informasi. Sedangkan di dunia umum, tanda tangan mempunyai arti yang lebih luas, yaitu sebarang tanda yang dibuat dengan maksud untuk melegalisasi dokumen yang ditandatangani. Dalam dunia nyata, untuk menjamin keaslian serta legalitas suatu dokumen digunakan tanda tangan. Tanda tangan ini merupakan suatu tanda yang bersifat unik milik seseorang dan digunakan untuk memberi pengesahan bahwa orang tersebut setuju dan mengakui isi dari dokumen yang ditandatangani. Untuk dokumen-dokumen elektronik pun dibutuhkan hal semacam ini. Oleh

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

karena itu, diciptakan suatu sistem otentikasi yang disebut tanda tangan digital. Tanda tangan digital merupakan suatu cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut. Tanda tangan digital menggunakan algoritma-algoritma serta teknik-teknik komputer khusus dalam penerapannya.

Berbicara mengenai keabsahan tanda tangan elektronik, suatu tanda tangan elektronik pasti diperoleh dengan adanya suatu transaksi, orang selalu akan mendasarkan pada ketentuan dalam Pasal 1320 Kitab Undang-undang Hukum Perdata yang menyatakan bahwa untuk sahnya suatu perjanjian diperlukan 4 (empat) syarat, yakni:

1. Sepakat mereka yang mengikatkan dirinya;
2. Cakap untuk membuat suatu perikatan;
3. Hal tertentu;
4. Sebab yang halal.

Dengan mendasarkan pada ketentuan Pasal 1320 KUHPerdata sebenarnya tidak dipermasalahkan mengenai media yang digunakan dalam transaksi, atau dengan kata lain Pasal 1320 KUHPerdata tidak mensyaratkan bentuk dan jenis media yang digunakan dalam bertransaksi. Oleh karena itu, dapat saja dilakukan secara langsung maupun secara elektronik. Namun suatu perjanjian dapat dikatakan sah bila telah memenuhi unsur-unsur sebagaimana dimaksud dalam Pasal 1320 tersebut. Demikian pula asas kebebasan berkontrak yang dianut KUHPerdata, dimana para pihak dapat bebas menentukan dan membuat suatu perikatan atau perjanjian dalam bertransaksi yang dilakukan dengan itikat baik (PasaL 1338). Jadi apapun bentuk dan media dari kesepakatan tersebut, tetap berlaku dan mengikat para pihak karena perikatan tersebut merupakan undang-undang bagi yang membuatnya. Permasalahan akan timbul dari suatu transaksi bila salah satu pihak ingkar janji. Penyelesaian permasalahan yang terjadi tersebut, selalu berkaitan dengan apa yang menjadi bukti dalam transaksi, lebih-lebih bila transaksi menggunakan

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

sarana elektronik. Hal ini karena penggunaan dokumen atau data elektronik sebagai akibat transaksi melalui media elektronik, belum secara khusus diatur dalam hukum acara yang berlaku, baik dalam Hukum Acara Perdata maupun dalam Hukum Acara Pidana. Mengenai hukum materiilnya pada dasarnya sudah secara tegas diatur dalam Pasal 15 ayat (1) Undang- Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan yang menyatakan bahwa "dokumen perusahaan yang telah dimuat dalam microfilm atau media lainnya dan atau hasil cetaknya merupakan alat bukti yang sah". Selanjutnya apabila kita perhatikan ketentuan dalam Pasal 1 angka 2 mengenai pengertian dokumen dan dikaitkan dengan ketentuan Pasal 12 ayat (1) dan ayat (2) Undang-Undang Nomor 8 Tahun 1997 jo. Pasal 1320 KUHPerdata, transaksi melalui media elektronik adalah sah menurut hukum.

KUH Perdata menjelaskan maksud hal tertentu, dengan memberikan rumusan dalam Pasal 1333 KUH Perdata, yang berbunyi sebagai berikut: "Suatu perjanjian harus mempunyai sebagai pokok perjanjian berupa suatu kebendaan yang paling sedikit ditentukan jenisnya. Tidaklah menjadi halangan bahwa jumlah kebendaan tidak tentu, asal saja jumlah itu kemudian dapat ditentukan atau dihitung". Secara sepintas, dengan rumusan "pokok perjanjian berupa barang yang telah ditentukan jenisnya, tampaknya KUH Perdata hanya menekankan pada perikatan untuk memberikan atau menyerahkan sesuatu. Namun demikian jika kita perhatikan lebih lanjut, rumusan tersebut hendak menegaskan kepada kita semua bahwa apapun jenis perikatannya, baik itu perikatan untuk memberikan sesuatu, berbuat sesuatu, atau untuk tidak berbuat sesuatu, KUH Perdata hendak menjelaskan, bahwa semua jenis perikatan tersebut pasti melibatkan keberadaan atau eksistensi dari suatu kebendaan yang tertentu. Perjanjian yang diperjanjikan harus suatu hal atau suatu barang yang cukup jelas atau tertentu. Syarat ini perlu untuk dapat menetapkan kewajiban dari si berhutang jika ada perselisihan. Barang yang dimaksudkan dalam perjanjian paling sedikit harus ditentukan jenisnya. Bahwa barang itu sudah ada atau sudah berada di tangannya si berhutang

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

pada waktu perjanjian dibuat, tidak diharuskan oleh undang-undang. Juga jumlahnya tidak perlu disebutkan, asal saja kemudian dapat dihitung atau ditetapkan. Syarat bahwa prestasi harus tertentu atau dapat ditentukan, gunanya ialah untuk menetapkan hak dan kewajiban kedua belah pihak, jika timbul perselisihan dalam pelaksanaan perjanjian. Jika prestasi kabur atau dirasakan kurang jelas, yang menyebabkan perjanjian itu tidak dapat dilaksanakan, maka dianggap tidak ada obyek perjanjian dan akibat hukum perjanjian itu batal demi hukum.[26]

Undang-undang Informasi dan Transaksi Elektronik (UU ITE) memiliki asas diantaranya netral teknologi atau kebebasan memilih teknologi. Hal ini termasuk memilih jenis tanda tangan elektronik yang dipergunakan untuk menandatangani suatu informasi elektronik dan/atau dokumen elektronik. Asas netral teknologi dalam UU ITE perlu dipahami secara berhati-hati, dan para pihak yang melakukan transaksi elektronik sepatutnya menggunakan tanda tangan elektronik yang memiliki kekuatan hukum dan akibat hukum yang sah seperti diatur dalam pasal 11 ayat 1 UU ITE.

Keabsahan Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut berdasarkan Pasal 11 Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu :

1. Data pembuatan tanda tangan elektronik terkait hanya kepada penanda tangan.
2. Data pembuatan tanda tangan elektronik pada saat proses penanda tangan elektronik hanya berada dalam kuasa penanda tangan.
3. Segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui.
4. Segala perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut setelah waktu penanda tanganan dapat diketahui.

[26] Rosa Agustina T. Pangaribuan, *Op.Cit.*, Hlm.1

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

5. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penanda-tangannya.
6. Terdapat cara tertentu untuk menunjukkan bahwa penanda tangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.

2.1.9. Latar Belakang Munculnya Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di Indonesia.

Pada bulan Juni 2000, Kongres mencoba untuk memecahkan masalah ini dengan Tanda Tangan Elektronik di Global dan Perdagangan Nasional Undang-Undang (E-Sign). Pada tanggal 30 Juni 2000, Presiden Clinton menandatangani menjadi undang-undang Tanda Tangan Elektronik di Global dan Perdagangan Nasional Undang-Undang (E-Sign). Kongres diundangkan undang-undang ini jauh diantisipasi dengan tujuan perampingan bisnis dengan memungkinkan lebih nyaman, dan lebih murah transaksi tanpa kertas, lebih cepat. Meskipun 40 negara telah berlaku hukum untuk menyediakan penggunaan tanda tangan elektronik, hukum-hukum ini sangat bervariasi. E-Kongres disesuaikan Daftar untuk memberikan status hukum dan seragam dengan tanda tangan elektronik. Sebagai e-Commerce telah meledak dalam dekade terakhir, pengadilan telah bergumul dengan tantangan untuk menerapkan hukum kontrak tradisional, sebagian dipandu oleh undang-undang penipuan, untuk transaksi elektronik. Patung penipuan memerlukan transaksi tertentu yang harus secara tertulis dan ditandatangani oleh pihak yang terlibat. Pengadilan dihadapkan dengan pertanyaan apakah transaksi elektronik memenuhi ini "persyaratan menulis," menjawab "ya. Kebingungan ini menimbulkan beberapa pertanyaan penting mengenai apakah pengadilan, dalam kasus-kasus masa depan, secara konsisten akan menegakkan kontrak elektronik. Ketidakpastian ini menimbulkan masalah serius yang pasti akan menghambat e-Commerce. Di antara kebingungan ini terletak kemungkinan hilangnya keamanan dan akuntabilitas yang diberikan oleh undang-undang penipuan Seperti Perwakilan Davis dicatat dalam diskusi US *House of E-Sign*. Semua hal lain dianggap sama, ketika pihak tahu

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

bahwa jaminan akuntabilitas tanda tangan, bahwa mereka mendapatkan manfaat, dan pada saat yang sama melaksanakan kewajiban tertentu sebagai imbalan, perilaku mereka selalu dibentuk oleh kepastian yang hasilnya saat pihak terikat secara kontraktual. Oleh karena itu, dalam rangka untuk mendapatkan perlindungan dari undang-undang penipuan, tanda tangan elektronik harus memiliki beberapa ukuran keamanan dan akuntabilitas. Ini adalah masalah di mana Kongres, negara, dan yang paling penting, pasar sendiri, harus terus menetapkan pedoman baru yang baik meningkatkan dan meningkatkan keamanan dan akuntabilitas transaksi online.

2.2 Kekuatan hukum dan keabsahan tanda tangan elektronik sebagai alat bukti.

Berbagai kemajuan teknologi ini kemudian diantisipasi dengan lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik selanjutnya ditulis UU ITE . Pengaturan Informasi, Dokumen, dan Tanda Tangan Elektronik, dituangkan dalam Pasal 5 sampai dengan Pasal 12 UU ITE. Secara umum dikatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah, yang merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Demikian halnya dengan Tanda Tangan Elektronik, memiliki kekuatan hukum dan akibat hukum yang sah. Namun pembuatan tanda tangan elektronik tersebut harus memenuhi persyaratan-persyaratan yang ditentukan. Namun sebelumnya, dalam Undang-Undang Nomor 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa (AAPS), juga menyinggung sedikit mengenai bukti elektronik dalam Pasal 4 ayat (3) yang menyatakan: Dalam hal disepakati penyelesaian sengketa melalui arbitrase terjadi dalam bentuk pertukaran surat, maka pengiriman teleks, telegram, faksimili, e-mail atau dalam bentuk sarana komunikasi lainnya, wajib disertai dengan suatu catatan penerimaan oleh para pihak. Tetapi apa yang telah dirumuskan dalam UU ITE maupun UU AAPS ini tidak

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

selamanya sejalan dengan peraturan lain dalam hukum nasional. Dalam BW maupun KUHP misalnya, pengaturan mengenai hal ini masih terasa bias, sehingga penginterpretasian atas keberadaan bukti elektronik seringkali masih multitafsir, dan tidak konsisten dalam penerapannya ketika terjadi sengketa

2.2.1 Atribut Tanda Tangan.

Untuk mencapai tujuan dari penandatanganan suatu dokumen elektronik, sebuah tanda tangan harus mempunyai atribut-atribut berikut:[27]

1. Otentikasi Penanda tangan adalah Sebuah tanda tangan seharusnya dapat mencapai mengindentifikasikan siapa yang menandatangani dokumen tersebut dan susah untuk ditiru orang lain.
2. Otentikasi Dokumen adalah Sebuah tanda tangan seharusnya mengidentifikasikan apa yang ditandatangani, membuatnya tidak mungkin dipalsukan ataupun diubah (baik dokumen yang ditandatangani maupun tandatangannya) tanpa diketahui.

Otentikasi penandatangan dan dokumen adalah alat untuk menghindari pemalsuan dan merupakan suatu penerapan konsep "*nonrepudiation*" dalam bidang keamanan informasi. *Nonrepudiation* adalah jaminan dari keaslian ataupun penyampaian dokumen asal untuk menghindari penyangkalan dari penandatangan dokumen (bahwa dia tidak menandatangani dokumen tersebut) serta penyangkalan dari pengirim dokumen (bahwa dia tidak mengirimkan dokumen tersebut).[28]

2.2.2 Cara Kerja Teknologi Tanda Tangan Digital.

Tanda tangan digital dibuat dengan menggunakan teknik kriptografi, suatu cabang dari matematika terapan yang menangani tentang pengubahan suatu informasi menjadi bentuk lain yang tidak dapat dimengerti dan dikembalikan seperti semula. Tanda tangan digital menggunakan "*public key cryptography*" (kriptografi kunci publik), dimana algoritmanya menggunakan dua buah kunci, yang pertama adalah

[27] B. Schneier, *Applied Cryptography*, 403-410, John Wiley & Sons, 1996.
[28] J. M. Perillo, *The Statute of Frauds in the Light of theFunctions and Disfunctions of Form*, Fordham L. Rev. 39, 48-641974.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

kunci untuk membentuk tanda tangan digital atau mengubah data ke bentuk lain yang tidak dapat dimengerti, dan kunci kedua digunakan untuk verifikasi tanda tangan digital ataupun mengembalikan pesan ke bentuk semula. Konsep ini juga dikenal sebagai "*assymmetric cryptosystem*" (sistem kriptografi non simetris). Sistem kriptografi ini menggunakan kunci privat, yang hanya diketahui oleh penandatangan dan digunakan untuk membentuk tanda tangan digital, serta kunci publik, yang digunakan untuk verifikasi tanda tangan digital. Jika beberapa orang ingin memverifikasi suatu tanda tangan digital yang dikeluarkan oleh seseorang, maka kunci publik tersebut harus disebarkan ke orang-orang tersebut. Kunci privat dan kunci publik ini sesungguhnya secara matematis 'berhubungan' (memenuhi persamaan-persamaan dan kaidah-kaidah tertentu). Walaupun demikian, kunci privat tidak dapat ditemukan menggunakan informasi yang didapat dari kunci publik. Proses lain yang tak kalah penting adalah "fungsi hash", digunakan untuk membentuk sekaligus memverifikasi tanda tangan digital. Fungsi hash adalah sebuah algoritma yang membentuk representasi digital atau semacam "sidik jari" dalam bentuk "nilai hash" (*hash value*) dan biasanya jauh lebih kecil dari dokumen aslinya dan unik hanya berlaku untuk dokumen tersebut. Perubahan sekecil apapun pada suatu dokumen akan mengakibatkan perubahan pada "nilai hash" yang berkorelasi dengan dokumen tersebut. Fungsi hash yang demikian disebut juga "fungsi hash satu arah", karena suatu nilai hash tidak dapat digunakan untuk membentuk kembali dokumen aslinya. Oleh karenanya, fungsi hash dapat digunakan untuk membentuk tanda tangan digital. Fungsi hash ini akan menghasilkan "sidik jari" dari suatu dokumen (sehingga unik hanya berlaku untuk dokumen tersebut) yang ukurannya jauh lebih kecil daripada dokumen aslinya serta dapat mendeteksi apabila dokumen tersebut telah diubah dari bentuk aslinya. Penggunaan tanda tangan digital memerlukan dua proses, yaitu dari pihak penandatangan serta dari pihak penerima. Secara rinci kedua proses tersebut dapat dijelaskan sebagai berikut:

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

1. Pembentukan tanda tangan digital menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat yang telah didefinisikan sebelumnya. Untuk dapat menjamin keamanan nilai hash maka seharusnya terdapat kemungkinan yang sangat kecil bahwa tanda tangan digital yang sama dapat dihasilkan dari dua dokumen serta kunci privat yang berbeda.
2. Verifikasi tanda tangan digital adalah proses pengecekan tanda tangan digital dengan mereferensikan ke dokumen asli dan kunci publik yang telah diberikan, dengan cara demikian dapat ditentukan apakah tanda tangan digital dibuat untuk dokumen yang sama menggunakan kunci privat yang berkorespondensi dengan kunci publik.

Untuk menandatangani sebuah dokumen atau informasi lain, penandatangan pertama-tama membatasi secara tepat bagian-bagian mana yang akan ditandatangani. Informasi yang dibatasi tersebut dinamakan "*message*". Kemudian aplikasi tanda tangan digital akan membentuk nilai hash menjadi tanda tangan digital menggunakan kunci privat. Tanda tangan digital yang terbentuk adalah unikbaik untuk *message* dan juga kunci privat.

Umumnya, sebuah tanda tangan digital disertakan pada dokumennya dan juga disimpan dengan dokumen tersebut juga. Bagaimanapun, tanda tangan digital juga dapat dikirim maupun disimpan sebagai dokumen terpisah, sepanjang masih dapat diasosiasikan dengan dokumennya. Karena tanda tangan digital bersifat unik pada dokumennya, maka pemisahan tanda tangan digital seperti itu merupakan hal yang tidak perlu dilakukan. Proses pembentukan dan verifikasi tanda tangan digital memenuhi unsur-unsur paling penting yang diharapkan dalam suatu tujuan legal, yaitu

1. Otentikasi Penandatangan: Jika pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah yang telah didefinisikan, maka tanda tangan digital akan dapat menghubungkan atau mengasosiasikan dokumen dengan penandatangan. Tanda tangan digital tidak dapat

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

dipalsukan, kecuali penandatangan kehilangan kontrol dari kunci privat miliknya.

2. Otentikasi Dokumen: Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan tingkat kepastian dan ketepatan yang jauh lebih tinggi daripada tanda tangan di atas kertas.

3. Penegasan: Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan. Tindakan ini dapat menegaskan bahwa penandatangan setuju dan bertanggung jawab terhadap isi dokumen.

4. Efisiensi: Proses pembentukan dan verifikasi tanda tangan digital menyediakan tingkat kepastian yang tinggi bahwa tanda tangan yang ada merupakan tanda tangan sah dan asli dari pemilik kunci privat.

Dengan tanda tangan digital , tidak perlu ada verifikasi dengan melihat secara teliti (membandingkan) antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya seperti yang biasa dilakukan dalam pengecekan tanda tangan secara manual.

2.2.3 Kelemahan dan Keunggulan Tanda Tangan Digital.

Kelemahan yang masih menyertai teknologi tanda tangan digital adalah:

1. Biaya tambahan secara institusional: Tanda tangan digital memerlukan pembentukan otoritas-otoritas yang berhak menerbitkan sertifikat serta biaya-biaya lain untuk menjaga dan mengembangkan fungsi-fungsinya.
2. Biaya langganan: Penanda tangan memerlukan perangkat lunak aplikasi dan juga membayar untuk memperoleh sertifikasi dari otoritas yang berhak mengeluarkan sertifikat.

Sedangkan kelebihan yang paling utama dari adanya tanda tangan digital adalah lebih terjaminnya otentikasi dari sebuah dokumen. Tanda tangan digital sangat sulit dipalsukan dan berasosiasi dengan kombinasi dokumen dan kunci privat secara unik.

2.2.4 Bentuk Kriptologi.

Tujuan dari suatu tandatangan dalam suatu dokumen adalah untuk

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

memastikan otentisitas dari dokumen tersebut. Suatu digital signature sebenarnya adalah bukan suatu tanda tangan seperti yang kita kenal selama ini, ia menggunakan cara yang berbeda untuk menandai suatu dokumen sehingga dokumen atau data sehingga ia tidak hanya mengidentifikasi dari pengirim, namuni ia juga memastikan keutuhan dari dokumen tersebut tidak berubah selama proses transmisi. Suatu digital signature didasarkan dari isi dari pesan itu sendiri.

Bedasarkan sejarahnya, penggunaan *digital signature* berawal dari penggunaan teknik kriptografi yang digunakan untuk mengamankan informasi yang hendak ditransmisikan atau disampaikan kepada orang yang lain yang sudah digunakan sejak ratusan tahun yang lalu. Dalam suatu kriptografi suatu pesan dienkripsi *(encrypt)* dengan menggunakan suatu kunci (*key*). Hasil dari enkripsi ini adalah berupa chipertext tersebut kemudian ditransmisikan atau diserahkan kepada tujuan yang dikehendakinya. *Chipertext* tersebut kemudian dibuka atau didekripsi *(decrypt*) dengan suatu kunci untuk mendapatkan informasi yang telah enkripsi tersebut. Terdapat dua macam cara dalam melakukan enkripsi yaitu dengan menggunakan kriptografi simetris (*symetric crypthography/secret key crypthography*) dan kriptografi simetris (*asymetric crypthography*) yang kemudian lebih dikenal sebagai public key crypthography yang digunakan pada tanda tangan elektronik. Kriptologi simetris hanya menggunakan sebuah kunci rahasia untuk mengenkripsi dan mendekripsi sebuah pesan. Salah satu algoritma simetris yang digunakan adalah *Data Encryption Standard* (selanjutnya disebut DES) yang mempunyai panjang kunci 64 bit. Teknik ini sudah semakin ditinggalkan karena tingkat kebocorannya sangat tinggi. Bila kunci rahasia tersebut diketahui oleh pihak ketiga maka dia dapat menggunakannya untuk mendekripsi, membaca bahkan memalsukan pesan rahasia tersebut. Untuk keluar dari kesulitan ini digunakanlah sebuah teknik pengkodean yang disebut Kriptologi asimetris. Tahun 1976, dua ahli matematika Diffie dan Hellman memperkenalkan sebuah sistem kriptologi asimetris atau kriptologi kunci publik, teknik ini menggunakan dua buah kunci. Konsep

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

ini kemudian diaplikasikan oleh Rivest, Shamir dan Adleman, dengan membuat sebuah algoritma asimetris RSA pada tahun 1977. Sebuah kunci RSA mempunyai panjang kunci yang bervariasi mulai dari 40 bits hingga 2048 bits12. Berkat algoritma ini, Phil Zimmerman mampu membuat sebuah piranti lunak yang diberi nama Pretty Good Privacy (selanjutnya disebut PGP). Karena piranti lunak ini didistribusikan secara bebas dan gratis maka penyebaran piranti lunak ini sangat cepat di kalangan pengguna pribadi.

Proses ini melibatkan dua buah kunci, yang disebut kunci privat dan kunci publik. Kunci privat digunakan untuk mengenkripsi pesan rahasia sedangkan kunci public digunakan untuk mendekripsi pesan rahasia tersebut agar dapat dibaca. Begitupun sebaliknya, kunci publik digunakan untuk mengenkripsi sebuah pesan rahasia dan kunci privat digunakan untuk mendekripsikan pesan tersebut. Sekalipun secara matematis, dua kunci ini saling berhubungan tetapi tidak dimungkinkan menemukan kunci privat dengan menggunakan kunci publik, sehingga sangat dimungkinkan untuk mendistribusikan seluas-luasnya kunci publik. Namun sebaliknya, kunci privat harus disimpan dan dijaga kerahasiaannya. Teknik kriptologi asimetris ini merupakan dasar dari pembuatan tanda tangan elektronik.

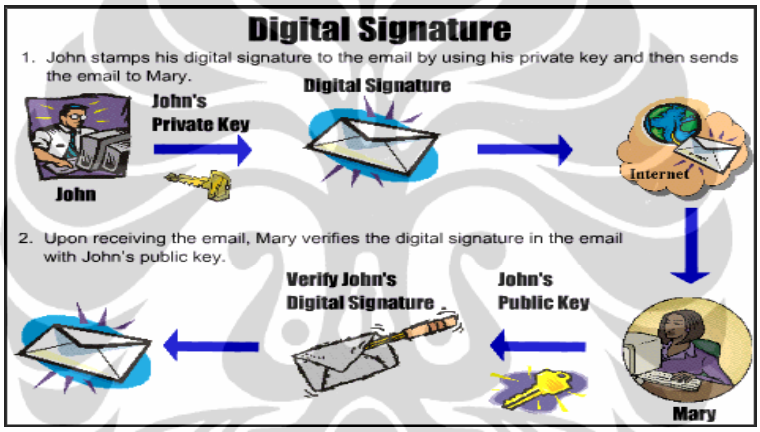
2.2.5 Proses Tanda Tangan Elektronik.

Untuk menandatangani secara elektronis sebuah pesan, dengan bantuan piranti lunak, pengirim akan membuat pertama-tama sebuah *message digest*16 dari pesan yang asli dengan menggunakan *fonction de hachage* (*hash* dalam bahasa inggris). *Message digest* dari setiap pesan asli adalah unik layaknya “sidik jari“, sehingga perubahan sekecil-kecilnya pada sebuah *message digest* akan mengakibatkan perubahan “sidik jarinya” pula. Keuntungannya, baik sang Pengirim maupun Penerima dapat mengetahui keintegritasan pesan tersebut. Selanjutnya *message digest* tersebut akan ditanda tangani dengan menggunakan kunci privat pengirim, dengan kata lain tanda tangan elektronik adalah *message digest* yang dienkripsi oleh kunci privat Pengirim. Kemudian pesan asli dan

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

tandatangan elektronik dikirim bersama-sama ketujuan yang diinginkan. Berkat kunci publik dari Pengirim yang dikomunikasikan terlebih dahulu ke penerima pesan, Penerima dapat mendekripsi tanda tangan elektronik tersebut, katakanlah hasilnya A1, selanjutnya penerima akan membuat *message digest* pada pesan asli yang diterima, katakanlah hasilnya A2. Maka langkah terakhir adalah membandingkan keduanya, yaitu A1 dan A2. Bila keduanya memiliki "sidik jari" yang sama, maka dapat dipastikan bahwa itu pesan asli dan belum pernah dirubah. Sekalipun begitu, proses ini tidak dapat mengotentifikasi identitas penulis pesan tersebut.

Contoh gambar tanda tangan elektronik :[29]



No	Penjelasan
1	John menjalankan (runs) data yang hendak ia kirimkan, melalui algoritma satu arah (one way algorithm) sehingga ia mendapat suatu nilai (value) yang unik dari data tersebut. Nilai ini disebut message digest. Nilai adalah semacam sidik jari bagi data tersebut dan akan digunakan dalam proses yang lebih lanjut untuk meneliti keutuhan (integrity) dari data tersebut.
2	Mary kemudian melakukan enkripsi terhadap messages digest tersebut dengan menggunakan kunci prifatnya sehingga ia akan mendapatkan digital signature dari data tersebut.

[29] Tbibistel, *tbibistel.wordpress.com*, 23 Mei 2011.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

3	Kemudian, Mary membuat (generates) suatu kunci simetris secara acak (random) dan menggunakan kunci itu melakukan enkripsi terhadap data yang hendak ia kirimkan, tandatangan (signature) miliknya, dan salinan dari sertifikat digitalnya yang berisi kunci publiknya. Untuk mendekripsi data tersebut John membutuhkan salinan dari kunci simetris tersebut.
4	Mary harus memiliki terlebih dahulu sertifikat milik John, sertifikat ini berisi salinan (copy) dari kunci publik milik John. Untuk menjamin keamanan transmisi dari kunci simetris maka kunsi tersebut dienkripsi dengan menggunakan kunci publik milik John. Kunci yang telah dienkripsi yang dikenal sebagai amplop digital (digital envelope) akan dikirimkan bersama-sama dengan data yang telah dienkripsi.
5	Mary kemudian akan mengirimkan data (message) tersebut yang berisi data yang telah dienkripsi dengan kunci simetris, tandatangan dan sertifikat digital, serta kunci simetris yang telah dienkripsi dengan kunci asimetris (digital envelope).
6	John menerima pesan (*messages*) dari Mary tersebut dan kemudian mendekripsi amplop digital dengan kunci prifat yang dipunyainya, ia kemudian akan mendapatkan kunci asimetris.
7	John kemudian menggunakan kunci simetris tersebut untuk mendekripsi data itu (*property descryption*), tandatangan Mary, dan sertifikat miliknya.
8	Ia kemudian mendekripsi digital signature milik Mary dengan menggunakan kunci publik milik Mary, yang didapat John dari sertifikat milik Mary. Dari dekripsi ini akan didapatkan message digest dari data tersebut.
9	John kemudian memproses *(run)* data itu dengan menggunakan algoritma satu arah yang sama yang digunakan Mary untuk *message digest*.
10	Akhirnya John akan membandingkan antara message digest

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

	yang didapatkannya dari proses dekripsi diatas dengan message digest yang didapatkan dari *digital signature* milik Mary. Kalau hasil yang didapat dari perbandingan itu adalah sama maka, John dapat merasa yakin bahwa data tersebut tidak pernah dirusak (*altered*) selama proses transmisi dan data itu ditandatangani dengan menggunakan kunci privat milik Mary. Kalau hasil dari perbandingan itu adalah tidak sama, maka data tersebut pastilah telah diubah atau dipalsukan setelah ditandatangani.

Catatan: Suatu tanda tangan digital *(Digital Signature)* akan menyebabkan data elektronik yang dikirimkan melalui open network tersebut menjadi terjamin.[30]

2.3 Pembuktian Hukum Perdata di Indonesia.

Hukum Pembuktian (yang tercantum dalam buku keempat dari BW (Burgerlijk Wetboek atau Kitab Undang-Undang Hukum Perdata), mengandung segala aturan-aturan pokok pembuktian dalam perdata. Pembuktian dalam BW semata-mata hanya berhubungan dengan perkara saja. Ada beberapa definisi yang dikemukakan oleh para ahli hukum yang dapat dijadikan acuan. Menurut Pitlo, Pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya. Menurut Subekti yang dimaksudkan dengan 'membuktikan' adalah meyakinkan hakim tentang kebenaran dalil atau dalil-dalil yang dikemukakan dalam suatu persengketaan.

Ada perbedaan antara bukti dalam ilmu pasti dengan bukti dalam hukum. Bukti dalam ilmu pasti menetapkan kebenaran terhadap semua orang, sedangkan bukti dalam suatu (perkara) hukum hanya menetapkan kebenaran terhadap pihak-pihak yang berperkara dan pengganti-penggantinya menurut hukum.

Kenapa diperlukan adanya pembuktian? Pembuktian dilakukan atas guna untuk senantiasa menetapkan akan adanya suatu fakta, atau

[30] Tbibistel, *Ibid.*

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

mendalilkan suatu peristiwa. Dapat kita lihat pula pada Pasal 163 HIR (283 RGB) yang mengatur perihal pembuktian: "Setiap orang yang mendalilkan bahwa ia mempunyai suatu hak, atau guna meneguhkan haknya sendiri maupun membantah hak orang lain, menunjuk pada suatu peristiwa diwajibkan membuktikan adanya hak atau peristiwa tersebut." Dari Pasal tersebut dapat kita simpulkan bahwa dalam pembuktian tidak hanya dalil peristiwa saja dapat dibuktikan, tetapi juga akan adanya suatu hak.

Dengan melakukan pembuktian maka akan dapat dilakukan suatu pembenaran atau penyangkalan terhadap suatu dalil yang dikemukakan oleh para pihak yang terlibat dalam perkara. Suatu pembuktian lazimnya baru dilakukan apabila ada suatu perselisihan. Suatu perselisihan diselesaikan di badan peradilan Indonesia, apabila telah disepakati oleh kedua belah pihak atau telah ada di dalam suatu kontrak yang di dalamnya terdapat suatu klausul yang menyebutkan bahwa setiap perselisihan yang timbul akan diselesaikan menurut hukum Indonesia dan diselenggarakan di Peradilan Indonesia.

Di dalam badan peradilan di Indonesia, dikenal suatu hukum acara yang fungsinya mengatur hal-hal yang diselenggarakan di dalam proses peradilan. Di dalam hal ini, hukum positif (hukum yang berlaku saat ini) yang ada adalah HIR (Herzien Inlands Reglement) atau yang dikenal dengan sebutan RIB (Reglemen Indonesia yang diperBaharui), yaitu undang-undang yang termuat dalam Staatsblaad 1941 No.44. Mungkin terpikir oleh awam, inilah yang sering didengungkan oleh para ahli hukum di Indonesia, mengenai produk hukum Belanda yang masih berlaku sampai sekarang ini. Hal ini benar adanya, sebagaimana adanya kekosongan hukum dan keberlakuan dari HIR ini, juga hanya diatur dalam UU Darurat. Kenyataan inilah yang harus kita hadapi bersama, mengingat sebagai produk lama maka besar pula kemungkinan dimana kita hanya menemui peraturan hukum yang mengatur mengenai hal-hal yang sifatnya tidak atau belum *up to date*, apalagi dalam hal ini kita membicarakan mengenai kegiatan sehubungan dengan *e-commerce* dengan penggunaan

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Digital Signature, sesuatu yang baru dan belum terpikirkan oleh pembentuk undang-undang ini pada waktu dibuatnya.

Sebagaimana diatur dalam 164 HIR (283 RBG) dan 1903 BW, hanya dikenal 5 (lima) macam alat bukti yang dapat dihadirkan di persidangan khususnya dalam acara perdata, di antaranya:

1. Bukti tulisan
2. Bukti dengan saksi
3. Persangkaan-persangkaan
4. Pengakuan
5. Sumpah

Sedangkan khusus dalam acara pidana, dikenal adanya barang bukti dan alat bukti.

Dalam doktrin ilmu hukum pidana, barang bukti dapat dikategorikan dalam tiga antara lain:

1. Barang yang digunakan untuk melakukan perbuatan pidana,
2. Barang yang digunakan untuk membantu terjadinya perbuatan pidana, dan
3. Barang yang menjadi hasil perbuatan pidana.

Sedangkan alat bukti dalam acara pidana (Pasal 184 KUHAP) dengan alat bukti dalam acara perdata secara umum adalah sama.

Digital Signature sebagai suatu data elektronik di dalam hal ini mempunyai masalah apabila diajukan sebagai alat bukti di dalam beracara di Badan Peradilan Indonesia. Digital Signature yang digunakan dalam transaksi e-commerce secara keseluruhan adalah merupakan paperless, bahkan scriptless transaction. Sesuai apa yang diatur dalam pasal tersebut, maka dalam hal ini berarti bukti-bukti berupa data elektronik yang diajukan akan dianggap tidak mempunyai kekuatan hukum pembuktian. Kemungkinan juga besar, terhadap ditolaknya hal ini sebagai alat bukti oleh hakim maupun pihak lawan.

Hukum Acara yang ada dan berlaku sekarang (hukum acara positif) dalam hal ini perlu ditinjau ulang untuk adanya kemungkinan dilakukannya suatu revisi, mengingat adanya kebutuhan yang mendesak

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

ini. Masalah e-commerce sudah ada di depan mata dan adanya kemungkinan munculnya suatu kasus perselisihan/dispute tinggal menunggu waktu saja. Apabila hal ini terjadi maka akan dapat diduga munculnya permasalahan pembuktian yang kompleks. Hal-hal yang telah disebutkan di atas hanyalah merupakan sebagian dari keseluruhan permasalahan.

Revisi hukum acara positif sebagai tujuan jangka panjang tentu saja membutuhkan waktu yang tidak singkat karena membutuhkan perumusan terlebih dulu, belum termasuk tahapan pembentukan undang-undang di badan legislatif. Menyikapi hal ini tentu saja kita perlu melakukan tindakan antisipatif dan perlu diambil langkah-langkah yang sifatnya memberikan solusi terhadap kemungkinan adanya kasus di bidang ini. Yang perlu dilakukan dalam waktu singkat adalah memberikan suatu pemahaman kepada seluruh masyarakat khususnya kepada para pelaku hukum mengenai permasalahan pembuktian yang mungkin timbul tersebut.

Hakim sebagai pemutus suatu perkara tentu saja mendapatkan perhatian terbesar dalam hal ini. Hakim dengan dibekali pengetahuan yang cukup mengenai skema perniagaan elektronik (*e-commerce*) seharusnya memahami, setidaknya mengetahui, bagaimana proses transaksi yang nyaris secara keseluruhan adalah non-paper based, bahkan scriptless! Hakim nantinya diharapkan peranannya, apabila menghadapi kasus yang berkenaan dengan e-commerce dengan menggunakan digital signature, untuk dapat mengambil langkah-langkah yang dianggap perlu.

Dalam menerima perkara, tidak boleh seorang hakim menolaknya dengan alasan belum ada ketentuan hukum yang mengaturnya, sebagaimana diatur dalam Pasal 22 AB (*Algemeine van Bepalingen*). Untuk inilah hakim dituntut untuk melakukan interpretasi terhadap suatu gejala hukum dan peraturan perundang-undangan yang sudah ada.

Penafsiran (interpretasi) yang dapat dilakukan oleh hakim maupun ahli hukum antara lain dapat melalui interpretasi analogis maupun interpretasi ekstentif.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Interpretasi analogis dapat dilakukan apabila belum ada suatu peraturan hukum yang mengatur mengenai data elektronik atau digital, terutama dalam hal ini yang berkaitan dengan digital signature, belum ada. Jadi hakim dapat mengambil norma-norma yang ada di masyarakat untuk melakukan interpretasi analogis. Interpretasi ekstentif dapat dilakukan apabila telah ada peraturan hukumnya, tetapi tidak secara langsung mengatur.

Interpretasi yang perlu dilakukan hakim dalam hal pembuktian adalah melakukan perluasan makna tertulis sebagai alat bukti.

Definisi Surat diberikan oleh para ahli hukum pembuat BW, yaitu pembawa tanda tangan bacaan yang berarti, yang menterjemahkan suatu isi pikiran. Atas bahan apa dicantumkannya tanda bacaan ini, adalah tidak penting (PITLO, dalam buku Bewijs en Verjaring naar het Nederlands Burgerlijk Wetboek). Jadi tidak memandang ditulisnya di atas lembaran kertas, di atas bungkus cigaret, maupun di atas buah semangka, tetap merupakan surat. Dalam permasalahan yang kita hadapi ini berkaitan dengan penggunaan data elektronik sebagai media penyampaian pesan.

Di dalam Pasal 1904 BW dikenal pembagian kategori 'tertulis' sebagai berikut:

1. Otentik
2. bawah tangan

Tetapi hal ini diatur lagi dalam Pasal 1905-1920 dalam Kitab Undang-Undang yang sama, yaitu:

1. Akta
2. Bukan Akta

Terdapat kerancuan mengenai hal ini, kenapa sampai ada dua pembagian ketentuan hukum yang berbeda mengenai kualifikasi tertulis? Saya akan mengambil teori yang dikemukakan oleh Pitlo, Sarjana Hukum Belanda, yang mengambil jalan tengah, yaitu menggabungkan unsur dan mengelompokkannya sesuai urutan kekuatannya:

1. Akta Otentik
2. Akta Bawah Tangan

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

3. Bukan Akta

Dalam persidangan, untuk dapat mempunyai kekuatan pembuktian yang penuh, maka selayaknya dalam mengajukan suatu fakta, pihak yang mengajukan fakta tersebut sudah selayaknya mengajukan alat bukti Surat Akta Otentik. Suatu Digital Signature sudah seharusnya mempunyai kekuatan pembuktian yang sama sebagaimana Surat Akta Otentik.

Dalam hal *e-commerce*, tidak ada alat bukti lain yang dapat digunakan selain data elektronik atau digital yang ditransmisikan kedua belah pihak yang melakukan perdagangan. Adapun saksi, persangkaan, pengakuan dan sumpah, kesemuanya itu adalah tidak mungkin dapat diajukan sebagai alat bukti karena tidak bisa didapatkan dari suatu transaksi e-commerce. Selain itu, apabila disamakan sebagai tulisan, apalagi akta otentik, kekuatan pembuktiannya sempurna, dalam arti bahwa ia sudah tidak memerlukan suatu penambahan pembuktian. Akta otentik juga mengikat, dalam arti bahwa apa yang ditulis dalam akta tersebut harus dipercaya oleh hakim, yaitu harus dianggap sebagai benar, selama ketidakbenarannya tidak dibuktikan.

Ada tiga macam kekuatan dari suatu akta otentik, yaitu:

1. Membuktikan antara para pihak, bahwa mereka sudah menerangkan apa yang ditulis dalam akta tersebut (pembuktian formal).
2. Membuktikan antara para pihak yang bersangkutan, bahwa sungguh-sungguh peristiwa yang disebutkan di sini telah terjadi (pembuktian mengikat).
3. Membuktikan tidak saja antara para pihak yang bersangkutan tetapi juga terhadap pihak ketiga, bahwa pada tanggal tersebut dalam akta, kedua belah pihak tersebut telah menghadap di muka pegawai umum dan menerangkan apa yang ditulis dalam akta tersebut. (pembuktian keluar).

Sebelum mengulas mengenai kekuatan pembuktian yang sama tersebut, kita tinjau terlebih dahulu mengenai surat otentik. Dikatakan sebagai suatu akta atau surat otentik apabila mengandung unsur-unsur

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

sebagai berikut ini sebagaimana diatur dalam Pasal 1905 BW, Akta otentik adalah akta yang dibuat menurut bentuk Undang-Undang oleh dan dihadapan seorang pegawai umum yang berwenang di tempat itu. Dapat disarikan di luar definisi sebagai berikut: bentuknya tertulis, dibuat oleh atau dihadapan pejabat atau pegawai umum yang berwenang. Pejabat yang dimaksudkan di sini adalah orang yang berwenang karena atas dasar jabatannya yang diangkat oleh negara, contohnya profesi notaris atau PPAT (Pejabat Pembuat Akta Tanah).

Bila dokumen elektronik tersebut mempunyai daya pembuktian yang sama dengan akta otentik, maka Undang-Undang Jabatan Notaris Nomor 30 Tahun 2004 haruslah direvisi, karena pada Pasal 1 ayat (7) akta notaris adalah akta otentik yang dibuat oleh atau di hadapan Notaris menurut bentuk dan tata cara yang di tetapkan dalam Undang-Undang ini. Kekuatan pembuktian dari dokumen elektronik tersebut hanyalah akta dibawah tangan, dimana bentuk akta di bawah tangan dibuat dalam bentuk yang tanpa perantara atau tidak perantara atau tidak dihadapan pejabat umum yang berwenang, Mempunyai kekuatan pembuktian sepanjang para pihak mengakuinya atau tidak ada penyangkalan dari salah satu pihak. Jika salah satu pihak tidak mengakuinya, beban pembuktian diserahkan kepada pihak yang menyangkal akta tersebut, dan penilaian penyangkalan atas bukti tersebut diserahkan kepada hakim. Terdapat satu hal yang patut dipertimbangkan dalam pengakuan suatu dokumen elektronik yang ditandatangani dengan tanda tangan elektronik, yaitu keamanan suatu sistem dan keterlibatan dari orang terhadap sistem komputer tersebut. Sedangkan eksistensi tanda tangan elektronik dalam sebuah dokumen elektronik harus diakui memiliki kekuatan hukum dan akibat hukum yang sama dengan tanda tangan pada dokumen tertulis lainnya. Hal ini berangkat dari pemahaman bahwa dokumen elektronik memiliki kekuatan hukum sebagai alat bukti dan akibat hukum yang sama sebagaimana dokumen tertulis lainnya.[31] Tanda tangan elektronik yang menggunakan teknologi kriptografi asimetris, menggunakan dua buah kunci yaitu kunci

[31] *Penjelasan Rancangan Peraturan Pemerintah Tentang Tanda Tangan Elektronik*

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

privat dan kunci publik, maka terdapat suatu bukti bahwa dokumen elektronik tersebut merupakan kehendak sendiri dari pengirim.[32] Agar tanda tangan elektronik pada suatu dokumen elektronik dapat mempunyai kekuatan pembuktian di pengadilan, maka harus mendaftarkan tanda tangan elektronik tersebut pada badan *Certification Authority (*CA*)*, maka *CA* tersebut dapat bertindak sebagai pejabat umum, sehingga dengan memanfaatkan infrastruktur yang diberikan *CA* khususnya keamampuan untuk mengetahui kapan transaksi elektronik itu ditandatangani. Tanda tangan digital yang telah memperoleh sertifikat dari lembaga *Certification Authority*, maka akan lebih terjaminya otentikasi dari sebuah dokumen, dan tanda tangan digital sangat sulit dipalsukan dan berasosiasi dengan kombinasi dokumen dan kunci privat secara unik, apabila sudah melaksanakan ketentuan yang ditetapkan dengan peraturan Perundang-Undangan yang terkait. Seringkali Badan Negara yang berwenang mengeluarkan Undang-Undang, antara satu Undang-Undang dengan Undang-Undang yang lain saling bertentangan satu sama lain, seperti Undang-Undang Nomor 11 Tahun 2008, yang bertentangan dengan Undang-Undang Nomor 30 Tahun 2004, maka terhadap kasus yang aturan hukumnya bertentangan satu dengan yang lain, maka hakim berpatokan pada azas lex *specialis derogate lex generalis*, artinya Undang-Undang yang bersifat khusus menyampingkan Undang-Undang yang bersifat umum, dalam hal ini Undang-Undang Nomor 11 Tahun 2008 menyampingkan Undang-Undang Nomor 30 Tahun 2004. Maka kekuatan pembuktian dokumen elektronik yang ditandatangani dengan tanda tangan elektronik sama dengan akta otentik.

Pengakuan dokumen yang telah ditandatangani dengan menggunakan *digital signature*, setelah dikeluarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik, maka pengakuan dokumen elektronik yang ditandatangani dengan tanda tangan *digital signature* tersebut, merupakan perluasan dari pembuktian hukum acara perdata di Indonesia, sehingga seluruh transaksi elektronik dengan

[32] Abdul Salam, 2008, *Alat Bukti Elektronik*, www.ui.edu/abdul.salam/2008/07/01

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

tanda tangan elektronik dapat dianggap sebagai akta, bahkan kekuatan pembuktiannya sama dengan akta otentik yang dibuat oleh pejabat yang berwenang. Kecuali yang ditentukan pada Pasal 5 ayat (4) Undang-Undang Nomor 11 tahun 2008 yaitu ketentuan mengenai Informasi elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk :

1. Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
2. Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Penjelasan Pasal 5 ayat (4) Undang-Undang Nomor 11 Tahun 2008, bahwa surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis itu meliputi namun tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana dan administrasi negara.[33]

Jika dianalisa ketentuan pasal 5 ayat 1, ayat 2, pasal 6, Penjelasan Umum dengan menggunakan metode logika induksi, maka kesimpulannya yang dimaksud dengan kedudukan adalah fungsi; jadi informasi yang dibuat melalui media elektronik ”fungsinya” disetarakan dengan informasi yang dibuat dengan menggunakan media kertas; oleh karena itu dalam UU ITE sama sekali tidak menentukan kedudukan hukum (dalam hal ini kedudukan, nilai, derajat, dan kekuatan pembuktian) dalam Hukum Acara yang berlaku di Indonesia.

Jadi apabila kita hendak mengajukan suatu digital signature sebagai sesuatu yang di-attach pada suatu pesan untuk menjadikannya berkekuatan hukum yang sama dengan surat akta otentik, maka ada permasalahan yang harus dipecahkan. Pertama, aspek tertulis. Kedua, dibuat oleh atau di hadapan pejabat negara yang berwenang atau pegawai umum.

[33] Jusuf Patrianto Tjahjono, 2008, *Dengan Berlakunya Undang-undang Nomor 11 tahun 2008 Tentang Informasi Dan Tanda Tangan Elektronik*, www. Legal-hukum.co.id.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Agar dapat diklasifikasikan dalam bentuk tertulis, ada beberapa cara yang dapat dilakukan, salah satunya yang lazim dilakukan adalah membuat suatu printout copy dari pesan yang masih berbentuk elektronik tersebut. Masalahnya hanya terletak pada tidak adanya satu peraturan hukum pun di Indonesia yang mengatur mengenai pengubahan dari bentuk data elektronik ke bentuk printout. Yang sudah ada aturannya justru kebalikannya yaitu dari bentuk nyata tertulis ke bentuk data elektronik, diatur dalam UU Dokumentasi Perusahaan pada Bab III Pengalihan bentuk Dokumen Perusahaan dan Legalisasi dari Pasal 12 sampai dengan Pasal 16. Kenapa hal ini menjadi penting dan dikemukakan, karena bila terjadi suatu perubahan bentuk dari suatu dokumen atau pesan, maka harus dapat dibuktikan bahwa perubahan bentuk tersebut tidak merubah isi dari dokumen/pesan yang diubah bentuknya itu. Konsekuensi hukumnya, kekuatan pembuktian dari bentuk ubahan tersebut harus sama sesuai kekuatan pembuktian dari bentuk asalnya.

Dari Pasal 1 point 4, Pasal 5 ayat (3), Pasal 6 dan Pasal 7 UU ITE dapat dikategorikan syarat formil dan materiil dari dokumen elektronik agar mempunyai nilai pembuktian, yaitu :

1. Berupa informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan, yang dapat dilihat, ditampilkan dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tulisan, suara, gambar dan seterusnya yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya;
2. Dinyatakan sah apabila menggunakan atau berasal dari Sistem Elektronik sesuai dengan ketentuan yang diatur dalam undang-undang;
3. Dianggap sah apabila informasi yang tecantum didalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Dari syarat-syarat formil dan materiil tersebut dapat dikatakan bahwa dokumen elektronik agar memenuhi batas minimal pembuktian

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

haruslah didukung dengan saksi ahli yang mengerti dan dapat menjamin bahwa sistem elektronik yang digunakan untuk membuat, meneruskan, mengirimkan, menerima atau menyimpan dokumen elektronik adalah sesuai dengan ketentuan dalam undang-undang; kemudian juga harus dapat menjamin bahwa dokumen elektronik tersebut tetap dalam keadaan seperti pada waktu dibuat tanpa ada perubahan apapun ketika diterima oleh pihak yang lain (*integrity*), bahwa memang benar dokumen tersebut berasal dari orang yang membuatnya (*authenticity*) dan dijamin tidak dapat diingkari oleh pembuatnya (*non repudiation*).

Hal ini bila dibandingkan dengan bukti tulisan, maka dapat dikatakan dokumen elektronik mempunyai derajat kualitas pembuktian seperti bukti permulaan tulisan (*begin van schriftelijke bewijs*), dikatakan seperti demikian oleh karena dokumen elektronik tidak dapat berdiri sendiri dalam mencukupi batas minimal pembuktian, oleh karena itu harus dibantu dengan salah satu alat bukti yang lain. Dan nilai kekuatan pembuktiannya diserahkan kepada pertimbangan hakim, yang dengan demikian sifat kekuatan pembuktiannya adalah bebas (*vrij bewijskracht*). Berdasarkan penalaran hukum di atas, maka dapatlah disimpulkan dokumen elektronik dalam hukum acara perdata dapat dikategorikan sebagai alat bukti persangkaan Undang-undang yang dapat dibantah (*rebuttable presumption of law*) atau setidak-tidaknya persangkaan hakim (*rechtelijke vermoden*).

Ketentuan yang ada dalam pasal-pasal tersebut menyebutkan, bahwa suatu bentuk tertulis nyata (dalam hal ini segala tulisan yang dibuat berkenaan dengan kegiatan perusahaan) dapat diubah ke bentuk lain (contohnya mikrofilm atau CD) setelah sebelumnya dilakukan suatu verifikasi dan legalisasi yang dalam hal ini dilakukan oleh pimpinan perusahaan atau pejabat yang ditunjuk di lingkungan perusahaan dengan dibuatkan suatu berita acara. Setelah ada verifikasi dan legalisasi bahwa kedua bentuk dokumen tersebut isinya sama secara keseluruhan maka sebagaimana disebutkan dalam Pasal 15 ayat (1) UU.ITE maka media hasil transformasi tersebut dan atau hasil cetaknya merupakan alat bukti

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

yang sah.

Dan mengenai isi Rencana Peraturan Pemerintah (RPP) tentang tanda tangan elektronik, yaitu dalam Pasal 1 memuat diantaranya : ”Tangan Tangan Elektronik adalah informasi elektronik yang dilekatkan, memiliki hubungan langsung atau terasosiasi pada suatu informasi elektronik lain yang dibuat oleh penandatangan untuk menunjukkan identitas dan statusnya sebagai subyek hukum, termasuk dan tidak terbatas pada penggunaan infrastruktur kunci publik (tanda tangan digital), biometrik, kriptografi simetrik, termasuk di dalamnya tanda tangan dalam bentuk asli yang diubah menjadi data elektronik”

Yang menjadi pertanyaan penting adalah : Apakah tanda tangan dalam bentuk asli yang diubah menjadi data elektronik memiliki kekuatan hukum dan akibat hukum yang sah?

Jika tanda tangan asli serta informasi yang ditanda tangani di atas kertas diubah ke data elektronik dengan peralatan scanner, maka cara ini tidak memiliki kekuatan hukum dan akibat hukum yang sah. Berikut penjelasannya:

1. Perlu dipahami dengan baik bahwa tanda tangan bertujuan untuk menyatakan persetujuan atas informasi yang disepakati oleh para pihak yang bertransaksi, dan mengidentifikasi siapa yang menandatangani.
2. Ada perbedaan tanda tangan dan informasi yang ditanda tangani antara di atas kertas dan secara elektronik. Kertas menjadi perekat antara tanda tangan dan informasi yang ditanda tangani, jika terjadi perubahan pada tanda tangan atau informasi yang ditanda tangani maka perubahan itu mudah dikenali misalnya adanya coretan.

Secara elektronik, bisa saja seseorang yang berniat jahat mengganti informasi elektronik yang telah ditanda tangani oleh para pihak dengan informasi elektronik lain tetapi tanda tangan tidak berubah. Dan kenyataannya pada data elektronik perubahan ini mudah terjadi dan tidak mudah dikenali. Oleh karena itu, tanda tangan elektronik harus terasosiasi

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

dengan informasi elektronik yang ditanda tangani seperti dimaksudkan pada Pasal 1 UU ITE untuk definisi Tanda Tangan Elektronik.

Yang dimaksudkan terasosiasi adalah informasi elektronik yang ingin ditanda tangani menjadi data pembuatan tanda tangan elektronik. Dengan demikian, antara tanda tangan elektronik dan informasi elektronik yang ditanda tangani menjadi erat hubungannya seperti fungsi kertas. Keuntungannya adalah jika terjadi perubahan informasi elektronik yang sudah ditanda tangani maka tentu tanda tangan elektronik juga seharusnya berubah. Tanda tangan elektronik dari informasi elektronik yang telah berubah dan bandingkan dengan tanda tangan elektronik yang ada, tentu hasilnya beda, dan ini menunjukkan bahwa informasi elektronik yang ditanda tangani telah mengalami perubahan.

Jika kita simak pasal 11 ayat 1 bagian c dan d, mewajibkan adanya metode untuk mengetahui segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dan mengetahui segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan. Perubahan itu dapat diketahui hanya apabila informasi elektronik menjadi data pembuatan tanda tangan elektronik.

Bagaimana dengan tanda tangan asli serta informasi yang ditanda tangani di kertas diubah ke data elektronik dengan peralatan scanner, apakah memiliki kekuatan hukum dan akibat hukum yang sah? Tentu tidak memiliki kekuatan hukum dan akibat hukum yang sah, karena tanda tangan itu tidak dibuat berdasarkan informasi yang disepakati atau dengan kata lain informasi yang disepakati tidak menjadi data pembuatan tangan tangan, sehingga perubahan tanda tangan elektronik dan/atau informasi elektronik setelah waktu penandatanganan tidak dapat diketahui.

2.3.1 Aspek Perlindungan Konsumen Dalam Penggunaan *Digital Signature*

Secara Nasional, pranata untuk memberikan perlindungan terhadap konsumen adalah UU No. 8 Tahun 1999 tentang Perlindungan Konsumen, namun UU perlindungan Konsumen ini secara khusus belum

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

mengantisipasi perkembangan teknologi informasi di dalam pengaturannya.

Dalam penggunaan *Digital Signature* kita mengenal adanya dua pihak, yaitu:

1. Certificate Authority (CA)

2. Subscriber

Hubungan ini menunjukkan kaitan antara CA sebagai penyelenggara jasa dan subscriber sebagai konsumen. Sebagai penyelenggara jasa, CA harus menjamin hak-hak subsscriber antara lain:

1. Privacy

Termaktub dalam pasal 4 butir 1 UU NO 8 tahun 1999. Contoh: Ketika subscriber meng"*apply*" kepada CA, subs akan dimintai keterangan mengenai identitasnya, besar kecilnya keakuratan dari identitas tersebut tergantung dari jenis tingkatan sertifikat tersebut. Semakin tinggi tingkat sertifikat maka semakin akurat pula identitas sebenarnya dari subscriber.

Namun dalam hal ini yang perlu diperhatikan adalah CA sebagai penyimpan data berkewajiban menjaga kerahasiaan identitas subs dari pihak yang tidak berkepentingan. CA hanya boleh mengkonfirm bahwa sertifikat yang dimiliki oleh subs adalah benar dan diakui oleh CA.

Di beberapa negara maju data pribadi mendapat perlindungan dalam undang-undang (*data protection act*). Di dalam Undang-Undang yang bersangkutan tercantum prinsip perlindungan data (*Data Protection Principles*) yang harus ditaati oleh orang-orang yang menyimpan atau memproses informasi dengan mempergunakan komputer yang menyangkut kehidupan orang-orang. Biro-biro komputer yang menyediakan jasa pelayanan bagi mereka yang hendak memproses informasi juga sama dikontrol dan harus melakukan pendaftaran menurut undang-undang tersebut. Individu-individu, yang informasi dirinya disimpan pada komputer, diberi hak-hak untuk akses dan hak untuk memperoleh catatan-catatan pembetulan dan penghapusan informasi yang tidak benar. Mereka itu pun dapat mengajukan pengaduan kepada Data Protection Registrar (yang daingkat berdasarkan undang-undang) apabila

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

mereka tidak merasa puas terhadap cara orang atau organisasi yang mengumpulkan informasi dan, menurut keadaan-keadaan tertentu, individu-individu memiliki hak atas ganti kerugian.

Pelanggaran terhadap prinsip-prinsip perlindungan data dapat menyebabkan tanggung jawab pidana, adapun prinsip-prinsip tersebut antara lain:

1. Informasi yang dimuat dalam data pribadi harus diperoleh, dan data pribadi itu harus diproses, secara jujur dan sah.
2. Data pribadi harus dipegang hanya untuk satu tujuan atau lebih yang spesifik dan sah.
3. Data pribadi yang dikuasai untuk satu tujuan dan tujuan-tujuan tidak boleh digunakan atau disebarluaskan dengan melalui suatu cara yang tidak sesuai dengan tujuan atau tujuan-tujuan tersebut.
4. Data pribadi yang dikuasai untuk keperluan suatu tujuan atau tujuan-tujuan harus layak, relevan dan tidak terlalu luas dalam kaitannya dengan tujuan atau tujuan-tujuan tersebut
5. Data pribadi harus akurat dan, jika diperlukan, selalu *up-to date*.
6. Data pribadi yang dikuasai untuk keperluan suatu tujuan atau tujuan-tujuan tidak boleh dikuasai terlalu lama dari waktu yang diperlukan untuk kepentingan tujuan atau tujuan-tujuan tersebut.
7. Tindakan-tindakan pengamanan yang memadai harus diambil untuk menghadapi akses secara tidak sah, atau pengubahan, penyebarluasan atau pengrusakan data pribadi serta menghadapi kerugian tidak terduga atau data pribadi.
8. Seorang individu akan diberikan hak untuk:
    a. Dalam jangka waktu yang wajar dan tanpa kelambatan serta tanpa biaya, yaitu dengan diberi penjelasan oleh pihak pengguna data tentang apakah pihaknya menguasai data pribadi di mana individu yang bersangkutan menjadi subyek data. Dan untuk akses pada suatu data demikian yang dikuasai oleh pihak pengguna data.
    b. Jika dipandang perlu, melakukan perbaikan atau penghapusan

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

data.

Prinsip yang terakhir berkaitan dengan pengamanan dan ancaman terhadap hal ini ada dua jenis:

1. Pengamanan dari akses tidak sah, dan
2. Berkaitan dengan *copy-copy back up*. pusat-pusat data yang berisi data pribadi.

Masih berkaitan dengan masalah jaminan privacy dalam kaitannya dengan kunci privat, adalah harus adanya jaminan bahwa CA tidak berusaha mencari pasangan kunci publik dari susbscriber. CA mempunyai peluang yang besar untuk bisa menemukan kunci pasangan dari subscriber karena CA mempunyai komputer yang lebih canggih untuk menemukannya.

Selain itu harus ada jaminan bahwa pencipta kartu yang berisikan kunci privat juga tidak akan menyebarluaskan atau pun menggandakannya. Hal ini sangat logis sekali karena pembuat kartu selain mengetahui kunci publik juga mengetahui kunci privatnya karena ia adalah penciptanya. Untuk menjamin hal ini perlu adanya suatu notary sysrem yang menjamin hal tersebut.

2. Accuracy

Termaktub dalam pasal 4 butir 2,3, dan 8 UU No 8 tahun 1999. Dalam prinsip ini terkandung pengertian "ketepatan" antara apa yang diminta dengan apa yang didapatkan. Bahwa apa yang didapat oleh subs sesuai dengan apa yang ia minta berdasarkan informasi yang diterimanya. Ketepatan informasi (informasi yang benar tanpa tipuan) juga merupakan prinsip accuracy. Sebagai contoh: subs yang meminta level tertentu dari sertifikat sebaiknya tidak diberikan level yang lebih rendah atau lebih tinggi.

CA juga berkewajiban memberitahukan segala keterangan yang berkaitan dengan penawaran maupun permintaan yang diajukan.

Secara tidak langsung subs berhak untuk mendapatkan CA yang berlisensi artinya ketika subs mengakses ke CA, terdapat praduga bahwa CA adalah CA yang sah dan berlisensi dan subs harus dilindungi dari

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

penyimpangan CA yang gadungan.

3. Property

Termaktub dalam pasal 4 buutir 8 UU No 8 tahun 1999. Subs harus dilindungi hak miliknya dari segala penyimpangan yang mungkin terjadi akibat masuknya subs ke dalam sistem ini. Artinya subs berhak dilindungi dari segala bentuk penyadapan, penggandaan, dan pencurian. Jika hal ini terjadi maka CA berkewajiban mengganti kerugian yang diderita.

4. Accessibility

Termaktub dalam pasal 4 butir4, 5, 6,dan 7 UU No 8 tahun 1999. Bahwa setiap pribadi berhak medapat perlakuan yang sama dalam hal untuk mengakses dan informasi. Artinya tiap subs bisa masuk ke dalam sistem ini jika memenuhi persyaratan, dan ia bisa mempergunakan sistem ini tanpa adanya hambatan. Dan subs juga berhak untuk didengar pendapat dan keluhannya.

Hak-hak konsumen untuk tercapainya perlindungan konsumen sudah tercantum atau dituangkan dalam bentuk Undang-Undang, yaitu UU No 8 tahun 1999. Maka artinya hak-hak tersebut sudah diakui keberadaannya dan memiliki kepastian hukumnya yang diatur dalam Undang-Undang positif. Upaya hukum yang dilakukan oleh konsumen yang merasa dirugikan bisa menggunakan pasal-pasal dalam UU No 8 tahun 1999 ini. Dalam kaitannya dengan penggunaan digital signature , CA dalam kedudukan yang lebih kuat harus bisa menjamin hak-hak konsumen. Terutama dalam perjanjian adhesi antara CA dan subscriber. Perjanjian diajukan sebaiknya tidak hanya berat sebelah, sehingga subscriber tidak mempunyai posisi penawaran (bargaining power). Untuk menutup resiko atas produk-produk yang cacat CA dapat mengasuransikan resiko tersebut. Hal ini untuk mengurangi beban yang harus ditanggung oleh CA apabila suatu saat ada konsimen (subscriber) yang menuntut CA karena merasa dirugikan. Dalam Undang-Undang Perlindungan Konsumen telah diatur pula hak dan kewajiban pelaku usaha serta larangan-larangan yang bertujuan untuk memberi perlindungan terhadap konsumen dan telah pula mengatur mengenai hak dan kewajiban

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

konsumen.

Namun khusus untuk perlindungan hak konsumen dalam transaksi *e-commerce* masih rentan, karena walaupun Undang-undang Perlindungan Konsumen telah mengatur hak dan kewajiban bagi produsen dan konsumen, namun kurang tepat untuk diterapkan dalam transaksi *e-commerce*. Kemajuan ilmu pengetahuan dan teknologi dalam proses produksi barang dan jasa ternyata belum diikuti dengan kemajuan perangkat hukum yang ada.

2.3.2 Penyelesaian Sengketa Hukum Perdata di Indonesia.

Arbitrase *online* tidak berbeda dengan arbitrase konvensional, yang berbeda hanyalah tata cara pelaksanaannya. Namun, timbul permasalahan menyangkut syarat sah dari perjanjian arbitrase yaitu tertulis dalam suatu dokumen dan ditandatangani.[34] Permasalahannya adalah bagaimana cara pemenuhan syarat tersebut dalam arbitrase *online*. Untuk itu perlu dijelaskan sebagai berikut.

1. Perjanjian Arbitrase, Tertulis Tidak Selalu Harus Tercetak

Undang-undang Nomor 30 Tahun 1999 memang menentukan perjanjian arbitrase harus tertulis. Timbul suatu pertanyaan, apakah yang dimaksud dengan tertulis berarti tulisan diatas media kertas. Undang-undang tidak menjelaskan lebih lanjut. Penyelesaian sengketa melalui arbitrase konvensional mendasarkan kegiatannya pada pertukaran dan pemeriksaan dokumen bermedia kertas (*paperbase*). Sedangkan, dalam arbitrase *online*, media kertas telah digantikan oleh data digital sehingga tidak lagi diperlukan adanya dokumen berbentuk kertas (*paperless*). Jika isu orisinalitas yang menjadi acuan harus digunakannya dokumen cetak bermedia kertas, saat ini sudah tidak relevan lagi. Masyarakat sering memahami bahwa suatu dokumen yang asli adalah dokumen yang tertulis di atas kertas, padahal untuk suatu sistem dokumentasi yang menggunakan komputer, dokumen yang asli sebenarnya adalah dalam bentuk data elektronik (*softcopy*) yang tersimpan dalam *hardisk* komputer bukan dalam

[34] Indonesia, *Undang-undang Tentang Arbitrase dan Pilihan Penyelesaian Sengketa*, UU No. 30, LN. No. 138 Tahun 1999, TLN. No. 3872.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

bentuk cetaknya (*hardcopy*).[35] Dengan demikian, nilai ataupun eksistensi suatu pernjanjian secara substansial tidak bergantung pada media apa yang digunakan sebagai fiksasinya, melainkan tergantung pada proses terjadinya perjanjian itu sendiri. Contohnya, suatu perjanjian arbitrase yang tertulis di atas kertas pun kalau proses penyusunannya tidak memenuhi syarat sah perjanjian maka batal demi hukum. Dapat disimpulkan, meskipun perjanjian arbitrase dibuat dalam bentuk data elektronik dan di-*online*-kan, sepanjang dapat dibuktikan prosesnya berjalan dengan baik dan dilakukan oleh pihak yang berhak, tetap memiliki kekuatan mengikat para pihak yang membuatnya. Adapun dimaksud dengan proses di sini adalah proses pada memasukkan data (*input*), proses pengolahan data (*editing*), proses penyimpanan data (*storing*), proses keluaran data atau tampilan data (*output*). *Ouput* suatu data tidak selalu harus berupa wujud fisik, tampilan pada layar monitor juga termasuk *data output*. Dalam hal ini berlakulah ketentuan dalam Pasal 1338 KUHPerdata yang menyatakan "Perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya."[36] Sebagai contoh sudah diterimanya perjanjian arbitrase *online* dalam pelaksanaan arbitrase *online* dapat dilihat ketentuan pelaksanaan arbitrase yang dikeluarkan oleh *America Arbitration Association* (AAA) pada *Supplementary Rules* untuk arbitrase *online* yang telah mengadopsi perjanjian dalam bentuk *online*. Hal ini terlihat dari pengantar *Supplementary Rules* yang menyatakan:

"The purpose of the Supplementary Procedures for Online Arbitration is to permit, where the parties have agreed to arbitration under these Supplementary Procedures, arbitral proceedings to be conducted and resolved exclusively via the Internet. The Supplementary Procedures provide for all party submissions to be made online, and for the arbitrator, upon review of such submissions, to render an award and to communicate

[35] Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian* (Jakarta: PT RajaGrafindo Persada, 2005) hlm. 239.

[36] *Kitab Undang-undang Hukum Perdata (Burgerlijk Wetboek) dengan Tambahan Undang-undang Pokok Agraria dan Undang-undang Perkawinan*, diterjemahkan oleh R. Subekti dan R. Tjitrosudibio, cet. 33, (Jakarta: Pradnya Paramita, 2003), psl. 1338.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

it to the parties via the Internet..."[37]

2. Perjanjian Arbitrase Harus Ditandatangani

Berdasarkan Pasal 4 ayat (2) Undang-undang Nomor 30 Tahun 1999, perjanjian arbitrase dimuat dalam satu dokumen dan ditandatangani. Artinya, suatu perjanjian arbitrase sah apabila telah ditandatangai oleh para pihak yang membuatnya. Timbul suatu pertanyaan, apakah tanda tangan dalam pasal tersebut hanya diartikan secara sempit yaitu sebagai tanda tangan hitam diatas putih? Perkembangan teknologi telah menggeser bentuk tanda tangan yang sebelumnya hanya di atas kertas, kini tanda tangan dapat berupa tanda tangan digital atau yang biasa disebut *Digital Signature* (DS).

Penggunaan tanda tangan dalam kegiatan sehari-hari secara harfiah disamakan dengan penggunaan DS dalam Internet yaitu ditujukan untuk nilai keotentikan suatu data atau informasi. Perbedaannya adalah, tanda tangan lazimnya merupakan kombinasi atau variasi dari nama atau singkatan nama seseorang. Di lain pihak dalam Internet tanda tangannya berupa kombinasi digital, yaitu kombinasi dari bilangan biner 0 dan 1 yang diinterpretasikan menjadi karakter yang unik dan melalui proses penyandian (*enkripsi*).

Tanda tangan digital sering disalahartikan menjadi tanda tangan di atas kertas lalu dengan melalui proses *scanning,* tanda tangan tersebut dimasukkan (*input*) kedalam komputer sehingga menjadi gambar tanda tangan yang kemudian dilekatkan dengan suatu dokumen untuk menyatakan dokumen tersebut "telah ditandatangani". Tidak jarang tanda tangan digital juga dipahami sebagai tanda tangan yang dibuat langsung di komputer menggunakan *mouse* sehingga berbentuk tanda tangan seperti lazimnya tanda tangan di atas kertas.[38]

Kembali ke pokok permasalahan yaitu apakah tanda tangan yang dimaksud Pasal 4 ayat (2) Undang-undang Nomor 30 Tahun 1999 terbatas

---

[37] American Arbitration Association, "Supplementary Procedures for *Online* Arbitration, diperoleh dari penelusuran data pada website WestLaw yang diakses menggunakan proxy Fakultas Hukum Universitas Indonesia *http://www.law.ui.ac.id/westlaw/index.php.*

[38] *http://www.wikipedia.org/digital_signature*

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

pada pengertian tanda tangan sebagai hitam di atas putih? Perlu dilihat dari pentingnya tanda tangan dalam perjanjian arbitrase. Dalam Pasal 9 ayat (2) Undang-undang Nomor 30 Tahun 1999 dikatakan apabila para pihak tidak menandatangani perjanjian arbitrase, maka perjanjian tersebut dibuat dalam bentuk akta notaris. Pasal ini menjelaskan tujuan tanda tangan dalam perjanjian arbitrase yaitu untuk keperluan pembuktian keotentikan perjanjian arbitrase tersebut.

Mark Taylor dalam tulisannya yang berjudul *Uses of Encryption: Digital Signatures* mengatakan:

Digital signatures designed in such a way that the authenticity and integrity of the data to which they are attached can be assured. In essence, the key issues for data which have been signed digitaly are:

1. *Whether those data have been altered between their being signed and being read or received by the intended recipient; and*
2. *Whether those data were actually signed by the person by whom the data purport to have been signed or whether the signature attached to them is forged in some way.*[39]

Jadi, apabila keperluan tanda tangan dalam perjanjian arbitrase adalah untuk pembuktian, perlindungan keotentikan suatu dokumen yang menggunakan tanda tangan digital jauh lebih kuat, karena sebuah tanda tangan digital memiliki karakter yang sangat unik dan telah tersandikan (*encrypted*) sehingga kemungkinan ditiru sangat kecil. Berdasarkan hal tersebut, seharusnya penggunaan tanda tangan digital dalam perjanjian arbitrase, khususnya perjanjian arbitrase *online* tidak usah dipermasalahkan. Justru dengan adanya tanda tangan digital seluruh data dalam proses arbitrase akan terlindung kerahasiaan dan keotentikannya, karena yang dapat membuka data tersebut hanyalah pihak yang tanda tangannya telah di-*accept* dalam dokumen saja yang dapat membuka dokumen.

Selain harus dipenuhinya persyaratan perjanjian arbitrase

[39] Mark Taylor, *Uses of Encryption: Digital Signatures,* (USA: Sweet & Maxwell Limited and Contributors, 1999), hlm. 2

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

sebagaimana dijelaskan sebelumnya, suatu proses arbitrase *online* memerlukan prosedur dan kelengkapan yang berbeda dengan proses arbitrase konvensional. Dalam sub bab selanjutnya akan diuraikan prosedur dan kelengkapan yang dibutuhkan untuk melangsungkan arbitrase *online*.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

BAB III
KESIMPULAN DAN SARAN

3.1. Kesimpulan

Berdasarkan penelitian dan pembahasan yang telah diuraikan pada bab sebelumnya, maka dapat disimpulkan bahwa :

1. Kedudukan dan kekuatan hukum dari tanda tangan elektronik sebagai bukti adalah berlandaskan kepada Pasal 11 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang ini memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum. Persyaratan yang disebutkan dalam Pasal 11 UU.ITE merupakan persyaratan minimum yang harus dipenuhi dalam setiap tanda tangan elektronik. Untuk pengaturan tanda tangan elektronik di tingkat internasional diatur dalam Pasal 7 UNCITRAL Model Law (The United Nations Commisions on International Trade Law) merupakan salah satu organisasi yang pertama kali mulai membahas perkembangan teknik informatika dan dampaknya terhadap perniagaan elektronik.
2. Tanggapan yang timbul mengenai keabsahan tanda tangan elektronik sebagai bukti adalah berbeda-beda dari penafsiran hukum masalah yang dialami. Dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik keabsahan tanda tangan elektronik diakui secara sah, Dalam pasal 5 ayat 1 dan 2 UU.ITE hanya disebutkan bahwa dokumen elektronik dan/atau hasil cetaknya adalah alat bukti hukum yang sah dan merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia, tetapi apabila penulis melihat perbandingan antara Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dengan Undang-Undang Nomor 30 Tahun 2004

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

tentang Jabatan Notaris maka keabsahan tanda tangan elektronik tidaklah sah, dikarenakan dalam UUJN bukti yang sah itu adalah akta otentik dan akta bawah tangan. Dan Notaris itu sendiri harus datang, melihat dan mendengar dalam setiap pembuatan akta dan ditanda-tangan oleh notaris itu sendiri dan para penghadap masing-masing langsung di tempat dibacakannya akta itu oleh Notaris. Dan haruslah tanda tangan asli dari Notaris dan para penghadap bukanlah tanda tangan elektronik yang bisa ditorehkan di dalam akta tersebut karena kekuatan pembuktian dalam hukum di Indonesia tidaklah sah.

3. Penggunaan dan pelaksanaan dan kekuataan bukti elektronik dalam perkara perdata adalah dalam proses persidangan perdata dokumen elektronik yang ditandatangani dengan tanda tangan elektronik didalam hukum pembuktian di Indonesia, diakui esensinya setelah diatur di dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa informasi elektronik atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah, dan merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia hal tersebut berdasarkan ketentuan pada Pasal 5 ayat 2 Undang-Undang Nomor 11 Tahun 2008. Berdasarkan pada Pasal 164 HIR dan Pasal 284 RBg, alat-alat bukti yang sah terdiri dari bukti tulisan, bukti dengan saksi-saksi, persangkaan- persangkaan, pengakuan dan sumpah. Oleh karena itu, alat bukti menurut hukum acara di atas yang dibuat dalam bentuk informasi elektronik/dokumen elektronik, dan informasi elektronik atau dokumen elektronik itu sendiri, merupakan alat bukti yang sah menurut Undang-Undang Informasi dan Transaksi Elektronik.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

3.2 Saran

Menurut saya pemerintah haruslah membuat Undang-Undang yang lebih jelas dan tertuju pada satu pembahasan pokok masalah yang sama yaitu apakah untuk kasus perdata mengenai transaksi elektronik khususnya mengenai tanda tangan elektronik itu dengan menggunakan aturan Undang-Undang di Indonesia dapat digunakan sebagai alat bukti yang sah tanpa mengesampingkan aturan dari UUJN yang sudah ada dasar mengenai alat bukti yang sah.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

DAFTAR REFERENSI

1. Buku

Adjie, Habib., 2008, *Sanksi Perdata Dan Administratif Terhadap Notaris Sebagai Pejabat Publik*, PT. Refika Aditama, Bandung.

Adam, Muhammad, 1985, *Asal Usul Dan Sejarah Akta Notariat*, CV. Sinar Baru, Bandung.

Ahmaturrahman., 2005, *Hukum Acara Perdata Di Indonesia*, Universitas Hukum Universitas Sriwijaya, Palembang.

Badrulzaman, Mariam Darus., *E-Commerce : Tinjauan Dari Hukum Kontrak Indonesia*, Volume 12, Jakarta.

Barkatullah, Abdul Prasetyo., Halim Teguh, 2005, *Bisnis E-commerce Studi Sistem Keamanan Dan Hukum Di Indonesia*, Pustaka Pelajar, Jakarta.

Kie, Tan Thong., 2007, *Studi Notariat dan Serba-Serbi Praktek Notaris*, PT.Ichtiar Baru Van Hoeve, Jakarta.

Makarim, Edmon., 2003, *Kompilasi Hukum Telematika*, Cetakan 1, Edisi 1, PT Raja Grafindo Persada, Jakarta.

Muljadi, Kartini., dan Widjaja, Gunawan., 2003, *Perikatan Pada Umumnya*, PT.Raja Grafindo, Jakarta.

Partodihardjo, Soemarno, 2009, *Tanya Jawab Sekitar Undang-Undang No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*, PT Gramedia Pustaka Utama, Jakarta.

Prodjodikoro, Wirjono., 1981, *Hukum Perdata Tentang Persetujuan-Persetujuan Tertentu*, Sumur Bandung, Jakarta.

Soekanto, Soerjono., 1984, *Pengantar Penelitian Hukum*, UI Press, Jakarta.

Soekanto, Soerjono,. dan Abdurrahman., 2003 *Metode Penelitian Hukum*, Cetakan Kedua, Rineka Cipta, Jakarta.

Soekanto, Soerjono., dan Mamudji, Sri., 1990, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Rajawali Press, Jakarta.

Soemitro, Ronny Hanitijo., 1990, *Metodologi Penelitian Hukum Dan Judimetri*, *Ghalia Indonesia*, Jakarta.

Sugiyono., 2003, *Metode Penelitian Administrasi*, Alfabeta, Bandung.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

Sutopo, HB., 1998, *Metodologi Penelitian Kualitatif* Bagian 11, UNS Press-Surakarta.

Tobing, Lumban G.H.S., 1980, *Peraturan Jabatan Notaris*, Erlangga, Jakarta.

2. Peraturan Perundang-Undangan

Undang-Undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-Undang Nomor 30 tahun 2004 Tentang Jabatan Notaris.

Undang-Undang Nomor 30 tahun 2009 Tentang Perlindungan Konsumen

Undang-Undang Nomor 30 tahun 1999 Tentang Arbitrase dan Alternatif Penyelesaian Sengketa

Rancangan Peraturan Pemerintah Tentang Tanda Tangan Elektronik.

Rancangan Peraturan Pemerintah Tentang Sertifikasi Elektronik.

3. Artikel/Makalah/Bahan Kuliah

Khairandy, Ridwan., 2001, *Pembaharuan Hukum Kontrak Sebagai Antisipasi Transaksi Elektronic Commerce*, Jurnal Hukum Bisnis, vol.16.

Committee, Information Security, 1996, *Section of Science & Technology – American Bar Association*, Digital Signature Guideliness (United States, American Bar Association.

4. Surat Kabar

Surya, 23 Januari 2007, *Keamanan Transaksi Secara Elektronik*, Harian Surat Kabar Bisnis Indonesia.

5. Internet

Dimyati, Kudzaifah., dan Wardiono, Kelik., 2008, *Dinamika Pemikiran Hukum*, www.google.com.

Dwipayono, Julius Indra., 2005, *Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia*, www.legalitas.org.

Gema, Ario Juliano ., 2008, *Apakah Dokumen Elektronik Dapat Menjadi Alat Bukti Yang Sah*, www.Legalminded.com.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.

I.B.R. Supancana, 2003, *Kekuatan Akta Elektronis Sebagai Alat Bukti Pada Transaksi l-commerce Dalam Sistem Hukum Indonesia*, www.Indoregulation.com.

Ronny, 2008, *Sembilan Peraturan Pemerintah Dan Dua Lembaga Yang Baru Undang-Undang Informasi Transaksi Elektronik*, www.ronny-hukum.blogspot.com.

Salam, Abdul., 2008, *Alat Bukti Elektronik*, www.blog.ui.edu/abdul.salam.

Tandiabang, Ronald Makaleo., Patria, Tomy Handaka., dan Barnea ,Anang., 2005, *Otentikasi Dokumen Elektronik Menggunakan Tanda Tangan Digital*, www.itb.go.id.

Tjahjono, Jusuf Patrianto, 2008, *Dengan Berlakunya Undang-undang Nomor 11 tahun 2008 Tentang Informasi Dan Tanda Tangan Elektronik*, www. Legal-hukum.co.id.

Keabsahan tanda..., Joan Venzka Tahapary, FH UI, 2011.