ASPEK HUKUM TANDA TANGAN DIGITAL DAN OTORITAS SERTIFIKASI DALAM TRANSAKSI PERDAGANGAN SECARA ELEKTRONIK

(E-COMMERCE)

Oleh:

DEASY MAULIANA

B 111 02 120

PROGRAM KEKHUSUSAN HUKUM EKONOMI

FAKULTAS HUKUM UNIVERSITAS HASANUDDIN

MAKASSAR

2006

HALAMAN JUDUL

ASPEK HUKUM TANDA TANGAN DIGITAL DAN OTORITAS SERTIFIKASI DALAM TRANSAKSI PERDAGANGAN SECARA ELEKTRONIK *(E-Commerce)*

Oleh

DEASY MAULIANA

B11102120

SKRIPSI

Diajukan sebagai Tugas Akhir dalam rangka Penyelesaian Studi Sarjana dalam Program Kekhususan Hukum Ekonomi Program Studi Ilmu Hukum

Pada

FAKULTAS HUKUM
UNIVERSITAS HASANUDDIN

MAKASSAR
AGUSTUS 2006

PENGESAHAN SKRIPSI

ASPEK HUKUM TANDA TANGAN DIGITAL DAN OTORITAS SERTIFIKASI DALAM TRANSAKSI PERDAGANGAN SECARA ELEKTRONIK (E-COMMERCE)

Disusun dan diajukan oleh

DEASY MAULIANA
NIM B 111 02 120

Telah dipertahankan di hadapan Panitia Ujian Skripsi yang Dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Kekhususan Hukum Ekonomi Program Studi Ilmu Hukum
Fakultas Hukum Universitas Hasanuddin
Pada Kamis, 10 Agustus 2006
Dan dinyatakan diterima

Panitia Ujian

Ketua,

Prof. DR. Sukarno Aburaera, SH
NIP. 130 369 534

Sekretaris,

Rastiawaty, SH
NIP. 132 300 744

Dekan Fakultas Hukum Unhas,

Prof. DR. H. Syamsul Bachri, S.H., M.S.
NIP. 130 936 997

PERSETUJUAN PEMBIMBING

Diterangkan bahwa skripsi dari:

Nama	: Deasy Mauliana
Nomor Pokok	: B 111 02 120
Program Studi	: Ilmu Hukum
Program Kekhususan	: Hukum Ekonomi
Fakultas	: Hukum Universitas Hasanuddin
Judul	: Aspek Hukum Tanda Tangan Digital dan Otoritas Sertifikasi Dalam Transaksi Perdagangan Secara Elektronik *(E-Commerce)*.

Telah diperiksa dan disetujui untuk diajukan dalam ujian skripsi.

Makassar, Juli 2006

Pembimbing I	Pembimbing II
Winner Sitorus, S.H., M.H., LLM	**Hasbir, S.H., M.H**
NIP. 131 961 575	NIP. 132 126 336

PERSETUJUAN MENEMPUH UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa:

Nama	: Deasy Mauliana
Nomor Induk	: B 111 02 120
Program Kekhususan	: Hukum Ekonomi
Judul Skripsi	: Aspek Hukum Tanda Tangan Digital dan Otoritas Sertifikasi Dalam Transaksi Perdagangan Secara Elektronik *(E-Commerce)*

Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir program studi.

Makassar, 3 Agustus 2006

Dekan Fakultas Hukum Unhas,

Prof. DR. H. Syamsul Bachri, S.H., M.S.
NIP. 130 936 997

ABSTRAK

DEASY MAULIANA (B11102120), *Aspek Hukum Tanda Tangan Digital dan Otoritas Sertifikasi Dalam Transaksi Perdagangan Secara Elektronik (E-Commerce)*, (dibimbing oleh Winner Sitorus dan Hasbir).

Penelitian ini bertujuan untuk mengetahui pengaturan *Electronic Commerce* khususnya mengenai Tanda Tangan Digital di indonesia, keabsahan Tanda Tangan Digital sebagai alat bukti, dan kedudukan Otoritas Sertifikasi dalam pengaturan mengenai Tanda Tangan Digital.

Penelitian ini dilaksanakan di Kota Makassar, yaitu pada Pengadilan Negeri Makassar dengan mewawancarai salah satu hakim pada Pengadilan tersebut. Selain itu, penelitian juga dilaksanakan pada Perpustakaan Pusat Universitas Hasanuddin. Analisis data dilakukan dengan menggunakan analisis kualitatif.

Temuan yang diperoleh dari penelitian ini antara lain: adalah (1) Tanda Tangan Digital belum diatur sepenuhnya oleh hukum di Indonesia, sehingga yang menjadi acuan adalah peraturan yang bersifat umum, yaitu hukum perdata Indonesia dengan sistem terbuka dalam hal kebebasan membuat suatu perjanjian selama tidak bertentangan dengan norma-norma kesusilaan dan ketertiban umum serta tidak bertentang dengan hukum yang berlaku. (2) Tanda tangan digital dapat dijadikan alat bukti yang sah, walaupun tidak mempunyai kekuatan pembuktian yang sempurna, sehingga harus didukung dengan alat-alat bukti lainnya seperti alat bukti tulisan, keterangan saksi, persangkaan, pengakuan, atau sumpah. (3) Otoritas Sertifikasi berwenang untuk mengeluarkan suatu tanda tangan digital apabila *subscriber* telah memenuhi syarat-syarat yang telah ditetapkan sebelumnya oleh Otoritas Sertifikasi tersebut. Otoritas Sertifikasi bertanggungjawab terhadap kerahasiaan *subscriber* berdasarkan prinsip kepercayaan dan prinsip kehati-hatian.

UCAPAN TERIMA KASIH

Alhamdulillaahirabbil 'aalamiin. Puji syukur penulis panjatkan kehadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penyusunan skripsi yang berjudul "Aspek Hukum Tanda Tangan Digital dan Otoritas Sertifikasi dalam Transaksi Perdagangan Secara Elektronik *(E-Commerce)*" ini dapat penulis selesaikan.

Dalam penyusunan skripsi ini, banyak kendala yang dihadapi. Namun atas rahmat Allah SWT, upaya optimal dan bantuan dari berbagai pihak, skripsi ini dapat diwujudkan. Skripsi ini penulis persembahkan kepada kedua orang tua tercinta, ayahanda Prof. DR. H. Aminuddin Salle, SH., MH dan Ibunda Hj. Suryana Aminuddin Salle, SH., MH atas kasih sayang, dorongan, semangat dan fasilitas yang penulis peroleh.

Terima kasih dan penghargaan yang setinggi-tingginya penulis sampaikan kepada Bapak Winner Sitorus, SH., MH., L.Lm sebagai Pembimbing I, dan Bapak Hasbir SH., MH sebagai Pembimbing II, atas segala dedikasi, bimbingan dan arahannya.

Terima kasih kepada para penguji, Bpk. Prof. DR. Soekarno Aburaerah, S.H (ketua), Ibu Rastiawaty, S.H (sekretaris), Bpk. DR. Anwar Borahima, S.H.,M.H., Bpk. DR. Muzakkir, SH.MH, Ibu Harustiati A. Moein, SH.MH, dan Ibu Oky Deviany Burhamzah, SH.MH.

Terima kasih dan penghargaan yang setinggi-tingginya juga penulis sampaikan kepada:

1. Rektor Unhas beserta jajarannya, Dekan Fakultas Hukum Unhas, Bapak Prof. DR. H. Syamsul Bachri, SH.,MS beserta para Pembantu Dekan Fakultas Hukum Unhas.
2. Panitera Pengadilan Negeri Makassar, Bpk. H. Muhammad Ichwan, SH.,MH, dan Hakim Pengadilan Negeri Makassar, Bpk. Dewa PY Hardika, SH.,MH atas kesediaannya menjadi narasumber pada penelitian penulis.

3. Kakak-kakakku tersayang, Buyung Romadhoni, SE., M.Si dan Harmelia Ridwan Saleh, SE, Dhini Fakhdiana, ST, dan Irfan Sirajuddin ST, adikku Dina Fadhilah Monika, serta *my lovely niece*, Aliya Fatma Al-Humairah atas semangat dan dorongan yang telah diberikan.
4. Direktur Lembaga Bimbingan Balajar Multi Prima College, Staf, Rekan Pengajar dan siswa-siswaku di Makassar dan Sorowako atas kesempatan dan pengalaman berharga yang penulis peroleh.
5. *My sisters* yang selalu membuat indah hari-hari penulis: Rosyanna, Marhani Maruddin, SH, Fika Febriana, Irma Wahyuni, SH, Maryana Trisna Radhy, SH, Lidya Wijayanti, Elvy Afriany, SH dan Lis Yuni Amalia. *My brothers* yang selalu setia menemani, menjaga, dan selalu ada ketika dibutuhkan: Arianto, SH, Haris Yusuf, SH, Ariantony, SH, dan Steven Winarso, SH.
6. Teman-teman KKN Profesi Angkatan VIII Polsekta Tallo, Triasmi Mayairani, A. Mamminnanga, Indraswaty, Hijrawati, Rahmatiah, Novianty Pasong, Novie Priscella, Adee Fauziah, Fitrianitasari, Kak Surya Gerhana, Amal Hidayat, Kak Reagend, Kak Rahmat, Melati, dan Jinar Ariady.
7. Teman-teman angkatan 2002, Amanda, Adelia, Aryani Fauziah, Melissa, Asmi Yuliarni, Arjuna, Anugerah Ningrat, Hendra Ardiansyah, Muh.Jafar Goro, Eka Yani Prativi dan teman-teman yang tidak sempat penulis sebut satu per satu.

Akhirnya, kritik dan saran membangun sangat penulis harapkan. Semoga segala apa yang telah diberikan merupakan amal bakti yang senantiasa mendapat ganjaran pahala yang setimpal dari Allah SWT. Amin.

Makassar, Agustus 2006

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Pesatnya pertumbuhan teknologi informasi menghadirkan masyarakat informasi *(information society)*, yang ditandai dengan semakin meningkatnya penggunaan media telekomunikasi dalam berbagai aktivitas kehidupan masyarakat. Pemanfaatan internet sebagai media komunikasi yang sangat efisien, baik dari segi waktu maupun biaya mengalami perkembangan yang sangat maju sehingga pada akhirnya menempatkan informasi sebagai komoditas ekonomi yang sangat penting dan menguntungkan.

Salah satu pemanfaatan dalam internet yang semakin banyak diminati oleh masyarakat adalah *Electronic Commerce* (*E-Commerce*). *Electronic Commerce* merupakan suatu transaksi perdagangan yang menggunakan internet sebagai media perantara antara individu-individu, organisasi-organisasi atau badan, dimana para pelaku bisnis tidak memerlukan pertemuan secara langsung seperti yang terjadi pada transaksi tradisional.

Penggunaan internet dalam *Electronic Commerce* memberikan dampak yang sangat positif, yaitu kecepatan dan kemudahan serta kecanggihan dalam melakukan interaksi global tanpa batasan tempat dan waktu. Transaksi bisnis yang lebih praktis tanpa menggunakan pena dan kertas, tidak memerlukan pertemuan langsung *(direct meeting)*, efisien dalam segi waktu, sehingga dapat dikatakan bahwa perdagangan secara elektronik atau

E-Commerce ini menjadi penggerak ekonomi baru dalam bidang teknologi khususnya di Indonesia.

Implikasi dari pengembangan teknologi tersebut tentu saja membawa keuntungan seperti yang telah disebutkan di atas. Namun, ada pula sisi negatif dari pengembangan tersebut yaitu berkaitan dengan persoalan keamanan dalam bertransaksi dengan menggunakan *E-Commerce* dan secara yuridis mengenai jaminan kepastian hukumnya *(legal certainty)*.

Masalah keamanan masih menjadi masalah dalam internet. Aspek-aspek yang dipermasalahkan itu antara lain:

a. Kerahasiaan *(confidentiality)* pesan;
b. Bagaimana cara agar pesan yang dikirimkan itu keutuhannya *(integrity)* sampai ke tangan penerima;
c. Keabsahan *(authenticity)* pelaku transaksi;
d. Keaslian pesan agar bisa dijadikan barang bukti.

Perdagangan ini juga melahirkan dampak negatif yang seringkali muncul dalam bentuk penyelewengan-penyelewengan yang cenderung merugikan konsumen dalam melakukan *E-Commerce* atau perdagangan secara elektronik. Dampak negatif tersebut dapat ditemukan dalam hal seperti produk yang dipesan tidak sesuai dengan produk yang ditawarkan, kesalahan dalam pembayaran, ketidaktepatan waktu menyerahkan barang atau pengiriman barang dan hal-hal lain yang tidak sesuai dengan kesepakatan sebelumnya. Keberadaan konsumen yang melakukan bisnis *E-Commerce* tidak tervisual secara jelas mengingat transaksi dilakukan dalam

dunia maya, sehingga terdapat kemungkinan-kemungkinan seperti pihak yang melakukan transaksi mungkin saja pihak yang secara hukum tidak diperkenankan melakukan tindakan hukum. Sebagai contoh, pihak konsumen yang melakukan transaksi berusia di bawah ketentuan yang tercantum dalam syarat-syarat dalam melakukan transaksi, ataupun apabila telah terjadi kata sepakat oleh kedua belah pihak dan ketika akan ditelusuri pihak konsumen fiktif.[1]

Dalam kegiatan transaksi *E-Commerce*, tentu saja diperlukan suatu perjanjian. Perjanjian yang dilakukan di *cyberspace* peraturan dasarnya tidak memiliki perbedaan yang ekstrim dengan perjanjian konvensional pada umumnya. Namun bagaimanapun terdapat keadaan yang sama sekali baru atau dapat dikatakan merupakan penemuan baru dalam bidang teknologi informasi dan tidak ada ketentuan yang berlaku tegas untuk hal ini sehingga menimbulkan ketidakpastian hukum. Ketidakpastian hukum tersebut akan menimbulkan suatu dilema baru yang harus dihadapi oleh masyarakat dunia.

Pada prinsipnya bentuk suatu perjanjian adalah bebas dan tidak terikat pada bentuk tertentu, namun ada beberapa perjanjian yang wajib dibuat secara tertulis dan di hadapan pejabat yang berwenang sehingga mempunyai kekuatan pembuktian yang sempurna.

Sejalan dengan perkembangan teknologi saat ini dikenal istilah perjanjian digital (kontrak digital) yang mengenal pula istilah yang terkait dengan *Digital Signature* (tanda tangan digital) yang secara umum bukan

---

[1] Abdul Halim Barakatullah, Bisnis *E-Commerce*, Studi Sistem Keamanan dan Hukum di Indonesia (Yogyakarta:Pustaka Pelajar), hal. 4

diistilahkan sebagai tanda tangan tertulis atau nyata. Tanda tangan digital di sini merupakan transformasi (perubahan bentuk) pesan dengan menggunakan sistem kriptografi asimetris (sistem yang membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman dengan menggunakan kunci privat dan kunci publik) sehingga dengan demikian, penerima pesan tersebut dapat menguji apakah transformasi yang dilakukan menggunakan kunci privat yang berpasangan dengan kunci publiknya, serta menguji apakah pesan tersebut telah diubah sejak transformasi dilakukan terhadap pesan tersebut.[2]

Dalam hukum Internasional, *Digital Signature* telah diatur dalam UNCITRAL[3] *Model Law on Electronic Commerce 1996*. Di negara lain, misalnya Amerika Serikat telah memiliki *Digital Millenium Copyrigts Act* 1998, dan Malaysia yang telah memiliki *Digital Signature Act* 1997. Sedangkan di Indonesia, belum ada satu pun regulasi yang mengatur mengenai *Electronic Commerce*, khususnya mengenai *Digital Signature*.

Belum adanya konsepsi dan legislasi hukum yang kuat yang mengatur mengenai *Digital Signature* melahirkan suatu kebingungan tentang hukum apa yang akan digunakan apabila timbul permasalahan di kemudian hari. Sehingga dalam tulisan ini akan dibahas lebih lanjut mengenai hukum apa

---

[2] *Ibid.*

[3] *United Nations Commission on International Trade Law*, adalah sebuah badan PBB yang mengatur mengenai perdagangan melalui sarana elektronik. Hal-hal yang diatur antara lain mengenai *Digital Signature, Certification Authority*, dan hal-hal lain yang berkaitan dengan hukum. UNCITRAL berpusat di kota New York, Amerika Serikat, dan dibentuk pada tahun 1996.

yang akan digunakan mengenai bisnis *E-Commerce* melalui internet di Indonesia, khususnya dalam hal sistem pembuktian *Digital Signature*.

B. Rumusan Masalah

1. Bagaimanakah pengaturan hukum Perdagangan Secara Elektronik (*Electronic Commerce)* khususnya mengenai Tanda Tangan Digital dalam transaksi perdagangan di Indonesia?
2. Bagaimanakah keabsahan Tanda Tangan Digital sebagai alat bukti berdasarkan hukum di Indonesia?
3. Bagaimanakah kewenangan Otoritas Sertifikasi dalam pengaturan mengenai Tanda Tangan Digital?

C. Tujuan dan Kegunaan Penelitian

a. Tujuan Penelitian

1. Untuk mengetahui pengaturan hukum Tanda Tangan Digital di Indonesia.
2. Untuk mengetahui keabsahan Tanda Tangan Digital sebagai alat bukti berdasarkan hukum di Indonesia.
3. Untuk mengetahui kedudukan Otoritas Sertifikasi dalam pengaturan mengenai Tanda Tangan Digital.

b. Kegunaan Penelitian

1. Diharapkan dapat memberikan pengetahuan mengenai pengaturan mengenai Perdagangan Secara Elektronik *(E-Commerce)* dan Tanda Tangan Digital di Indonesia.

2. Diharapkan dapat memberikan pemahaman tentang pembuktian Tanda Tangan Digital dalam hukum di Indonesia.
3. Merupakan sumbangan pemikiran bagi perkembangan peraturan-peraturan di bidang Hukum dan Teknologi Informasi khususnya dalam hal pembuktian.

BAB II

TINJAUAN PUSTAKA

A. Sejarah Internet

a. Internet dan Perkembangannya

Kemajuan teknologi informasi telah mengubah pandangan manusia tentang berbagai kegiatan yang selama ini hanya dimonopoli oleh aktifitas fisik semata. Lahirnya internet mengubah paradigma komunikasi manusia dalam kehidupan sehari-hari, baik dalam hal bergaul, berbisnis, dan bahkan berasmara. Internet mengubah konsep jarak dan waktu secara drastis sehingga seolah-olah dunia menjadi kecil dan tidak terbatas. Setiap orang dapat berhubungan, berbicara dan berbisnis dengan orang lain yang berada ribuan kilo-meter dari tempat di mana ia berada hanya dengan menekan tuts-tuts *keyboard* dan *mouse* komputer yang ada di hadapannya.

Pada awalnya, internet lahir dari ARPANET, yang merupakan jaringan komputer milik Departemen Pertahanan Amerika yang bertujuan untuk mempermudah pertukaran informasi diantara pengkaji pertahanan *(defence researcher)*. Namun, tidak ada yang pernah menyangka bahwa perkembangan internet sedemikian pesatnya sehingga digunakan di seluruh dunia.

b. Pengertian Internet

Dalam *Oxford Dictionary*, pengertian internet adalah *international computer network connecting other networks and computers from companies, university, etc.* Internet merupakan jaringan komputer

internasional yang berhubungan dengan jaringan komputer lain, baik digunakan oleh perusahaan, universitas, dan lain sebagainya.

Pada intinya, internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik, satelit, maupun gelombang frekuensi.[4]

Dari segi penulisannya, internet memiliki 2 (dua) arti, yaitu:[5]

1. internet
   Jaringan internet (huruf "i" kecil sebagai huruf awal) adalah suatu jaringan komputer yang mana komputer-komputer terhubung dapat berkomunikasi walaupun perangkat keras dan lunaknya berlainan (sering kali disebut juga *internet-working*)
2. Internet
   Jaringan Internet (huruf "I" besar sebagai huruf awal adalah jaringan dari sekumpulan jaringan *(network of networks)* yang terdiri dari jutaan komputer yang dapat berkomunikasi satu sama lain dengan menggunakan suatu aturan komunikasi jaringan komputer (protokol) yang sama. Protokol yang digunakan tersebut adalah *Transmission Control Protocol/Internet Protocol (TCP/IP)*

The Federal Networking Council (FNC) memberikan definisi mengenai internet dalam resolusinya tanggal 24 Oktober 1995. Definisi yang diberikan adalah sebagai berikut:[6]

> *Internet refers to the global information system that –*
> *(i) is logically linked together by a globally unique address space based in the internet Protocol (IP) or its subsequent extensions/follows-on;*
> *(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its sub-sequent extension/follows-on, and/or other Internet Protocol (IP)-compatible protocols; and*

---

[4] Agus Raharjo, *Cyber Crime:* Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi (Bandung: PT. Citra Aditya Bakti, 2002), hal. 59

[5] (Fransisca Haryati Chandra, "Internet: *Information Superhighway*" 1995:1-2, sebagaimana dikutip oleh Agus Raharjo, *Cyber Crime:* Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi (Bandung: PT. Citra Aditya Bakti, 2002), hal. 60

[6] Raharjo, *op.cit.*, hal. 60

(iii) Providers, uses or makes accessible, either publicly or privately, high level services layered on the communication and related infrastructure describe herein.

Pada tahun 2003, Internet telah menghubungkan jaringan komputer lebih dari tiga ratusan ribu jumlahnya (*network of networks*), yang menjangkau sekitar seratus negara di dunia ini. Dalam setiap tiga puluh menit (waktu rata-rata) muncul satu jaringan tambahan lagi. Ratusan halaman informasi *(web pages)* yang baru tersajikan setiap menitnya sehingga memperkaya khazanah yang telah ada, sejumlah lebih dari 50-an juta halaman.[7]

Di Indonesia, internet diperkenalkan pada tahun 1994. Hingga dewasa ini internet di Indonesia telah mengalami pertumbuhan dan perkembangan yang sangat pesat. Dari sekitar 240 juta penduduk Indonesia pada saat ini, 16 juta diantaranya adalah pengguna internet.[8] Jumlah pengguna internet ini bisa jauh lebih banyak jika dibandingkan dengan jumlah pelanggan internet, karena seringkali terjadi bahwa satu *personal computer* (PC) digunakan 3-5 orang, seperti yang terjadi pada warung-warung internet yang semakin menjamur di Indonesia.

---

[7] Budi Agus Riswandi, Hukum dan Internet di Indonesia (Yogyakarta: UII Press, 2003), hal. 14

[8] Berdasarkan data yang diperoleh dari Asosiasi Penyelenggara Internet Indonesia (APJII), tanggal 5 Agustus 2006

Perkembangan Jumlah Pelanggan & Pemakai Internet (kumalatif)

Tahun	Pelanggan	Pemakai
1998	134.000	512.000
1999	256.000	1.000.000
2000	400.000	1.900.000
2001	581.000	4.200.000
2002	667.002	4.500.000
2003	865.706	8.080.534
2004	1.087.428	11.226.143
2005*	1.500.000	16.000.000

*** perkiraan s/d akhir 2005**

Sumber: APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), http://www.apjii.or.id/dokumentasi/statistik.php

Dari tabel di atas, dapat kita lihat bahwa internet di Indonesia mengalami perkembangan yang sangat signifikan walaupun internet masih relatif baru dikenal dan frekuensi pemakaiannya pun belum terlalu banyak.

Internet lebih digemari dari media-media telekomunikasi lainnya disebabkan oleh beberapa faktor berikut ini:[9]

1. *Efficiency* (Efisiensi)
2. *Without Boundary* (Tanpa Batas)
3. *24-Hours online* (terbuka 24 jam)
4. *Interactive*
5. *Hyperlink*
6. *No License Required* (Tidak Perlu Izin)
7. *No Censorship* (Tanpa Sensor)

c. Permasalahan Hukum di Internet

Walaupun terdapat banyak kelebihan dan keunggulan internet dibandingkan dengan media lainnya, internet juga memiliki beragam masalah

[9] *Ibid*, hal. 15

dan kekurangan. Persoalan hukum yang timbul berkaitan dengan mekanisme pembayaran dalam transaksi secara elektronik *(E-Commerce)*, kontrak, perlindungan terhadap data-data individual konsumen, *Digital Signature*, penyelesaian sengketa, dan lain sebagainya.

Inilah kiranya persoalan-persoalan hukum yang muncul ke permukaan ketika internet mulai menjadi *trend* dalam kehidupan individu maupun masyarakat. Belum adanya regulasi nasional yang mengatur mengenai penggunaan internet di Indonesia merupakan masalah krusial yang membutuhkan perhatian pemerintah secepatnya.

B. Perdagangan Secara Elektronik (*E-Commerce)*

Salah satu bukti dari kemajuan teknologi internet yang sangat dirasakan manfaatnya oleh konsumen dalam bidang bisnis/perdagangan adalah *Electronic Commerce* atau yang sering disebut dengan *E-Commerce*. Melalui *E-Commerce*, konsumen memiliki ruang gerak yang semakin luas dalam bertransaksi, sehingga konsumen memiliki kemampuan untuk mengumpulkan serta membandingkan produk barang dan atau jasa yang diinginkannya dan konsumen pun menjadi lebih aktif berperan serta dalam pasar dunia.

Sebelum melangkah lebih jauh lagi, terlebih dahulu harus diketahui mengenai apa dan bagaimana *Electronic Commerce* itu sendiri. Istilah *E-Commerce* didefinisikan sebagai berikut:[10]

---

[10] Julian Ding, *E-Commerce: Law and Office,(*Malaysia: Sweet and Maxwell Asia, 1999), hal. 25, sebagaimana dikutip oleh Abdul Halim Barakatullah, Bisnis *E-Commerce*: Studi Sistem Keamanan dan Hukum di Indonesia (Yogyakarta: Pustaka Pelajar, 2005), hal.11

"Electronic Commerce or E-Commerce as it also known, is a commercial transaction between avendor and purchaser or parties in similar contractual relationship for the supply of goods, services or acquisition of "rights". This commercial transaction is executed or entered into electronic medium (or digital medium) where the physical presence of parties is not required, and medium exist in a public network or system as opposed to private network (closed system). The public network system must considered on open system (e.g the internet or world wide web). The transaction concluded regardless of national boundaries or local requirement".

Dalam pengertian ini, yang dimaksud *E-Commerce* merupakan suatu transaksi komersial yang dilakukan antara penjual dan pembeli atau dengan pihak lain dalam hubungan perjanjian yang sama untuk mengirimkan sejumlah barang, pelayanan, atau peralihan hak. Transaksi komersial ini terdapat di dalam media elektronik (media digital) yang secara fisik tidak memerlukan pertemuan para pihak dan keberadaan media ini dalam *public network* atas sistem yang berlawanan dengan *private network* (sistem tertutup), dan sistem *public network* ini harus mempertimbangkan sistem terbuka.

Dalam kamus *Black's Law Dictionary Seventh Edition*, *E-Commerce* didefinisikan:

"E-Commerce; The practice of buying and selling goods and services through online consumer services on the internet: The e, a shortened of electronic, has become a popular prefix for other terms associated with electronic transaction".

Electronic Commerce atau disingkat dengan *E-Commerce* adalah kegiatan-kegiatan bisnis yang menyangkut konsumen (*consumers*), manufaktur (*manufactures*), *service providers* dan pedagang perantara *(intermediateries)* dengan menggunakan jaringan-jaringan komputer

(computer network) yaitu internet. Penggunaan sarana internet merupakan suatu kemajuan teknologi yang dapat dikatakan menunjang secara keseluruhan spektrum kegiatan komersial.[11]

Definisi yang paling lengkap adalah definisi yang dikemukakan oleh ECEG *(Electronic Commerce Expert Group)* yang mendefinisikan *E-Commerce* sebagai:

> *"a broad concept that covers any commercial transaction that is effected via electronic means and would include such means as facsimile, telex, EDI, internet and the telephone. For the purpose of this report the term is limited to those trade and commercial transaction involving computer to computer communicatons whether utilising an open or closed network".*[12]

E-Commerce adalah sebuah konsep yang luas yang meliputi setiap transaksi dagang yang dilakukan via alat-alat elektronik dan meliputi alat-alat seperti faksimili, teleks, EDI, internet dan telepon. Untuk tujuan laporan ini, istilah *e-commerce* dibatasi pada setiap transaksi perdagangan dan niaga yang menggunakan komunikasi komputer ke komputer baik menggunakan jaringan terbuka atau tertutup.

Berdasarkan pengertian-pengertian mengenai *Electronic Commerce* di atas, maka dapat disimpulkan bahwa *E-Commerce* adalah segala bentuk transaksi perdagangan/perniagaan barang atau jasa *(trade of goods and services)* yang dilakukan melalui perantara media elektronik.

Media elektronik yang dibicarakan dalam tulisan ini adalah media internet, mengingat penggunaan media jaringan internet yang saat ini paling

---

[11] *Ibid.*

[12] Melissa De Zwart, *"Electronic Commerce: Promises, Potential and Proposal"* dalam UNSW *Law Journal*, sebagaimana dikutip oleh M. Aryad Sanusi, *E-Commerce:* Hukum dan Solusinya (Bandung: PT. Mizan Grafika Sarana, 2001), hal. 16

populer digunakan oleh banyak orang. Dengan melakukan perdagangan melalui internet, tentu saja membuat transaksi perdagangan antara konsumen dan produsen atau penyedia jasa menjadi lebih mudah, efisien, dan murah karena para pihak tidak harus bertemu. Keuntungan lainnya adalah untuk perluasan pangsa pasar ke seluruh dunia tanpa harus pergi atau mengirim utusan ke tujuan pemasaran.

Walaupun internet dan *E-Commerce* merupakan hal yang baru, namun berdasarkan data yang diperoleh, pengguna *E-Commerce* di Indonesia pada tahun 2003 mencapai 600.000 pengguna, dengan total dana US$ 1,2 miliar.[13]

Di dalam *E-Commerce*, para pihak yang melakukan kegiatan perdagangan/perniagaan hanya berhubungan melalui suatu jaringan publik *(public network)* yang dalam perkembangan terakhir menggunakan media internet.

Namun, walaupun terdapat banyak kemudahan yang ditawarkan oleh penggunaan *E-Commerce*, koneksi yang dilakukan ke dalam jaringan internet sebagai jaringan pubik merupakan koneksi yang tidak aman. Hal ini menimbulkan konsekuensi bahwa *E-Commerce* yang dilakukan dengan koneksi ke internet merupakan bentuk transaksi berisiko tinggi yang dilakukan di media yang tidak aman.

---

[13] Hasil survei *International Data Corporation* (IDC), disadur dari situs *Global Technology*, http://www.globaltechnology.co.id/seminar/e_commerce/seri001.htm, tanggal 5 Agustus 2006

Kelemahan yang dimiliki oleh internet sebagai jaringan publik yang tidak aman ini dapat diminimalisasi dengan adanya penerapan teknologi penyandian informasi *(crypthography)*. *Electronic Data Transmission* dalam *E-Commerce* disekuritisasi dengan melakukan proses enkripsi sehingga menjadi *chiper/locked data* yang hanya bisa dibaca dan dibuka dengan melakukan proses deskripsi sebelumnya. Hasil dari proses inilah yang dinamakan dengan *Digital Signature.*[14]

C. Aspek Hukum Pembuktian Dalam Transaksi *E-Commerce*

Legalitas dari suatu kontrak atau perjanjian pada *Electronic Commerce* menjadi sebuah fenomena yuridis yang relatif baru bagi hukum Indonesia (hukum positif) pada umumnya, yang perlu dikaji lebih lanjut terhadap aspek hukum pembuktian pada khususnya.[15]

Alat-alat bukti yang diakui dalam peradilan perdata Indonesia diatur dalam HIR *(Herzien Indonesisch Reglement)* Pasal 164 dan Kitab Undang-undang Hukum Perdata (KUH Perdata) Pasal 1866 BW ialah:

1. bukti tulisan;
2. bukti dengan saksi-saksi;
3. persangkaan-persangkaan;
4. pengakuan; dan
5. sumpah

---

[14] Arrianto Mukti Wibowo, Kerangka Hukum *Digital Signature* (http:/www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html), tanggal 14 Maret 2006

[15] Mukti Fajar ND, Aspek Hukum Pembuktian *Digital Evidence* Dalam *Electronic Commerce* (http://www.umy.ac.id/hukum/download/fajar.htm), disadur tanggal 14 Maret 2006

Sedangkan alat bukti yang sah untuk diajukan di depan persidangan, seperti yang diatur Pasal 184 Kitab Undang-Undang Hukum Pidana adalah :

1. Keterangan saksi;
2. Keterangan ahli;
3. Surat;
4. Petunjuk;
5. Keterangan terdakwa.

Berkaitan dengan permasalahan penulisan ini yaitu tentang alat bukti dalam *Electronic Commerce* maka alat-alat bukti yang ada dibatasi pada alat bukti tertulis saja. Hal ini sesuai dengan kenyataan bahwa jenis surat atau akta dalam perkara perdata, memegang peran yang amat penting. Semua kegiatan yang menyangkut bidang perdata, sengaja dicatat atau dituliskan dalam surat atau akta. Setiap perjanjian jual-beli, sewa-menyewa, penghibaan, pengangkutan, asuransi, perkawinan, kelahiran dan kematian, sengaja dibuat dalam bentuk tertulis dengan maksud sebagai alat bukti atas transaksi atau peristiwa hubungan hukum yang terjadi. Atas kenyataan tersebut, dalam perkara perdata, alat bukti yang dianggap paling dominan adalah alat bukti surat (tulisan).[16]

Alat bukti tertulis diatur dalam Pasal 1867-1894 BW. Alat bukti tertulis atau surat ialah segala sesuatu yang memuat tanda-tanda bacaan yang dimaksudkan untuk mencurahkan isi hati atau menyampaikan buah pikiran

---

[16] M. Yahya Harahap, Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian, dan Putusan Pengadilan (Jakarta: Sinar Grafika, 2005), hal. 557

seseorang dan dipergunakan sebagai pembuktian. Dengan demikian maka segala sesuatu yang tidak memuat tanda-tanda bacaan, atau meskipun memuat tanda bacaan, akan tetapi tidak mengandung buah pikiran, tidaklah termasuk dalam pengertian alat bukti tertulis atau surat.[17]

Namun, seiring dengan perkembangan jaman, kebenaran tidak hanya diperoleh dari alat bukti tertentu, tetapi dari alat bukti mana saja pun harus diterima kebenaran sepanjang hal itu tidak bertentangan dengan ketertiban umum. Oleh sebab itu perlunya diberlakukan perkembangan ke arah alat bukti terbuka, yang memungkinkan hakim bebas dan leluasa menerima alat bukti yang diajukan oleh para pihak.

Ditanggalkannya sistem yang menyebut satu per satu alat bukti berdasar alasan, alat bukti yang lama dianggap tidak komplit, karena sistem itu tidak menyebut dan memasukkan alat bukti modern yang dihasilkan perkembangan ilmu pengetahuan dan teknologi. Misalnya, alat bukti elektronik *(electronic evidence)*, meliputi data elektronik *(electronic data)*, berkas elektronik *(electronic file)*, maupun segala bentuk sistem komputer yang dapat dibaca *(system computer readable form)*.[18]

Untuk lebih mengenal aspek hukum pembuktian dalam *Electronic Commerce* maka akan lebih jelasnya jika diuraikan tentang beberapa hal yang terkait dengan aspek hukum pembuktian tersebut, yaitu tentang kontrak tertulis, legalitas tanda tangan dan bentuk tulisan serta selanjutnya

---

[17] Mukti Fajar, *op.cit.*,

[18] Alan M. Gathan, Electronic Evidence, (Toronto: Carswell, 1999), hal. 1, sebagaimana dikutip oleh Yahya Harahap, *op. cit.*,

baru akan dibahas perihal keabsahan sebagai alat bukti dalam *electronic commerce*.

1. Kontrak Tertulis

Hukum negara tentang perdagangan secara umum mengenal secara luas transaksi komersial sebagai sesuatu yang valid, berkekuatan penuh dan tanpa syarat yang spesifik untuk mereduksinya ke dalam bentuk tertulis. Kontrak tertulis merupakan kontrak yang dibuat oleh para pihak dalam bentuk tulisan.[19]

Ada tiga bentuk perjanjian tertulis, yaitu:[20]

1. perjanjian di bawah tangan yang ditandatangani oleh para pihak yang bersangkutan saja (Pasal 1867 KUHPerdata);
2. perjanjian dengan saksi notaris untuk melegalisasi tanda tangan para pihak (Pasal 1868 KUHPerdata);
3. perjanjian yang dibuat di hadapan dan oleh notaris dalam bentuk akta notariel(Pasala 1868 KUHPerdata).

Pada umumnya, *invoice* (faktur), surat pengantar, dan dokumen komersial lainnya pada dasarnya tidak perlu dalam bentuk tertulis jika terjadi dalam transaksi antara pihak-pihak swasta. Walaupun demikian, di banyak negara Eropa otoritas pajak memerlukan *invoice* dan dokumen akuntansi lainnya dalam bentuk tertulis. Rekaman akuntansi yang dikomputerisasi diterima oleh otoritas pajak di negara-negara tertentu, terutama di negara-negara yang sistem komputernya mampu menangani keperluan formal tertentu yang ditetapkan oleh administrasi pajak. Singkatnya, ada

[19] Salim HS, Hukum Kontrak: Teori dan Teknik Penyusunan Kontrak (Jakarta: Sinar Grafika, 2005), hal. 29.
[20] Syahmin AK, Hukum Kontrak Internasional (Jakarta: PT RajaGrafindo Persada. 2005), hal. 43

ketidakseragaman yang cukup parah, baik yang bersifat domestik maupun internasional mengenai pertanyaan apakah transmisi elektronik (walaupun dalam bentuk yang sudah terkenal seperti halnya fax) akan diterima sebagai tulisan.[21]

2. Legalitas Tanda Tangan

Tanda tangan mungkin dalam bentuk tulisan tangan, tercetak pada kertas fax, bentuk-bentuk cetakan, tanda dalam bentuk simbol, atau bentuk lain yang dibuat secara mekanis maupun elektronis, jika konsisten dengan hukum suatu negara dimana dokumen tersebut dikeluarkan.

Sifat yang diinginkan dari legalitas tanda tangan di antaranya adalah:[22]

a. Tanda tangan itu asli (otentik), tidak mudah ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatangan tak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya.
b. Tanda tangan itu hanya sah untuk dokumen (pesan) itu saja. Tanda tangan itu tidak bisa dipindahkan dari suatu dokumen ke dokumen lainnya. Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
c. Tanda tangan itu dapat diperiksa dengan mudah. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu dengan penandatangan.
d. Tanda tangan itu juga sah untuk salinan dari dokumen yang sama persis. Meskipun ada banyak skenario, ada baiknya kita perhatikan salah satu skenario yang cukup umum dalam penggunaan tanda tangan digital. Tanda tangan digital memanfaatkan fungsi *hash* satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Bukan dokumen tersebut secara keseluruhan

---

[21] Richard Hill and Ian Walden, sebagaimana dikutip oleh Mukti Fajar ND, Aspek Hukum *Digital Evidence* Dalam *Elektronic Commerce*, (http://www.umy.ac.id/hukum/download /fajar.htm), disadur tanggal tanggal 14 Maret 2006.

[22] Arrianto Mukti Wibowo (1998:2), sebagaimana dikutip oleh Mukti Fajar ND, Aspek Hukum *Digital Evidence* Dalam *Elektronic Commerce*, (http://www.umy.ac.id/hukum/download /fajar.htm), disadur tanggal tanggal 14 Maret 2006.

yang ditandatangani, namun biasanya yang ditandatangani adalah sidik jari dari dokumen itu beserta *time stamp*-nya dengan menggunakan kunci privat. *Time stamp* berguna untuk menentukan waktu pengesahan dokumen.

Penandatanganan suatu dokumen secara umum mempunyai tujuan sebagai berikut:[23]

1. Bukti *(evidence)*: Suatu tanda tangan akan mengotentifikasikan penandatangan dengan dokumen yang ditandatanganinya. Pada saat penandatanganan membubuhkan tanda tangan dalam suatu bentuk yang khusus, tulisan tersebut akan mempunyai hubungan *(attribute)* dengan penandatangan.
2. *Ceremony*: Penandatanganan suatu dokumen akan berakibat penandatangan tahu bahwa ia telah melakukan suatu perbuatan hukum, sehingga akan mengeliminasi adanya *inconsiderate engagement*.
3. Persetujuan *(approval)*: Dalam penggunaannya dalam berbagai konteks baik oleh hukum atau oleh kebiasaan, tanda tangan melambangkan adanya persetujuan atau otorisasi terhadap suatu tulisan, atau penandatangan telah secara sadar mengetahui bahwa tanda tangan tersebut mempunyai konsekuensi hukum.
4. *Efficiency and logistics*: tanda tangan dalam suatu dokumen tertulis seringkali menimbulkan kejelasan dan keabsahan dari suatu transaksi dan juga akan mengurangi kebutuhan untuk mengecek keabsahan suatu dokumen kepada orang yang bersangkutan.

Uncitral Model Law 1996 secara eksplisit memberikan solusi teknis yang pas dan sama nilai legalnya dengan tanda tangan tradisional, yang dalam maksud-maksud tertentu para pihak bisa menyetujuinya jika mereka mau. Teknologi tanda tangan elektronik masa depan ini dapat diperkenalkan sebagai teknologi yang cocok, tanpa harus mengubah undang-undang.

---

[23] Abdul Halim Barakatullah, Bisnis *E-Commerce*: Studi Sistem Keamanan dan Hukum di Indonesia (Yogyakarta: Pustaka Pelajar, 2005), hal.117-118

Ketentuan-ketentuan Pasal 7 dalam *Model Law* berhubungan erat dengan praktik yang sedang berlangsung.[24]

Article 7.

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

Ketika ada aturan hukum mensyaratkan tanda tangan, atau memberi konsekuensi tertentu jika tanpa tanda tangan, maka dalam hubungannya dengan pesan data, aturan itu akan terpenuhi jika :

a. Ada metode yang digunakan untuk mengidentifikasi si pembuat asli dari pesan data dan mengindikasi persetujuan si pembuat asli terhadap kandungan informasi yang ada pada pesan data tersebut; dan

b. Metode tersebut bisa diandalkan sebagai metode yang cocok untuk kebutuhan dimana pesan data tersebut dihasilkan dan dikomunikasikan, dalam segala kondisi yang ada, termasuk semua persetujuan antara si pembuat asli dengan yang si penerima pesan data.

[24] Richard Hill and Ian Walden, sebagaimana dikutip oleh Mukti Fajar ND, Aspek Hukum *Digital Evidence* Dalam *Elektronic Commerce*, (http://www.umy.ac.id/hukum/download/fajar.htm), disadur tanggal tanggal 4 Maret 2006.

Walaupun demikian, interpretasi ini belum diadopsi oleh konvensi-konvensi internasional yang lain, yang membatasi karakteristik arti tanda tangan pada dokumen khusus. Kenyataannya, hukum di negara-negara tertentu tidak memperbolehkan bentuk-bentuk lain tanda tangan, selain dari bentuk tradisional tanda tangan "tinta di atas kertas". Walaupun, ketika hukum sebuah negara tidak melarang tanda tangan elektronis, hukum tidak akan berkembang dengan baik, dan para pelaku bisnis akan memberi perhatian penuh sampai pengadilan mengakui tanda tangan elektronis.[25]

3. Bentuk Tulisan

Dalam Pasal 6 dalam *Model Law*, secara tegas memberikan nilai legal yang sama kepada transmisi elektronik seperti halnya bentuk tertulis.

Article 6.

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained there in is accessible so as to be usable for subsequent reference.

Penyamaan nilai legal antara transmisi elektronik dengan bentuk tertulis dimaksudkan untuk mempermudah posisi transmisi ini sehingga dapat digunakan sebagai bukti nyata dalam pembuktian dan sebagai salah satu pendekatan yang relatif paling mudah sebagai solusi yang ditawarkan.[26]

4. Keabsahan Sebagai Alat Bukti

---

[25] *Ibid.*
[26] *Ibid.*

Solusi yang ditawarkan oleh *Uncitral Model Law 1996* dengan pendekatan yang diadopsi oleh *Model Law* ini tidak secara menyeluruh menyatakan bahwa transmisi elektronik adalah sebuah bentuk tulisan, atau tidak juga mensyaratkan teknik spesifik untuk tanda tangan. Secara bijak, *Model Law* memulainya dengan membatasi ruang lingkup aplikasi *E-Commerce*: "Hukum ini beraplikasi terhadap segala macam informasi dalam bentuk pesan data yang digunakan dalam konteks aktifitas komersial".[27]

Apabila terdapat perkara, khususnya perkara perdata, maka untuk mengambil dan melegalisasi dokumen yang akan dijadikan sebagai barang bukti yang berada di negara lain, dapat digunakan *Convention on the Taking Evidence Abroad in Civil Commercial Matters (1968).* Di dalam konvensi ini juga diatur cara mengenai kesaksian apabila saksi berada di negara yang berlainan. Konvensi ini diselenggarakan di Den Haag (The Hague) 26 Oktober 1968. *Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (1965) mengatur mengenai cara melakukan panggilan-panggilan dalam perkara perdata apabila ada pihak yang berada di luar negeri atau melakukan pemberitahuan bagi para pihak jika mereka di luar negeri. [28]

Dalam pembahasan mengenai keabsahan alat bukti dengan *digital evidance* dalam *Electronic Commerce,* keaslian dari alat bukti dan penerimaannya secara hukum merupakan hal yang harus diperhatikan yang baik secara yuridis maupun teknis dapat menjaga validitas suatu alat bukti.

---

[27] *Ibid.*
[28] *Ibid.*

Pasal 8 dalam *Uncitral Model Law on Electronic Commerce 1996* mempersoalkan tentang keaslian dan penerimaan secara hukum, menyebutkan bahwa :

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented

Dalam setiap proses legal, tidak ada satu pun aplikasi aturan tentang bukti yang diterapkan untuk menolak pesan data sebagai barang bukti. Informasi dalam bentuk pesan data seharusnya diberi hak bobot *evidential.* Dalam menilai bobot *evidential* pesan data, perhatian seharusnya diarahkan pada kehandalan cara kerjanya yang berhubungan dengan bagaimana pesan data itu dihasilkan, disediakan, atau dikomunikasikan; kehandalan cara kerjanya yang berhubungan dengan bagaimana integritas informasi dipertahankan; kehandalan cara kerjanya yang berhubungan dengan bagaimana si pembuat asli data diidentifikasi, dan faktor-faktor lain yang relevan.[29]

Di Indonesia hingga saat ini belum ada suatu aturan mengenai *Electronic Commerce* khususnya mengenai *Digital Signature*. Sampai saat ini, hukum pembuktiannya masih menggunakan ketentuan hukum yang lama (BW, HIR, dan RBg). Namun demikian, keberadaan UU No. 8 Tahun 1997

---

[29] *Ibid.*

tentang Dokumen Perusahaan telah mulai menjangkau ke arah pembuktian data elektronik.[30]

Dalam UU Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan disebutkan pada Pasal 12 ayat 4 bahwa:

"Dalam hal dokumen yang dialihkan ke dalam microfilm atau media lainnya adalah naskah asli yang mempunyai kekuatan pembuktian otentik dan masih mengandung kepentingan hukum tertentu, pimpinan perusahaan wajib tetap menyimpan naskah asli tersebut."

Penerimaan ini diperkuat dengan definisi dari telekomunikasi yang mempunyai hubungan secara ekplisit dengan hal ini, dalam Ketentuan Umum vide 1 Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi dinyatakan bahwa:

"Telekomunikasi adalah setiap pemancaran, pengiriman dan atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik."

Kriteria untuk menilai integritas sebuah informasi, yaitu apakah informasi harus tetap lengkap dan tidak dapat diubah, termasuk penambahan semua pengesahan dan semua perubahan yang muncul dalam rangkaian komunikasi, penyimpanan, pertunjukan; dan standar kehandalan perlu untuk diuji dalam setiap kegunaannya dimana informasi dihasilkan dan dalam setiap kondisi yang relevan.[31]

Dalam konsideran UU RI Nomor 8 Tahun 1997 tentang Dokumen Perusahaan vide f disebutkan bahwa: "Kemajuan teknologi memungkinkan

---

[30] Isis Ikhwansyah, "Prinsip-prinsip Universal Bagi Kontrak Melalui *E-Commerce* dan Sistem Hukum Pembuktian Perdata Dalam Teknologi Informasi" dalam Cyber Law: Suatu Pengantar (Bandung: ELIPS II, 2001), hal. 31

[31] Mukti Fajar ND, Aspek Hukum Pembuktian *Digital Evidence* Dalam *Elektronic Commerce*, (http://www.umy.ac.id/hukum/download/fajar.htm), disadur tanggal tanggal 14 Maret 2006.

catatan dan dokumen yang dibuat di atas kertas dialihkan ke dalam media elektronik atau dibuat secara langsung dalam media elektronik".

Selanjutnya Pasal 15 dalam UU Nomor 8 Tahun 1997 masalah ini lebih diperjelas dengan menyebutkan :

(1) Dokumen perusahaan yang dimuat dalam *microfilm* atau media lainnya sebagaimana dimaksud dalam pasal 12 (1) dan atau hasil cetaknya merupakan alat bukti yang sah.
(2) Apabila dianggap perlu dalam hal tertentu dan untuk keperluan tetentu dapat dilakukan legalisasi terhadap hasil cetak dokumen perusahaan yang telah dimuat dalam microfilm atau media lainya.

D. Tanda Tangan Digital (*Digital Signature*)

Digital Signature adalah suatu sistem pengamanan yang menggunakan *public key cryptoghraphy system*, atau secara umum pengertiannya adalah: "*A data value generated by public key algorithm based on the contents of a lock data and private key, yielding so individualized crypto checksum*".[32]

Dari perspektif hukum, *digital signature* adalah sebuah pengaman pada data digital yang dibuat dengan kunci tanda tangan pribadi *(private signature key)*, yang kebolehan penggunaannya tergantung pada kunci publik *(public key)* yang menjadi pasangannya.[33]

Dari perspektif teknis, *digital signature* adalah sebuah nilai numerik yang dipadankan dengan sebuah data, dengan menggunakan sebuah prosedur matematika yang diketahui oleh pemilik kunci kriptografi. Dari perspektif ini, *digital signature* menjadikan suatu nilai numerik bersifat unik

---

[32] Arrianto Mukti Wibowo, Kerangka Hukum *Digital Signature* (http:/www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html), disadur tanggal 14 Maret 2006

[33] Danrivanto Budhijanto, "Aspek Hukum *Digital Signature* dan *Certification Authorities* Dalam Transaksi *E-Commerce*" dalam *Cyber Law*: Suatu Pengantar, (Bandung: ELIPS II, 2002), hal. 67

karena nilai numerik itu sudah sepadan dengan kunci kriptografi yang dikuasai oleh pemilik aslinya.[34]

Digital Signature dapat pula dinyatakan sebagai berikut:

> *"A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged".*[35]

Tujuan dari suatu tanda tangan dalam suatu dokumen adalah untuk memastikan otentisitas dari dokumen tersebut. Suatu *Digital Signature* sebenarnya adalah bukan suatu tanda tangan seperti yang dikenal selama ini. *Digital Signature* menggunakan cara yang berbeda untuk menandai suatu dokumen sehingga dokumen atau data yang dimaksud tidak hanya dapat diidentifikasi pengirimnya namun juga dapat dipastikan keutuhan dokumen tersebut selama proses transmisi.[36]

a. Teknik Kriptografi

Kriptografi adalah bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun deskripsi data. Teknik ini digunakan untuk mengkonversi atau mengubah data ke dalam bentuk kode-kode tertentu, dengan tujuan informasi yang disimpan maupun ditransmisikan melalui jaringan yang tidak aman, tidak dapat dibaca oleh siapa pun kecuali oleh orang-orang yang berhak.[37]

---

[34] *Ibid.*
[35] Budi Agus Riswandi, Hukum *Cyberspace* (Yogyakarta: Gita Nagari, 2006), hal. 27
[36] Mukti Fajar ND, Aspek Hukum *Digital Evidence* Dalam *Elektronic Commerce*, http://www.umy.ac.id/hukum/download/fajar.htm, disadur tanggal tanggal 14 Maret 2006.
[37] Edmon Makarim, Pengantar Hukum Telematika: Suatu Kompilasi Kajian (Jakarta: PT RajaGrafindo Perkasa, 2005), hal. 264.

Dalam suatu kriptografi, suatu pesan dienkripsi *(encrypt)* dengan menggunakan suatu kunci *(key)*. Hasil dari enkripsi ini adalah berupa *chipertext* yang kemudian akan ditransmisikan atau diserahkan kepada tujuan yang dikehendaki. Terdapat dua macam cara dalam melakukan enkripsi yaitu dengan menggunakan kriptografi simetris *(symetric crypthography/secret key crypthography)* dan kriptografi asimetris *(asymetric crypthography)* yang kemudian lebih dikenal sebagai *public key crypthography.*[38]

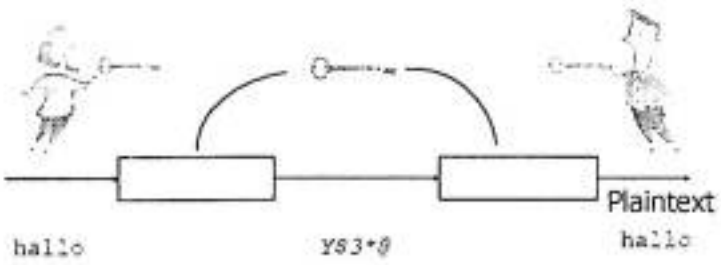
Secret key crypthografy atau yang dikenal sebagai kriptografi simetris, menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi terhadap suatu pesan (*message*), disini pengirim dan penerima menggunakan kunci yang sama sehingga mereka harus menjaga kerahasian *(secret)* terhadap kunci tersebut. Salah satu algoritma yang terkenal dalam kriptografi simetris ini adalah *Data Encryption standard (DES).*[39]

---

[38] *Ibid*

[39] *Data Encryption Standard* (DES) adalah merupakan suatu algoritma blok yang telah disetujui dan diakui oleh U.S. *National Institute for Standards and Technology* (NIST) dan *American National Standard Institute* (ANSI) sebagai sebuah standard yang dapat memberikan tingkat keamanan yang memadai untuk informasi-informasi yang tidak diklasifikasikan sebagai informasi yang sensitif.

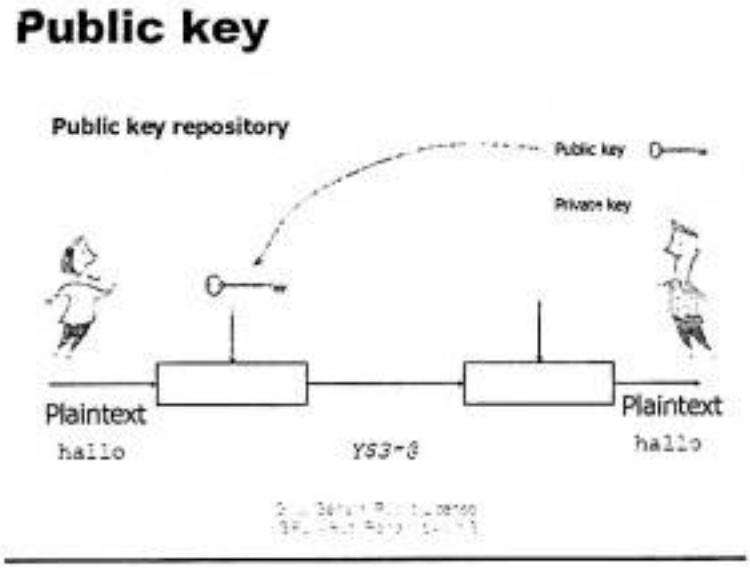
Private key



Kunci yang digunakan untuk enkripsi dan dekripsi sama!

Public key crypthography, atau dikenal juga sebagai kriptografi asimetris, menggunakan dua kunci (key): satu kunci digunakan untuk melakukan enkripsi terhadap suatu pesan (*message*) dan kunci yang lain digunakan untuk melakukan dekripsi terhadap pesan tersebut. Kedua kunci tersebut mempunyai hubungan secara matematis sehingga suatu pesan yang dienkripsi dengan suatu kunci hanya dapat didekripsi dengan kunci pasangannya. Seorang pengguna mempunyai dua buah kunci, yaitu sebuah kunci privat *(privat key)* dan juga sebuah kunci publik *(public key)*. Pengguna *(user)* tersebut kemudian mendistribusikan/menyebarluaskan kunci publik miliknya. Karena terdapat hubungan antara kedua kunci tersebut, pengguna dan seseorang yang menerima kunci publik akan merasa yakin bahwa suatu data yang diterimanya dan telah berhasil dideskripsi hanya dapat berasal dari pengguna yang mempunyai kunci privat. Kepastian/keyakinan ini hanya

ada selama kunci privat ini tidak diketahui oleh orang lain. Kedua kunci ini berasal atau diciptakan sendiri oleh penggunanya.[40]



Pada saat dua orang hendak saling berkomunikasi atau saling bertukar data/pesan secara aman, mereka kemudian saling mengirimkan salah satu kunci yang dipunyainya, yaitu kunci publiknya. Sedangkan mereka menyimpan kunci privat sebagai pasangan dari kunci publik yang didistribusikannya. Karena data/pesan ini hanya dapat dienkripsi dan dekripsi dengan menggunakan kunci pasangannya maka data ini dapat dapat ditransmisikan dengan aman melalui jaringan yang relatif tidak aman (melalui internet).

b. Jaminan Keamanan *Digital Signature*

Namun demikian, dalam hukum pembuktian baik dengan alat bukti konvensional maupun *digital evidence* harus memenuhi beberapa persyaratan, dengan digunakan teknologi *Digital Signature* maka secara

[40] Arrianto Mukti Wibowo, Kerangka Hukum *Digital Signature* (http:/www.geocities.com/arrianto/resource/hukum_ttd/hukum_ttd.html), disadur tanggal 14 Maret 2006

teknis dapat mendukung kekuatan yuridis dari *digital evidence*, hal hal yang harus dijamin keamanannya oleh sistem *Digital Signature* adalah:[41]

(a). *Authenticity* (Keaslian Pesan)

Dengan memberikan *Digital Signature* pada data elektronik yang dikirimkan maka akan dapat ditunjukkan dari mana data elektronis tersebut sesungguhnya berasal. Terjaminnya integritas pesan tersebut bisa terjadi karena keberadaan dari *Digital Certificate*. *Digital Certificate* diperoleh atas dasar aplikasi kepada *Cerfication Authority* oleh pengguna/pemohon. *Digital certificate* berisi informasi mengenai pengguna antara lain:

1. identitas
2. kewenangan
3. kedudukan hukum
4. status dari *user*

(b). *Integrity* (Keutuhan Pesan)

Integritas/*integrity* berhubungan dengan masalah keutuhan dari suatu data yang dikirimkan. Seorang penerima pesan/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.

Penggunaan *Digital Signature* yang diaplikasikan pada pesan/data elektronik yang dikirimkan dapat menjamin bahwa pesan/data elektronik

---

[41] *Ibid.*

tersebut tidak mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang. Jaminan *authenticity* ini dapat dilihat dari adanya *hash function*[42] dalam sistem *Digital Signature*, dimana penerima data (*recipient*) dapat 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.

(c). *Non-Repudiation* (Tidak dapat disangkal keberadaannya)

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.

---

[42] *Hash function* atau fungsi hash merupakan suatu fungsi matematis satu arah yang menggunakan data atau informasi yang sangat panjang sebagai *input* (kadangkala disebut dengan *pra-image*) dan kemudian mengeluarkan rangkaian data atau informasi yang tetap dengan panjang tertentu sebagai *output*nya (disebut dengan *hash, hash value, hash word* atau *message digest* –intisari pesan). Proses interaktif yang dilakukan untuk menghitung *hash* yang dihasilkan dari suatu *pra image* biasa disebut dengan istilah *hashing*. *Hashing* ini biasanya dilakukan untuk membuktikan bahwa pesan-pesan yang disampaikan dalam suatu proses perdagangan elektronik tidak mengalami modifikasi, penyalahgunaan atau perubahan.

(d). *Confidentiality* (Kerahasiaan Pesan)

Pesan dalam bentuk data elektronik yang dikirimkan tersebut bersifat rahasia *(confidential)*, sehingga tidak semua orang dapat mengetahui isi data elektronik yang telah ditandatangani dan dimasukkan dalam *digital envelope*. Keberadaan *digital envelope* 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 pada panjang kunci/*key* yang dipakai untuk melakukan enkripsi. Standar panjang kunci yang sering digunakan adalah sebesar 128 bit.

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.

(e) *Reliability* (dapat dipertanggungjawabkan)

Pesan yang disampaikan melalui media *cyber* tetap harus mampu dipertanggungjawabkan para pihak yang saling melakukan transaksi dan pihak pihak terkait lainnya. Dengan protokol kunci publik dan kunci privat

dalam proses "penandatanganan" *Digital Signature* segala transaksi dalam *Electronic Commerce* yang dilakukan di ruang maya *(cyber space)* dapat dipertanggungjawabkan baik secara teknis maupun yuridis.

E. Otoritas Sertifikasi *(Certification Authority*/CA)

Keunggulan dari *public-key cryptography* dibandingkan dengan algoritma yang lain ternyata masih menyimpan kelemahan dalam hal keamanan *(security)*. Kelemahan ini adalah kemungkinan pihak ke-3 yang tidak berhak menukar kunci publik milik seseorang dengan kunci miliknya. Juga terdapat ketidakpastian tentang identitas dari pemilik kunci publik. Kelemahan ini akan mengurangi keamanan dari sistem *public-key cryptography* karena seseorang dapat dengan mudah mengatakan bahwa suatu dokumen yang telah ditandatangani adalah tidak sah karena kuncinya telah diambil atau mengatakan bahwa kunci itu adalah bukan miliknya.

Untuk mengatasi hal ini dibutuhkan adanya pihak ke-3 yang terpercaya *(trusted third party)* yang dinamakan dengan Otoritas Sertifikasi *(Certification Authority)* yang akan menghubungkan kunci dengan pemiliknya.

Certification Authority adalah sebuah lembaga yang bertugas untuk memberikan sertifikasi jati diri pelanggan agar pelanggan itu bisa dikenali di dunia digital.[43]

a. Tugas *Certification Authority* (CA)

Secara umum tugas dari *Certification Authority* adalah sebagai berikut:[44]

---

[43] Edmon Makarim, Pengantar Hukum Telematika: Suatu Kompilasi Kajian (Jakarta: PT RajaGrafindo Persada, 2005), hal. 406

1. Membuat kunci publik/privat miliknya sendiri;
2. Melakukan verifikasi terhadap identitas seorang calon pelanggan yang hendak meminta sertifikat dari *Certification Authority* tersebut. Verifikasi ini adalah berdasarkan patokan atau standar yang sudah ditentukan sebelumnya;
3. Pelanggan kemudian menyerahkan kunci publiknya kepada *Certification Authority;*
4. *Certification Authority* kemudian mencek apakah kunci itu pasangan dari kunci privat yang dimiliki calon pelanggan tersebut;
5. Apabila semua persyaratan tersebut sudah dipenuhi maka *Certification Authority* akan menerbitkan sebuah sertifikat digital *(digital certificate)* atas nama orang tersebut. *Digital certificate* tersebut berisi kunci duplikat dari kunci publik pelanggan dan juga identitas dari pelanggan. *Certification Authority* kemudian akan menandatangani *digital certificate* tersebut dengan menggunakan kunci privat miliknya.

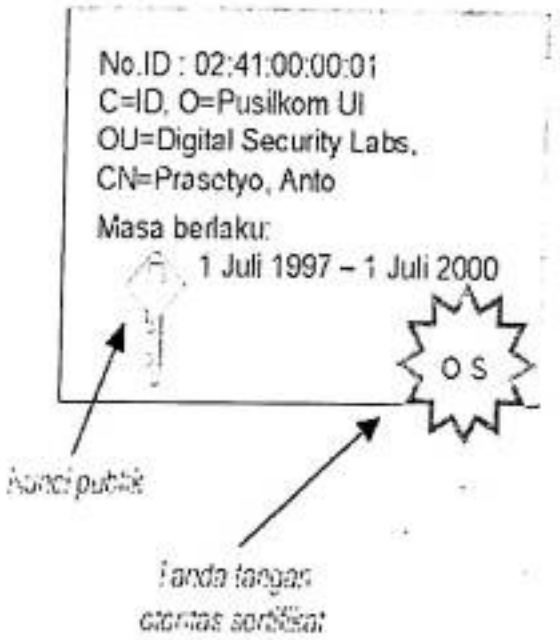
Tahapan-tahapan tersebut tidak mutlak harus seperti di atas, akan tetapi tergantung pada ketentuan-ketentuan yang telah ditetapkan oleh C.A. itu sendiri. Hal ini berkaitan dengan *level*/tingkatan dari sertifikat yang diterbitkannya dan level/tingkatan ini berkaitan juga dengan besarnya kewenangan yang diperoleh pelanggan *(subscriber)* berdasarkan sertifikat yang didapatkannya. Semakin besar kewenangannya yang diperoleh dari suatu *Digital Certificate* yang diterbitkan oleh CA 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 CA bahkan memerlukan kehadiran secara fisik pelanggan/pemohon sehingga CA dapat memperoleh kepastian pihak yang akan memperoleh sertifikat tersebut.[45]

---

[44] Abdul Halim Barakatullah, Bisnis *E-Commerce:* Studi Sistem Keamanan dan Hukum di Indonesia (Yogyakarta: Pustaka Pelajar, 2005), hal. 34

[45] Arrianto Mukti Wibowo, Kerangka Hukum *Digital Signature* (http:/www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html) disadur tanggal 14 Maret 2006

Setelah persyaratan-persyaratan tersebut diuji keabsahannya maka CA menerbitkan sertifikat pengesahan (dapat berbentuk *hard-copy* maupun *soft-copy*). Sebelum diumumkan secara luas pelanggan/pemohon 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 pelanggan/pemohon dapat mengumumkan sertifikat tersebut secara luas atau tindakan tersebut dapat diwakilkan kepada CA atau suatu badan lain yang berwenang untuk itu (suatu lembaga notariat). Selain untuk memenuhi sifat *integrity* dan *authenticity* dari sertifikat tersebut, CA akan membubuhkan *Digital Signature* miliknya pada sertifikat tersebut.



Gambar 3. Konsep sertifikat digital

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

1. Identitas C.A. yang menerbitkannya.

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

b. Fungsi *Certification Authority*

Fungsi-fungsi C.A adalah sebagai berikut:

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

BAB III

METODE PENELITIAN

A. Lokasi Penelitian

Untuk pengumpulan data dan informasi yang diperlukan dalam penyusunan skripsi ini, maka penulis memilih lokasi di Kota Makassar, yaitu Pengadilan Negeri Makassar dan Perpustakaan Pusat Universitas Hasanuddin. Alasan penulis memilih kedua lokasi tersebut adalah karena Pengadilan Negeri merupakan tempat penyelesaian perkara apabila timbul sengketa di kemudian hari, sedangkan alasan penulis melakukan penelitian di Perpustakaan Pusat Universitas Hasanuddin dengan pertimbangan bahwa koleksi literatur yang terdapat pada Perpustakaan Pusat Universitas Hasanuddin telah cukup memadai untuk dijadikan bahan acuan penyelesaian skripsi ini.

B. Jenis dan Sumber Data

a. Data primer, yaitu data yang diperoleh langsung di lokasi penelitian. Data ini bersumber dari hasil wawancara dengan salah satu hakim di Pengadilan Negeri Makassar.

b. Data sekunder, yaitu data yang diperoleh dari hasil kajian pustaka, beberapa buku, internet, makalah, perundang-undangan, serta literatur-literatur lainnya yang berkaitan dengan masalah yang dibahas dalam skripsi ini.

C. Teknik Pengumpulan Data

a. Penelitian Pustaka *(Library Research)*

Penelitian dilaksanakan dengan mengumpulkan data dan landasan teoritis dengan mempelajara buku, karya ilmiah, artikel serta sumber-sumber bacaan lainnya yang ada relevansinya dengan permasalahan yang diteliti.

b. Penelitian Lapangan *(Field Research)*

Teknik penelitian data di lapangan dalam penelitian ini dilaksanakan dengan wawancara. Teknik wawancara yang dipakai ialah wawancara berstruktur yang mengacu pada akar permasalahan.

D. Analisis Data

Analisis data dilakukan penulis dengan menggunakan metode analisis kualitatif yaitu menguraikan masalah dengan mengemukakan pendapat serta memecahkan permasalahan berdasarkan data yang ada. Dari hasil analisis ini didapat kesimpulan yang diharapkan dapat menjawab permasalahan yang dibahas dalam penulisan skripsi ini.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Pengaturan Tanda Tangan Digital Dalam Transaksi Perdagangan Secara Elektronik di Indonesia

Sebagaimana diketahui bahwa belum ada pengaturan yang secara spesifik mengatur mengenai tanda tangan digital dalam transaksi perdagangan elektronik di Indonesia.

Menurut Hakim di Pengadilan Negeri Makassar, karena tidak adanya pengaturan yang jelas mengenai Tanda Tangan Digital dan Transaksi Perdagangan Elektronik *(E-Commerce)* di Indonesia, maka kita kembali pada peraturan yang bersifat umum, yaitu hukum perdata Indonesia dengan sistem terbuka dalam hal kebebasan membuat suatu perjanjian selama tidak bertentangan dengan norma-norma kesusilaan dan ketertiban umum serta tidak bertentangan dengan hukum yang berlaku di Indonesia.[46]

Maka apabila terjadi suatu kesalahan isi dari perjanjian tersebut, maka pengenaan sanksi hukum untuk hal tersebut tergantung pada penafsiran perluasan pasal-pasal yang terdapat dalam KUH Perdata yang dapat dikenakan pada isi perjanjian.

Sehingga dapat disimpulkan bahwa perjanjian dalam bentuk apapun diperbolehkan dalam hukum perdata di Indonesia, selama tidak melanggar Undang-undang, kepentingan umum, dan kesusilaan walaupun pada

---

[46] Wawancara dengan salah satu hakim di Pengadilan Negeri Makassar, Bpk. Dewa PY Hardika, tanggal 1 Juni 2006.

hakikatnya bentuk dari perjanjian tersebut memiliki perbedaan dalam media yang digunakan, yakni dalam hal ini melalui media internet.[47]

Selanjutnya, Hakim di Makassar juga menilai bahwa apabila telah terpenuhinya syarat-syarat perjanjian, maka perjanjian tersebut mengikat para pihak.

Adapun syarat-syarat perjanjian berdasarkan ketentuan Pasal 1320 KUH Perdata, untuk sahnya suatu perjanjian diperlukan syarat-syarat sebagai berikut:

1. Sepakat mereka yang mengikatkan dirinya;
2. Kecakapan untuk membuat suatu perikatan;
3. Suatu hal tertentu;
4. Suatu sebab yang halal.

Dua syarat yang pertama, dinamakan syarat subjektif, karena kedua syarat tersebut mengenai orang-orangnya atau subjek-subjek hukum yang melakukan perjanjian. Untuk dua syarat yang terakhir dinamakan syarat-syarat objektif karena keduanya berkaitan dengan perjanjiannya itu sendiri atau objek dari perbuatan hukum yang dilakukan itu.[48]

1. Sepakat Mereka yang Mengikatkan Dirinya

Suatu kesepakatan kehendak terhadap suatu kontrak dimulai dari adanya unsur penawaran *(offer)* oleh salah satu pihak, diikuti oleh penerimaan penawaran *(acceptance)* dari pihak lainnya, sehingga

[47] Abdul Halim Barakatullah, Bisnis *E-Commerce*: Studi Sistem Keamanan Di Indonesia (Yogyakarta: Pustaka Pelajar, 2005), hal. 105
[48] *Ibid.*, hal. 86

akhirnya terjadilah suatu kesepakatan diantara kedua belah pihak tersebut.[49]

2. Kecakapan Untuk Membuat Suatu Perikatan

Menurut ketentuan Pasal 1329 KUH Perdata: "Setiap orang adalah cakap untuk membuat perikatan-perikatan, jika ia oleh undang-undang tidak dinyatakan tidak cakap. Kecakapan untuk membuat suatu perikatan, hal ini mempunyai arti bahwa orang yang membuat suatu perjanjian harus cakap menurut hukum. Pada asasnya setiap orang yang sudah dewasa dan sehat pikirannya adalah cakap menurut hukum. Namun tidak semuanya cakap untuk melakukan perbuatan hukum."

Orang-orang yang menurut undang-undang dinyatakan tidak cakap untuk melakukan perbuatan hukum menurut Pasal 1330 KUH Perdata adalah:

1. Orang-orang yang belum dewasa, yaitu anak yang belum mencapai umur 21 tahun atau belum pernah melangsungkan perkawinan;
2. Orang-orang yang ditaruh di bawah pengampuan, yaitu orang-orang dewasa tapi dalam keadaan dungu, gila, mata gelap, dan pemboros;
3. Orang-orang yang dilarang oleh undang-undang untuk melakukan perbuatan-perbuatan hukum tertentu, misalnya orang yang dinyatakan pailit.

[49] Munir Fuady, Hukum Kontrak: Dari Sudut Pandang Hukum Bisnis (Bandung: PT Citra Aditya Bakti, 2001), hal. 35

3. Suatu Hal Tertentu

Suatu hal tertentu ini mengacu pada objek yang diperjanjikan dalam perjanjian tersebut. Barang atau objek harus ditentukan jenisnya. Bahwa barang tersebut sudah ada atau sudah berada di tangan si pembeli pada waktu perjanjian dibuat, tidak diharuskan oleh undang-undang.

4. Suatu sebab yang halal

Suatu sebab yang halal, adalah isi dari perjanjian itu sendiri. Sebab tersebut merupakan sebab yang halal yang mempunyai arti bahwa isi yang menjadi perjanjian tersebut tidak menyimpang dari ketentuan-ketentuan perundang-undangan yang berlaku di samping tidak menyimpang dari norma-norma ketertiban dan kesusilaan. Sebab perjanjian adalah apa yang ingin dicapai oleh para pihak dengan dilakukannya perjanjian yaitu tujuan perjanjian, jadi causa perjanjian ditentukan oleh tujuan dari perjanjian itu.[50]

B. Keabsahan Tanda Tangan Digital Sebagai Alat Bukti

Alat-alat bukti yang diakui dalam peradilan perdata Indonesia diatur dalam HIR *(Herzien Indonesisch Reglement)* Pasal 164 dan Kitab Undang-undang Hukum Perdata (KUH Perdata) pada Pasal 1866, yang berbunyi:

Alat-alat bukti terdiri atas:

1. bukti tulisan;
2. bukti dengan saksi-saksi;
3. persangkaan-persangkaan;

[50] *Op. Cit.*, hal. 97

4. pengakuan; dan

5. sumpah

Apabila melihat pada ketentuan ini dan kemungkinan Tanda Tangan Digital digunakan sebagai alat bukti tidak dimungkinkan atau akan ditolak baik oleh hakim maupun pihak lawan. Hal ini karena pembuktian yang dihendaki berdasarkan ketentuan di atas mensyaratkan bahwa alat bukti itu berupa tulisan, sementara Tanda Tangan Digital sifatnya tanpa kertas bahkan merupakan *scripless transaction*.

Menurut Bapak Dewa PY Hardika, SH., MH, suatu Tanda Tangan Digital yang terdapat dalam perdagangan secara elektronik tidak mempunyai kekuatan pembuktian sempurna, maka tidak dapat dijadikan sebagai alat bukti tunggal. Sehingga harus didukung dengan alat-alat bukti lainnya, seperti bukti-bukti tulisan lainnya, keterangan saksi atau kesaksian, persangkaan-persangkaan, pengakuan dan sumpah.

Ditambahkan lagi, apabila terjadi suatu perkara di kemudian hari yang mempermasalahkan mengenai keabsahan suatu Tanda Tangan Digital, hendaknya dihadirkan saksi ahli yang mengetahui persis mengenai seluk-beluk Tanda Tangan Digital dan *E-Commerce*.

Suatu tanda tangan digital yang terdapat dalam suatu perjanjian yang menggunakan media internet dapat dikategorikan sebagai perjanjian dalam

bentuk tulisan. Hal ini dapat dimasukkan sebagai tulisan biasa diperkuat terlebih dahulu oleh saksi ahli, alasannya adalah:[51]

- berbeda dengan lisan, transaksi elektronik tanpa tanda tangan digital tetap merupakan sesuatu yang bisa di-*retrieve* ulang dalam bentuk aslinya.
- Meskipun tidak menggunakan tanda tangan elektronik, bisa jadi transaksi elektronik itu menggunakan teknik kriptografi kunci simetrik. Untuk beberapa jenis aplikasi, sebenarnya pengamanan dengan kunci simetrik bisa saja mencukupi kebutuhan dan bisa jadi cukup aman. Oleh karena itu, dalam pembuktian transaksi elektronik yang diamankan dengan kunci simetrik, bisa saja menggunakan saksi ahli untuk memperkuat bukti.
- Menurut para penulis KUH Perdata, surat dapat ditulis pada media apapun. Jadi dapat diinterpretasikan bahwa termasuk media elektronik dapat dijadikan 'tempat menulis'.

Suatu Tanda Tangan Digital yang dalam hal ini berwujud dokumen, akan menjadi suatu akta apabila tulisan atau dokumen tersebut dibubuhi tanda tangan dan akan menjadi akta otentik bila dibuat di hadapan atau oleh pejabat notaris.

KUH Perdata hanya mengakui surat yang bertandatangan, karena surat dalam KUH Perdata diperlukan sebagai pembuktian di masa depan.

---

[51] Arrianto Mukti Wibowo, sebagaimana dikutip oleh Abdul Halim Barakatullah, Bisnis *E-Commerce*: Studi Sistem Keamanan Di Indonesia (Yogyakarta: Pustaka Pelajar, 2005), hal. 119

Surat yang tidak bertandatangan, tidak diakui dalam KUH Perdata, karena tidak dapat diketahui siapa penulisnya. Surat bertanda tangan itu disebut dengan akta.

Dalam KUH Perdata, surat sebagai alat bukti tertentu dibagi atas dua, yaitu:

1. Akta di bawah tangan: penandatanganan atas surat/akta tersebut dilakukan tidak di depan pejabat umum atau tidak ditandatangani oleh pejabat umum, sebagaimana dijelaskan dalam KUH Perdata Pasal 1874, dan juga sebagian pada Pasal 1869.
2. Akta Otentik: penandatanganan surat/akta tersebut dilakukan di depan pejabat umum atau ditandatangani langsung oleh pejabat umum, sesuai Pasal 1868 KUH Perdata akta otentik memiliki kekuatan yang paling utama di depan hakim.

Sehingga menurut penulis, keberadaan hukum transaksi elektronik yang bertandatangan digital diperlakukan sama denga akta, baik akta di bawah tangan maupun akta otentik, selama tanda tangan tersebut dapat dibuktikan di pengadilan, dan tidak ada pembuktian terbalik atas tanda tangan digital tersebut.

Salah satu cara untuk mengetahui keotentikan tanda tangan digital tersebut adalah dengan cara melakukan pemeriksaan terhadap infrastruktur yang digunakan untuk membuat tanda tangan digital tersebut. Dalam hal ini, pemberi lisensi adalah *Certification Authority*. Oleh sebab itu, tanda tangan yang dihasilkan oleh infrastruktur kunci publik yang disediakan oleh CA yang

berlisensi seharusnya dapat langsung diterima di pengadilan tanpa harus membuktikan keasliannya.

Dalam hal sistem pembayaran elektronik, tidak ada alat bukti lain yang dapat digunakan selain data elektronik/digital berupa Tanda Tangan Digital. Untuk dapat diklasifikasikan dalam bentuk tertulis banyak cara yang dapat dilakukan. Salah satunya dengan membuat suatu *print out* atau *copy* dari pesan yang masih berbentuk elektronik. Walaupun hukum Indonesia belum mengatur hal ini secara spesifik, namun hukum Indonesia mengatur kebalikannya, peralihan tersebut terjadi dari bentuk tertulis ke bentuk data elektronik. Hal ini dapat ditemukan pada Pasal 12 UU No.8 Tahun 1997 tentang Dokumen Perusahaan yang berbunyi:

(1) Dokumen perusahaan dapat dialihkan ke dalam mikrofilm atau media lainnya;
(2) Pengalihan dokumen perusahaan ke dalam mikrofilm atau media lainnya sebagaimana dimaksud dalam ayat (1) dapat dilakukan sejak dokumen tersebut dibuat atau diterima oleh perusahaan yang bersangkutan;
(3) Dalam mengalihkan dokumen perusahaan sebagaimana yang dimaksud dalam ayat (1), pimpinan perusahaan wajib mempertimbangkan kegunaan naskah asli dokumen yang perlu tetap disimpan karena mengandung nilai tertentu demi kepentingan perusahaan atau kepentingan nasional;
(4) Dalam hal dokumen perusahaan yang dialihkan ke dalam mikrofilm atau media lainnya adalah naskah asli yang mempunyai kekuatan pembuktian otentik dan masih mengandung kepentingan hukum tertentu, pimpinan perusahaan wajib tetap menyimpan naskah asli tersebut.

Setelah proses pengalihan dokumen, suatu dokumen perusahaan membutuhkan adalah proses legislasi agar mempunyai kekuatan alat bukti.

Pasal 13 UU No. 8 Tahun 1997, berbunyi: "Setiap pengalihan dokumen perusahaan sebagaimana dimaksud dalam Pasal 12 ayat (1) wajib dilegalisasi."

Selanjutnya, Pasal 14, berbunyi:

(1) Legislasi sebagaimana dimaksud dalam Pasal 13 dilakukan oleh pimpinan perusahaan atau pejabat yang ditunjuk di lingkungan perusahaan yang bersangkutan, dengan dibuat berita acara;
(2) Berita acara yang dimaksud dalam ayat (1) sekurang-kurangnya memuat:
    a. keterangan tempat, hari, tanggal, bulan dan tahun dikeluarkannya legalisasi;
    b. keterangan bahwa pengalihan dokumen perusahaan yang dibuat di atas kertas ke dalam mikrofilm atau media lainnya telah dilakukan sesuai dengan aslinya;
    c. tanda tangan dan nama jelas pejabat yang bersangkutan.

Setelah proses pengalihan dan legalisasi, maka dokumen perusahaan tersebut dinyatakan sebagai alat bukti yang sah. Hal ini dapat didasarkan pada Pasal 15 UU No.8 Tahun 1997, yang berbunyi:

(1) Dokumen perusahaan yang telah dimuat dalam mikrofilm atau media lainnya sebagaimana dimaksud dalam Pasal 12 ayat (1) dan atau hasil cetakannya merupakan alat bukti yang sah;
(2) Apabila dianggap perlu dalam hal tertentu dan untuk keperluan tertentu dapat dilakukan legalisasi terhadap hasil cetak dokumen perusahaan yang telah dimuat dalam mikrofilm atau media lainnya.

Untuk memformulasikan aturan hukum, *Model Law on Electronic Commerce* layak untuk dijadikan acuan dalam pengaturan Tanda Tangan Digital ini.[52]

Pasal 5 *Uncitral Model Law on Electronic Commerce* menyatakan bahwa *data messages* mempunyai kekuatan hukum dan dapat dijalankan

[52] Abdul Halim Barakatullah, Bisnis *E-Commerce*: Studi Sistem Keamanan Di Indonesia (Yogyakarta: Pustaka Pelajar, 2005), hal. 129

secara hukum. *Model Law* menyatakan beberapa persyaratan agar suatu pesan dapat masuk ke dalam kriteria "*writing*". Kriteria yang dipakai adalah:[53]

1. Adanya bukti yang cukup yang dapat membuktikan adanya kata sepakat dari para pihak;
2. Memberitahukan kepada para pihak bahwa perbuatan yang dilakukannya ini mempunyai akibat hukum;
3. Memberitahukan bahwa dokumen tersebut berlaku kepada para pihak;
4. Mempertahankan keberadaan dokumen tersebut (dokumentasi) untuk suatu jangka waktu tertentu;
5. Memungkinkan dilakukannya otentifikasi terhadap dokumen tersebut dengan menggunakan tanda tangan yang ada;
6. Memudahkan verifikasi yang dilakukan oleh pemerintah atau untuk kepentingan pengadilan;
7. Untuk memudahkan para pihak menutup perjanjian *(finalize)* dan menyediakan bukti telah adanya kesepakatan itu;
8. Untuk memastikan data atau informasi yang ada belum pernah diubah/dirusak sejak ia pertama kali dibuat;
9. *Digital Signature* yang terdapat dalam pesan atau *data messages* ini adalah dibuat dalam suatu jangka waktu yang terdapat di dalam *certificate*;

[53] Muhammad Aulia Adnan (57-68) dikutip oleh Abdul Halim Barakatullah, Bisnis *E-Commerce*: Studi Sistem Keamanan Di Indonesia (Yogyakarta: Pustaka Pelajar, 2005), hal. 129-131

10. Untuk memudahkan pendokumentasian data dalam bentuk tertentu *(in tangible form);*
11. *Digital Signature* tersebut milik dari orang yang dianggap telah menandatangani. Berdasarkan hal ini maka sangat penting untuk menjaga kerahasiaan kunci privat agara jangan sampai digunakan oleh orang yang tidak berhak. Apabila kunci privat itu hilang atau dicuri orang, maka *certificate* pasangannya harus segera di-*revoke*;
12. *Digital Signature* yang digunakan oleh pemiliknya, digunakan dengan kesadaran yang penuh dari penandatangan. Penandatangan tersebut harus bebas dari unsur tekanan, paksaan ataupun kekhilafan;
13. Untuk menunjang dilakukannya kontrol dan audit untuk kepentingan akuntansi, pajak dan ketentuan perundangan yang berlaku lainnya.

C. Kedudukan Otoritas Sertifikasi dalam pengaturan mengenai Tanda Tangan Digital

a. Otoritas Sertifikasi (*Certification Authority*/CA)

Certification Authority adalah sebuah lembaga yang bertugas untuk memberikan sertifikasi jati diri pelanggan/subjek agar pelanggan itu bisa dikenali di dunia digital. Dengan cara memberikan autentifikasi dan verifikasi identitas, kemudian menerbitkan sertifikat untuk setiap pelangganya sehingga dalam transaksi yang dilakukan oleh pelanggan dengan pihak lain, CA berperan sebagai pihak ketiga yang terpercaya, dan memiliki kewajiban agar pelanggan yang telah menggunakan jasanya dapat dipercaya juga oleh

pihak lawan dalam transaksi tersebut. Dengan demikian, transaksi dapat berjalan dengan baik.[54]

Untuk dapat dipercaya, suatu CA harus memenuhi beberapa standar yang sudah ditetapkan secara internasional oleh masyarakat internet dan berlaku secara umum, seperti dalam ketentuan yang terdapat pada *UNCITRAL Model Law On Electronic Signatures 2001*, diantaranya adalah bahwa CA harus:[55]

1. menjalankan usahanya berdasarkan dengan ketentuan yang ada pada *Certificate Practice Statement* (CPS) dan *Certificate Policy* (CP);
2. melakukan dengan segala cara pengamanan untuk menjamin keakuratan dan keutuhan dari semua material yang mendukung keberadaan suatu sertifikat;
3. menyediakan kemudahan dalam pengaksesan sehingga pihak lain dapat melakukan pemeriksaan terhadap sertifikat, baik itu mengenai identitas dari penyedia jasa, pelanggan pemegang sertifikat dan keberlakuan sertifikat digital tersebut.
4. menjalankan sistem, prosedur dan sumber daya manusia yang *trustworthy* dalam usahanya sebagai penyedia jasa.

Standar yang telah ditetapkan ini merupakan persyaratan yang harus dipenuhi oleh CA, baik itu CA yang akan mulai beroperasi maupun CA yang sedang berjalan. Dengan demikian, semua CA yang ada terikat pada

---

[54] Edmon Makarim, Pengantar Hukum Telematika (Jakarta: PT RajaGrafindo Persada, 2005), hal. 407

[55] *ibid.*

ketentuan yang merupakan hasil dari konsensus masyarakat internet dan tentunya merupakan jaminan bahwa CA tersebut layak dipercaya sebagai pihak ketiga dalam transaksi.

Dengan demikian, hak dan kewajiban yang ditanggung oleh CA sama dengan hak dan kewajiban yang ditanggung oleh produsen. Tanggung jawab CA terhadap konsumennya sangat berpengaruh terhadap tingkat *trustworthy* dari CA itu sendiri karena apabila suatu CA menjalankan usahanya secara bertanggungjawab, dalam hal ini berarti berdasarkan prinsip kehati-hatian dan berdasarkan standar secara maksimal, hasil atau *output* yang keluar dari proses usahanya tersebut juga akan bagus sesuai dengan proses yang dijalankannya.

Dalam Dokumen UNCITRAL disebutkan bahwa *Certification Authorities* dalam suatu *Public Key Infrastucture* (PKI) dapat didirikan dalam suatu struktur yang hirarkis, yakni jika suatu *Certification Authority* hanya menjamin *Certification Authorities* yang lain, yang menyediakan langsung kepada pengguna *(subscriber)*. Dalam struktur tersebut, suatu *Certification Authority* adalah subordinat dari *Certification Authorities* yang lain.[56]

Supaya suatu CA mendapat kepercayaan dari masyarakat luas, ia harus memberikan pelayanan komunikasi yang aman bagi para pelaku transaksi. Karenanya, setiap CA harus membuat perjanjian kerjasama dengan CA lain dalam kerangka pembangunan suatu jaringan. Hal ini akan

---

[56] Danrivanto Budhijanto, "Aspek Hukum Digital Signature dan Certification Authorities Dalam Transaksi E-Commerce" dalam Cyber Law: Suatu Pengantar, (Bandung: ELIPS II, 2002), hal. 70

memudahkan pengguna (*subscriber*, pen.) dari setiap CA untuk berkomunikasi secara aman dengan setiap pengguna lainnya yang ada dalam suatu wilayah yurisdiksi negara yang sama.[57]

Tetapi, dalam kerangka kerja seperti ini, dengan tidak adanya suatu lembaga internasional yang berkaitan dengan CA yang diakui oleh negara-negara, kemungkinan timbulnya berbagai implikasi hukum yang berkaitan dengan tingkat keparcayaan tanda tangan digital yang disertifikasi oleh CA negara lain, menjadi sangat besar. Untuk meminimalisasi kemungkinan implikasi-implikasi tersebut, *cross recognition* yang biasa digunakan dalam Hukum Internasional, yakni dengan mendasar kepada asas resiprositas *(reciprocity principle)*.

Setiap CA, baik swasta maupun publik, harus memiliki dan mempertahankan syarat-syarat mutlak yang terkait erat dengan segala aktivitasnya, yakni:[58]

a. independensi;
b. keamanan internal;
c. arsip data jangka panjang;
d. sumber finansial dan pengetahuan hukum yang cukup;
e. *back up plan* yang terencana;
f. pengalaman dan kapabilitas yang cukup dalam teknologi enkripsi dan dekripsi dan keakraban yang cukup memadai terhadap prosedur pengamanan;
g. metode perlindungan yang baik untuk kunci pribadi milik CA itu sendiri;
h. prosedur pencabutan *(revocation procedures)*;
i. asuransi;
j. hubungan dan kerjasama yang baik dengan CA yang lain, baik dalam yurisdiksi negara yang sama maupun dengan CA di luar negeri; dan

---

[57] *Ibid.*
[58] *Ibid.*

k. sumber daya manusia yang baik dan manajemen yang handal.

Di samping itu, sebagai penyelenggara jasa, CA harus menjamin hak-hak pengguna (*subscriber)* antara lain:

1. Privacy

Termaktub dalam Pasal 4 butir 1 UU NO 8 tahun 1999 tentang Perlindungan Konsumen. Contoh: Ketika *subscriber* memohon kepada CA, *subscriber* akan dimintai keterangan mengenai identitasnya, besar kecilnya keakuratan dari identitas tersebut tergantung pada 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 *subscriber* dari pihak yang tidak berkepentingan. CA hanya boleh mengkonfirmasi bahwa sertifikat yang dimiliki oleh *subscriber* 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 diangkat berdasarkan undang-undang) apabila mereka tidak merasa puas terhadap cara orang atau organisasi yang mengumpulkan informasi dan menurut keadaan-keadaan tertentu, individu-individu memiliki hak atas ganti kerugian.[59]

Pelanggaran terhadap prinsip-prinsip perlindungan data dapat menyebabkan tanggung jawab pidana, adapun prinsip-prinsip tersebut antara lain:[60]

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

---

[59] Mukti Fajar. Aspek Hukum Pembuktian *Digital Evidence* Dalam *Electronic Commerce*. http://www.umy.ac.id/hukum/download /fajar. htm), diakses tanggal 14 Maret 2006.

[60] *Ibid.*

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:
      - 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 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 *susbcriber*. 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 system* 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 *subscriber* sesuai dengan apa yang ia minta berdasarkan informasi yang diterimanya. Ketepatan informasi (informasi yang benar tanpa tipuan) juga merupakan prinsip *accuracy*. Sebagai contoh: *subscriber* 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 *subscriber* berhak untuk mendapatkan CA yang berlisensi artinya ketika *subscriber* mengakses ke CA, terdapat praduga

protokol *Secure Electronic Transaction* (SET)[61] yang dirancang oleh Visa dan MasterCard. VeriSign lebih mengkonsentrasikan dirinya pada pemberian sertifikat digital untuk individu atau badan usaha umum.[62]

b. IndoSign, otoritas sertifikasi pertama di Indonesia, dibentuk pada tahun 2000. Anggota pertama otoritas sertifikasi ini adalah Indosatcom, PT Pos, Lintas Artha, PPAU Mikroelektronika ITB, Telkom, Kadin, dan Deperindag.[63]

Namun, ketiadaan regulasi khusus yang mengatur mengenai *Digital Signature, Certification Authorities and Related Legal Issues* menyebabkan kurang berkembangnya Otoritas Sertifikasi ini.

b. Sertifikat Digital (*Digital certificate)*

Sertifikat Digital adalah informasi mengenai identitas pemilik yang ditandatangani secara digital oleh sebuah badan independen yang menjamin bahwa si pemilik sertifikat layak untuk ikut dalam transaksi jual beli tersebut Termasuk dalam informasi yang terdapat dalam sertifikat digital adalah kunci publik, sehingga sertifikat digital ini juga merupakan mekanisme pertukaran kunci publik[64].

---

[61] Protokol *Secure Electronic Transaction* (SET) dirancang oleh sebuah konsorsium yang antara lain melibatkan Visa, Mastercard, Microsoft, Netscape, IBM, dan lain-lain. Tujuannya adalah untuk menetapkan standard teknis tunggal yang nantinya akan digunakan untuk melindungi jual beli yang dilakukan dengan menggunakan kartu kredit melalui internet.

[62] Tanya Jawab Seputar Tanda Tangan & Sertifikat Digital, (http:www.hukumonline.com), tanggal 14 Maret 2006

[63] Ihsan Hariadi, Sertifikat Digital Pertama, http://www.mail-archive.com/itb@itb.ac.id/msg13940.html, diakses tanggal 24 Juli 2006

[64] Budi Agus Riswandi, Hukum dan Internet di Indonesia (Yogyakarta: UII Press, 2003), hal. 52

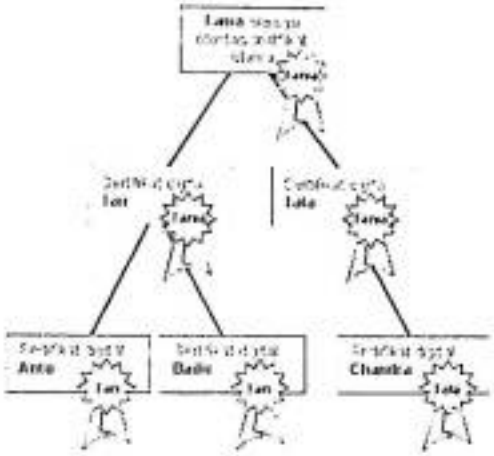
Sertifikat digital selain berisi kunci publik juga berisi informasi lengkap mengenai jati diri pemilik kunci tersebut, sebagaimana layaknya KTP, seperti nomor seri, nama pemilik, kode negara/perusahaan, masa berlaku dsb. Sama halnya dengan KTP, sertifikat digital juga ditandatangani secara digital oleh lembaga yang mengeluarkannya, yakni otoritas sertifikat atau *certificate authority* (CA). Dengan menggunakan kunci publik dari suatu sertifikat digital, pemeriksa tanda tangan dapat merasa yakin bahwa kunci publik itu memang berkorelasi dengan seseorang yang namanya tercantum dalam sertifikat digital itu.[65]

Sertifikat digital ini selain mempunyai hubungan dengan kunci publik dan identitas pemilik, ia juga memiliki hubungan yang sangat erat dengan nomor rekening bank pemilik sertifikat ini. Walaupun tidak secara langsung informasi rekening bank ini tercantum dalam sertifikat, CA menyimpan nomor rekening tersebut dalam basis data miliknya, sehingga nomor rekening tersebut dapat diasosiasikan denga sertifikatnya. Terdapat kedudukan hirarki di antara CA. Sebuah CA dapat memiliki sertifikat yang ditandatangani oleh CA di tingkat atasnya, demikian pula di tingkat lebih atasnya lagi, begitu seterusnya sampai *Root* CA. Sertifikat *Root* CA ditandatangani oleh dirinya sendiri. Oleh karena tingkatan sertifikat CA identik dengan tingkatan kunci publik, maka *Root* CA sering disebut dengan *Root key*[66].

---

[65] Arianto Mukti Wibowo, Mengenal Tanda Tangan & Sertifikat Digital (http://www.infokomputer.com/arsip/internet/0698/cakra/cakrawa2.shtml), diakses tanggal 22 Juli 2006

[66] *ibid.*



- Root CA: CA yang menandatangni sertifikat CA yang lain
- Sertifikat root CA: self-sign
- Distribusi sertifikat Root CA biasanya di luar network
- Jika root CA dijebol maka seluruh piramida di bawahnya akan runtuh

Contoh hirarki *root* otoritas sertifikasi
Sumber: http://www.bl.ac.id/dosen/imelda/download/1

Mengenai manajemen sertifikat, dalam sebuah model *public key infrastructure* terdapat beberapa pihak, yaitu:[67]

1. *Subject* atau *subscriber*
2. Otoritas Sertifikasi *(Certification Authority/*CA)
3. *Registration Authority* (RA)
4. *Certificate Repository*
5. *Relying Party*

Subscriber

Sebenarnya *subscriber* dari sebuah sertifikat digital tidaklah harus orang atau perusahaan, namun bisa juga peralatan (*device*) pada jaringan, aplikasi *software* dan *downloadable application*. Seorang *subscriber* harus bisa menjaga *private key*-nya baik-baik, jangan sampai tercuri oleh orang lain.

[67] Konsep Infrastruktur Kunci Publik (*Public Key Infrastructure / PKI*) (http://www.cs.ui.ac.id/kuliah/infosec/kuliah/Transparan%20Digisec-3%20PKI.doc), disadur tanggal 22 Juli 2006

Untuk keamanan dari kunci privat *subcriber*, biasanya kunci itu disimpan dalam PSE (*Personal Security Environment*) yang baik seperti dalam *smartcard*. Namun, karena faktor biaya, kadang kala kunci privat itu cukup dienkripsi dalam sebuah file sehingga bisa diletakkan di *hard disk*, disket atau CD-ROM.

Certification Authority

Certification Authority (CA) ada sebuah lembaga yang bertugas untuk mensertifikasi jati diri *subscriber / subject* agar *subscriber* itu bisa dikenali di dunia digital, dengan menerbitkan sertifikat digital untuk tiap *subscriber*nya.

Tentunya, CA harus merupakan entitas yang independen dan terpercaya (*trusted third party*).

Untuk memberikan gambaran bagaimana CA bekerja, kita ambil contoh bagaimana cara sebuah perusahaan meminta SSL.[68] Perusahaan itu perlu menunjukkan kepada CA dua lembar surat, yakni surat ijin usaha dan surat izin penggunaan suatu *domain name* tertentu. Barulah setelah memeriksa keabsahan kedua dokumen tersebut, CA menerbitkan sertifikat digital SSL untuk perusahaan yang bersangkutan.

CA-internal di sebuah perusahaan bisa saja mengeluarkan *digital ID* buat pegawainya, untuk keluar masuk ruangan (*access control card*).

---

[68] SSL merupakan singkatan dari *Secure Socket Layer*, yaitu sebuah protocol yang dirancang oleh Netscape Communications untuk memungkinkan dilakukannya enkripsi dan pengabsahan terhadap komunikasi-komunikasi yang dilakukan melalui internet. SSL ini sebagian besar digunakan (namun tidak secara eksklusif) di dalam komunikasi-komunikasi yang terjadi antara web browser dan web server. URL-URL (*Uniform Resource Locator* –sistem pembuatan alamat standard untuk *World Wide Web*) yang diawali dengan 'https' (bukannya 'http') mengindikasikan bahwa URL tersebut akan menggunakan koneksi SSL.

Registration Authority

Registration authority (RA) bertanggung jawab untuk melakukan proses identifikasi dan otentikasi terhadap *subscriber* dari sertifikat digital, tetapi tidak menandatangani sertifikat itu. Dalam kehidupan sehari-hari, banyak sekali dokumen yang diperiksa namun ditandatangani oleh orang yang berbeda.

Adanya sebuah RA dalam PKI memang sifatnya *optional* (tidak harus ada), karena memang RA hanya menjalankan beberapa tugas yang didelegasikan oleh CA jika CA tidak sanggup melakukannya. Artinya, bisa saja dalam suatu skenario tertentu, seluruh tugas RA berada dalam CA. Tugas-tugas RA dapat mencakup:

- Otentikasi calon *subscriber* secara fisik
- Registrasi calon *subscriber*
- Membuat pasangan key untuk *subscriber* (jika *subscriber* tidak sanggup membuat sendiri pasangan kuncinya).
- Membuat backup dari kunci privat yang dipergunakan untuk enkripsi (*key recovery*)
- Pelaporan kalau ada sertifikat yang dicabut (*revocation reporting*)

Certificate Repository

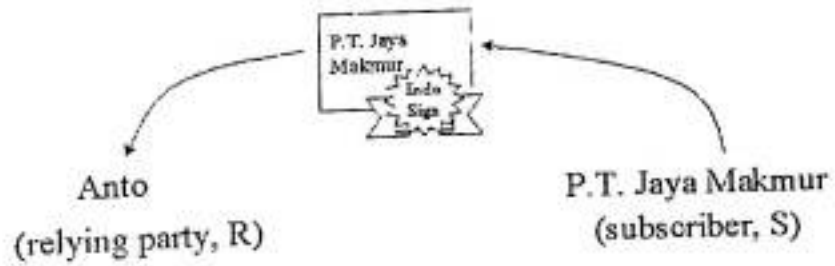
Seorang *subscriber* dapat menyerahkan sertifikat digitalnya kepada orang lain yang ingin berkomunikasi dengan aman dengannya. Teknik penyerahan sertifikat digital oleh pribadi ini disebut dengan istilah *private dissemination*. Tapi, teknik ini memiliki beberapa kekurangan:

1. Teknik ini hanya bisa untuk PKI dengan user dalam jumlah kecil. Artinya *scalability*-nya rendah, karena penyebaran informasinya tidak 'meluas'.
2. Umumnya tidak sesuai dengan struktur perusahaan pada umumnya, yang cenderung sifatnya *centralized/hierarchial*, ketimbang *user-centric*.

Sebuah tempat penyimpanan (*repository*) *on-line* untuk sertifkat digital dibutuhkan dalam PKI. *Repository* ini juga berguna untuk menyimpan daftar sertifikat yang dibatalkan/CRL (yang tidak berlaku sebelum masa berlakunya habis).

Relying Party

Relying party adalah pihak yang mempercayai keberadaan dan keabsahan suatu sertifikat digital.



Gambar 1. Konsep *relying party*

Kemungkinan Anto mengenali dan mengakui keabsahan dari sertifikat digital tersebut, karena:

1. Anto mengakui IndoSign sebagai pihak ketiga yang dipercaya yang melakukan proses sertifikasi. Karena itu, Anto mengakui keabsahan sertifikat yang ditandatangani IndoSign.

2. Sertifikat *web server* (*SSL certificate*) P.T. Jaya Makmur ditandatangani oleh IndoSign.
3. Maka Anto mengakui keotentikan *web server* P.T. Jaya Makmur.

Anto adalah *relying party*.

BAB V

PENUTUP

A. Kesimpulan

1. Tanda tangan digital belum diatur sepenuhnya oleh hukum di Indonesia. Sehingga yang menjadi acuan adalah peraturan yang bersifat umum, yaitu Buku III KUH perdata Indonesia dengan sistem terbuka dalam hal kebebasan membuat suatu perjanjian selama tidak bertentangan dengan norma-norma kesusilaan dan ketertiban umum serta tidak bertentangan dengan hukum yang berlaku di Indonesia. Menurut hakim di Pengadilan Negeri Makassar, perjanjian yang menggunakan tanda tangan digital dapat dianggap sah apabila para pihak mengakui keberadaan dan kebenaran tanda tangan digital tersebut.
2. Tanda tangan digital dapat dijadikan alat bukti yang sah, walaupun tidak mempunyai kekuatan pembuktian yang sempurna, sehingga harus didukung dengan alat-alat bukti lainnya seperti bukti-bukti tulisan lainnya, keterangan saksi atau kesaksian, persangkaan-persangkaan, pengakuan dan sumpah. Tanda Tangan Digital yang dalam hal ini telah berwujud dokumen, akan menjadi suatu akta apabila tulisan atau dokumen tersebut dibubuhi tanda tangan dan akan menjadi akta otentik bila dibuat di hadapan atau oleh pejabat notaris.

3. Otoritas Sertifikasi berwenang untuk mengeluarkan suatu tanda tangan digital apabila *subscriber* telah memenuhi syarat-syarat yang telah ditetapkan sebelumnya oleh Otoritas Sertifikasi tersebut. Di samping itu, Otoritas sertifikat juga bertanggungjawab terhadap kerahasiaan *subscriber* berdasarkan prinsip kepercayaan dan prinsip kehati-hatian.

B. Saran

1. Transaksi elektronik yang dilakukan secara virtual *(Electronic Commerce)* semakin hari akan semakin berkembang karena keunggulannya yang melebihi perdagangan konvensional. Di sisi lain, belum adanya aturan yang jelas membuat adanya ketimpangan yang terjadi. Sehingga diperlukan suatu tatanan hukum yang secara spesifik mengatur mengenai perdagangan secara elektronik pada umumnya, dan tanda tangan digital pada khususnya.
2. Perlunya dibentuk suatu lembaga atau badan khusus yang dapat menjembatani kepentingan-kepentingan para pihak seperti konsumen, produsen, *intermediatries*, maupun pemerintah dalam bertransaksi secara elektronik.

DAFTAR PUSTAKA

AK, Syahmin. ***Hukum Kontrak Internasional***. (Jakarta: PT RajaGrafindo Persada, 2005)

Barkatullah, Abdul Halim, ***Bisnis E-Commerce: Studi Sistem Keamanan dan Hukum di Indonesia***. (Yogyakarta: Pustaka Pelajar. 2005)

Budhijanto, Danrivanto, "Aspek Hukum Digital Signature dan Certifcation Authorities dalam Transaksi E-Commerce" dalam ***Cyber Law: Suatu Pengantar*** (Bandung: Elips II, 2002)

Fuady, Munir. **Hukum Kontrak Dari Sudut Pandang hukum Bisnis** (Bandung, PT Citra Aditya Bakti, 2001)

Harahap, M. Yahya. ***Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian, dan Putusan Pengadilan***. (Jakarta: Sinar Grafika. 2005)

H.S., Salim. ***Hukum Kontrak: Teori dan Teknik Penyusunan Kontrak***. (Jakarta: Sinar Grafika. 2003)

Ikhwansyah, Isis. "Prinsip-prinsip Universal Bagi Kontrak Melalui E-Commerce dan Sistem Hukum Pembuktian Perdata dalam Teknologi Informasi" dalam ***Cyber Law: Suatu Pengantar*** (Bandung: Elips II, 2002)

Makarim, Edmon. ***Pengantar Hukum Telematika: Suatu Kompilasi Kajian*** (Jakarta: PT RajaGrafindo Perkasa, 2005)

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

Riswandi, Budi Agus. ***Hukum Cyberspace*** (Yogyakarta: Gita Nagari, 2006)

_____. ***Hukum dan Internet di Indonesia***.(Yogyakarta. UII Press. 2003)

Sanusi, M. Arsyad, ***E-Commerce: Hukum dan Solusinya*** (Bandung: PT Mizan Grafika Sarana, 2001)

Sumber Lain:

Global Technology, http://www.globaltechnology.co.id/seminar/e-commerce/seri001.htm, diakses tanggal 5 Agustus 2006

Hariadi, Ihsan. ***Sertifikat Digital Pertama***, http://www.mail-archive.com/itb@itb.ac. id/msg13940.html, diakses tanggal 24 Juli 2006

Konsep Infrastruktur Kunci Publik (Public Key Infrastructre/PKI) (http://www.cs.ui.ac.id/kuliah/infosec/kuliah/transparan%20%Digisec3%20PKI.doc), diakses tanggal 22 Juli 2006

ND, Mukti Fajar. ***Aspek Hukum Pembuktian Digital Evidence Dalam Electronic Commerce***. http://www.umy.ac.id/hukum/download/fajar. htm), diakses tanggal 14 Maret 2006

Wibowo, Arrianto Mukti. ***Kerangka Hukum Digital Signature.*** http://www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html, diakses tanggal 14 Maret 2006

Wibowo, Arianto Mukti ***Mengenal Tanda Tangan & Sertifikat Digital*** (http://www.infokomputer.com/arsip/internet/0698/cakra/cakrawa2.shtml), diakses tanggal 22 Juli 2006

Peraturan Perundang-undangan:

Indonesia, **Undang-undang Tentang Perlindungan Konsumen**, UU No. 8 Tahun 1999.

Indonesia, **Undang-undang Tentang Telekomunikasi,** UU No. 36 Tahun 1999 .

Indonesia, **Undang-undang Tentang Dokumen Perusahaan**, UU No. 8 Tahun 1997.

Kitab Undang-undang Hukum Perdata (Burgerlijk Wetboek), diterjemahkan oleh R. Subekti daR. Tjitrosudibio, cet. 18, (Jakata: PT. Pradnya Paramita, 1984).

UNCITRAL *Model Law on Electronic Commerce* *as asopted by the General Assembly Resolution* 51/162 of December 16, 1996 (*with additional Article 5 bis as adopted in* 1998).