

TESIS

**PEMBUKTIAN *DIGITAL SIGNATURE*  
DALAM *E-COMMERCE***

**Diajukan untuk memenuhi sebagian persyaratan  
Guna memperoleh Gelar Master  
Program Magister (S-2) Ilmu Hukum  
Universitas Islam Indonesia Yogyakarta**

OLEH:

NAMA : AZWIR  
NIM : 04 M 0079  
BKU : HUKUM BISNIS

---

**PROGRAM MAGISTER (S2) ILMU HUKUM  
UNIVERSITAS ISLAM INDONESIA  
YOGYAKARTA  
2006**

**HALAMAN PENGESAHAN**

**TESIS**

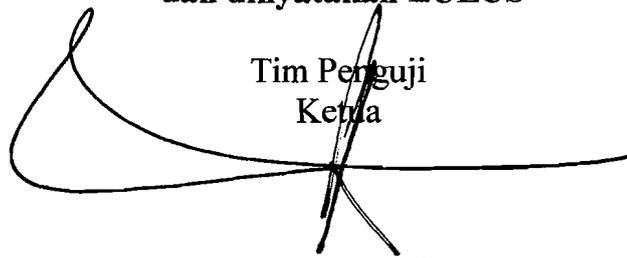
**PEMBUKTIAN *DIGITAL SIGNATURE*  
DALAM *E-COMMERCE***

*Disusun Oleh*

**Nama : Azwir**  
**Nomor Mahasiswa : 04 M 0079**  
**Program Studi : Ilmu Hukum**  
**Bidang Kajian Utama : Hukum Bisnis**

**Telah Dipertahankan di depan Dewan Penguji  
Pada tanggal 16 September 2006  
dan dinyatakan LULUS**

Tim Penguji  
Ketua



**(DR. Ridwan Khairandy, SH, MH)**

Anggota



**(Siti Anisah, SH, M.Hum)**

Anggota



**(Fahmi, SH, MH)**

Mengetahui

Direktur Program Pasca Sarjana Fakultas Hukum  
Universitas Islam Indonesia  
Yogyakarta



**(DR. Ridwan Khairandy, SH, MH)**

**HALAMAN PERSETUJUAN**

**TESIS**

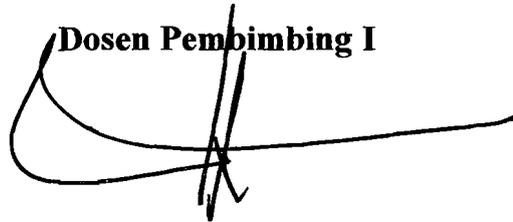
**PEMBUKTIAN *DIGITAL SIGNATURE*  
DALAM *E-COMMERCE***

*Disusun Oleh*

**Nama : Azwir**  
**Nomor Mahasiswa : 04 M 0079**  
**Program Studi : Ilmu Hukum**  
**Bidang Kajian Utama : Hukum Bisnis**

**Telah dilakukan pembimbingan dan disetujui layak untuk  
diajukan di hadapan Tim Penguji Tesis Program Pasca Sarjana  
Fakultas Hukum Universitas Islam Indonesia Yogyakarta**

**Dosen Pembimbing I**



**(DR. Ridwan Khairandy, SH, MH)**

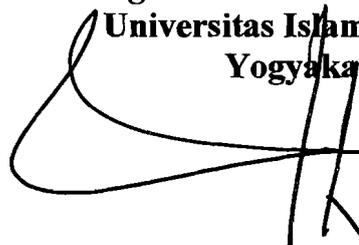
**Dosen Pembimbing II**



**(Fahmi, SH, MH)**

**Mengetahui**

**Direktur Program Pasca Sarjana Fakultas Hukum  
Universitas Islam Indonesia  
Yogyakarta**



**(DR. Ridwan Khairandy, SH, MH)**



## ABSTRAK

Tesis ini mengangkat tema tentang *e-commerce* dengan mengambil judul **Pembuktian *Digital Signature* dalam Transaksi Bisnis dengan *E-Commerce***. Pengangkatan tema tersebut dikarenakan semakin maraknya bisnis yang menggunakan manfaat internet sebagai media *marketing*, *bargaining*, perjanjian dagang dan transaksi. Dengan kata lain perdagangan semakin tidak bisa lepas dari fungsi internet.

Secara spesifik akan dijelaskan sistematika ke dalam bab per bab sebagai berikut:

Bab I yang berisikan latar belakang masalah, rumusan masalah, tujuan penelitian dan kerangka teori yang menjadi tolak ukur dalam pembahasan lebih lanjut serta metode penelitian yang dipakai dalam penelitian dan penulisan tesis ini. Di dalam permasalahan yang timbul sebagai bahan analisis dengan disertai pembuktian pada bab selanjutnya menurut data-data akurat yang diberikan.

Bab II memaparkan secara umum tentang batasan *e-commerce*, sistem keamanan *e-commerce*, definisi kriptografi dan penggunaan kriptografi. Ilmu ini sebagai salah satu acuan atau rujukan dalam hal pembuktian sehingga dapat lebih mempertajam analisa terhadap permasalahan tersebut.

Bab III merupakan pembahasan atas rumusan masalah berdasarkan hasil penelitian. Pemaparan tentang operasional *digital signature*, mengenai pembuktian *digital signature*, pembuktian dalam peradilan Indonesia, pembuktian di luar badan peradilan selain *alternative dispute resolution*, dan aspek perlindungan konsumen dan sekaligus di dalam pembahasan ini diberikan perbandingan sebagai salah satu cara memandang kasus tersebut di atas khususnya di dalam kerangka mencari aspek pembuktian melewati norma aturan yang berlaku, sehingga di masa mendatang akan lebih mudah mendapatkan kepastian hukumnya.

Bab IV merupakan bagian penutup dalam penulisan tesis ini yang memuat bagian kesimpulan dan saran. Seperti yang telah di bahas dalam Bab III maka di dalam kesimpulan saran ini perlu sekali untuk lebih diberikan pencermatan mengenai aspek hukum *normative* bagi para pelaku bisnis dalam bidang ini.

Sebagai salah satu referensi data yang diambil maka tesis ini dilengkapi dengan daftar pustaka dan lampiran pada bagian akhir.

## KATA PENGANTAR

Assalamu'alaikum wr, wb.

Dengan mengucapkan syukur alhamdulillah kehadirat Allah SWT, karena berkat rahmat dan karunia-Nya akhirnya penulis dapat menyelesaikan penulisan tesis dengan judul Pembuktian Digital Signature Dalam E-Commerce Adapun dilakukannya penulisan tesis ini adalah dalam penyelesaian ujian Master Hukum pada Program Pasca Sarjana Fakultas Hukum Universitas Islam Indonesia bekerja sama dengan Universitas Lancang Kuning Pekanbaru, Riau.

Kemudian dengan selesainya tesis ini, ucapan terima kasih dan penghargaan yang tiada terhingga penulis sampaikan kepada semua pihak yang telah membantu baik langsung maupun tidak langsung secara moral dan materil demi terlaksanya penulisan tersebut.

Dalam kesempatan yang sama penulis ingin menyampaikan ucapan terima kasih dan penghargaan yang setinggi-tingginya kepada yang terhormat :

1. Prof.DR.Ir Luthfy Hasan, MS, selaku Rektor Universitas Islam Indonesia.
2. DR.Ir.Irwan Effendi,MSc,selaku Rektor Universitas Lancang Kuning
3. DR.Ridwan Khirandy,SH,MH selaku Dosen Pembimbing I dan sekaligus Direktur Program Pasca Sarjana Fakultas Hukum Universitas Islam Indonesia, Yogyakarta atas perhatian, bantuan pemikiran, saran dan bimbingan.
4. Hj. Hasnati Hasan, SH, HM, selaku Ketua Program Studi Magister Ilmu Hukum Universitas Lancang Kuning, Riau
5. Fahmi, SH, MH, selaku Pembimbing II atas segala bantuannya di dalam membimbing penulis, hingga tesis ini dapat terselesaikan.
6. Bukhari Ibrahim, orang tuaku yang selaku memberikan dorongan untuk selalu menambah ilmu pengetahuan terutama S-2 ini.

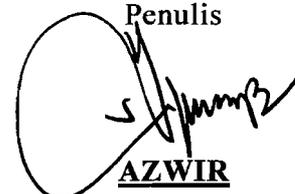
7. Dra. Hj. Fatimah Hadi, mertuaku yang selalu mendidik supaya selalu menambah ilmu pengetahuan.
8. Dra. Nizma Hanum, Istriku tercinta yang selalu mendorong supaya dapat menyelesaikan magister hukum tersebut.
9. Danny Firmansyah, Anakku tersayang yang mendorong selalu supaya ayah lulus menempuh ujian tesis tersebut.
10. Rekan – rekan seangkatan (angkatan I dan II) Program Pasca Sarjana Fakultas Hukum Universitas Islam Indonesia bekerja sama enagn Universitas Lancang Kuning Pekanbaru, Riau.

Mengingat segala keterbatasan, kemampuan maupun literatur yang diperoleh, maka segala kritik maupun saran yang bersifat membangun akan penulis terima dengan penuh keterbukaan dan senang hati guna penyempurnaan tesis ini. Segala amal kebaikan yang telah diberikan oleh semua pihak senantiasa bermanfaat dan mendapatkan ridho dari Allah SWT, Amien.

Akhirnya penulis berharap semoga tesis ini dapat bermanfaat khususnya pada penulis sendiri dan umu bagi para pembaca.

Wassalamu'aikum wr, wb.

Pekanbaru, Juni 2006

Penulis  
  
AZWIR

## DAFTAR ISI

<b>HALAMAN JUDUL</b>	
<b>HALAMAN PENGESAHAN</b> .....	i
<b>HALAMAN PERSETUJUAN</b> .....	ii
<b>ABSTRAK</b> .....	iii
<b>KATA PENGANTAR</b> .....	iv
<b>DAFTAR ISI</b> .....	vi
<b>BAB I : PENDAHULUAN</b>	
A. Latar Belakang Masalah .....	1
B. Rumusan Masalah .....	9
C. Tujuan Penelitian .....	9
D. Tinjauan Pustaka.....	10
E. Metode Penelitian .....	14
F. Sistematika Penulisan.....	16
<b>BAB I : TRANSAKSI BISNIS DENGAN <i>E-COMMERCE</i> DAN SISTEM PENGAMANANNYA.</b> .....	18
A. Pengertian <i>e-commerce</i> .....	20
B. Macam Transaksi Bisnis Dengan Sistem <i>e-commerce</i> ..	25
C. Keabsahan Kontrak Bisnis dengan Menggunakan <i>e- commerce</i> .....	30
<b>BAB III : PENGGUNAAN <i>DIGITAL SIGNATURE</i> DALAM TRANSAKSI BISNIS <i>E-COMMERCE</i></b> .....	47
A. Penggunaan <i>Digital Signature</i> Dalam Transaksi Bisnis Dengan E-Commerce .....	47
B. Kekuatan Pembuktian <i>Digital Signature</i> Dalam Sistem Hukum Indonesia .....	64
C. Aspek Perlindungan Konsumen Dalam <i>Digital Signature</i> ..	93

**BAB IV : PENUTUP**

A. Kesimpulan .....	100
B. Saran – saran .....	100

<b>DAFTAR PUSTAKA .....</b>	<b>103</b>
-----------------------------	------------

# BAB I

## PENDAHULUAN

### A. Latar Belakang Masalah

Dunia perdagangan saat ini semakin meningkat aktifitas dan perluasannya baik perdagangan domestik maupun perdagangan yang melintasi batas-batas teritorial suatu negara atau perdagangan internasional. Berbagai bentuk kesibukan di bandara-bandara dan pelabuhan menggambarkan volume perdagangan semakin meningkat dari waktu ke waktu.

Dalam perdagangan klasik, terjadi pertemuan langsung (tatap muka) antara penjual dan pembeli. Secara umum dalam perdagangan konvensional, dalam suatu proses transaksi perdagangan terdapat momen yang menuntut penjual dan pembeli berhadapan secara langsung.

Perkembangan teknologi informasi (TI) dan khususnya juga Internet ternyata tak hanya mengubah cara bagaimana seseorang berkomunikasi, mengelola data dan informasi, melainkan lebih jauh dari itu mengubah bagaimana seseorang melakukan bisnis. Banyak kegiatan bisnis yang sebelumnya tak terpikirkan, kini dapat dilakukan dengan mudah dan cepat dengan model-model bisnis yang sama sekali baru. Begitu juga, banyak kegiatan lainnya yang dilakukan hanya dalam lingkup terbatas kini dapat dilakukan dalam cakupan yang sangat luas, bahkan mendunia.

Namun, lebih dari itu, perubahan-perubahan yang terjadi juga dinilai sangat revolusioner. Munculnya bisnis dotcom, meski terbukti sebagian besar mengalami kegagalan, tetapi sebagian besar lainnya mengalami keberhasilan, dan

sekaligus ini dianggap fenomenal. Karena selain itu merupakan sesuatu yang sama sekali baru, dimensinya pun segera mendunia.

Di sisi lain, perkembangan TI dan Internet ini, juga telah sangat mempengaruhi hampir semua bisnis di dunia untuk terlibat dalam implementasi dan menerapkan berbagai aplikasi. Banyak manfaat dan keuntungan yang bisa diraih kalangan bisnis dalam kaitan ini, baik dalam konteks internal (meningkatkan efisiensi dan efektivitas organisasi), dan eksternal (meningkatkan komunikasi data dan informasi antar berbagai perusahaan pemasok, pabrikan, distributor) dan lain sebagainya.

Terkait dengan semua perkembangan tersebut, yang juga harus menjadi perhatian adalah bagaimana hal-hal baru tersebut, misalnya dalam kepastian dan keabsahan transaksi, keamanan komunikasi data dan informasi, dan semua yang terkait dengan kegiatan bisnis, dapat terlindungi dengan baik karena adanya kepastian hukum. Mengapa diperlukan kepastian hukum yang lebih kondusif, meski boleh dikata sama sekali baru, karena perangkat hukum yang ada tidak cukup memadai untuk menaungi semua perubahan dan perkembangan yang ada.

Hadirnya masyarakat informasi (*information society*) yang diyakini sebagai salah satu agenda penting masyarakat dunia di milenium ketiga antara lain ditandai dengan pemanfaatan Internet yang semakin meluas dalam berbagai aktivitas kehidupan manusia, bukan saja di negara-negara maju tapi juga di negara-negara berkembang termasuk Indonesia. Fenomena ini pada gilirannya telah menempatkan "informasi" sebagai komoditas ekonomi yang sangat penting dan menguntungkan. Untuk merespon perkembangan ini Amerika Serikat sebagai pionir dalam pemanfaatan Internet telah mengubah paradigma ekonominya dari

ekonomi yang berbasis manufaktur menjadi ekonomi yang berbasis jasa (*from a manufacturing-based economy to a service-based economy*). Perkembangan teknologi internet saat ini telah masuk dalam dunia perdagangan sehingga mempermudah proses perpindahan barang dari produsen hingga konsumen.<sup>1</sup>

Kemajuan internet dalam perdagangan menghadirkan pelayanan *Digital Signature* sebagai sarana untuk legalitas perjanjian/kontrak jual-beli tanpa harus bertemu secara tatap muka antara pembeli dan penjual. Sistem kontrak perdagangan dengan cara ini telah banyak dilakukan oleh para pelaku perdagangan baik domestik maupun internasional.<sup>2</sup>

Kontrak perdagangan internasional secara umum (bukan dalam konteks *e-commerce*) diatur dalam *United Nations in Contracts for International Sale of Goods* (UNCISG) 1980 dan 1986. Indonesia belum meratifikasi untuk UNCISG tahun 1980, meskipun demikian konvensi ini patut kita pertimbangkan sebagai platform bagi konvensi jual beli internasional yang baru. Konvensi ini mengatur masalah-masalah kontraktual yang berhubungan dengan kontrak jual beli internasional. Konvensi ini sebenarnya hanya mengatur masalah jual beli antara *business to business* (B2B), sedangkan *e-commerce* yang kita bahas disini adalah hubungan bisnis antara *Business to Consumer* (B2C) dan juga *business to business* tetapi didalam konvensi tersebut terdapat beberapa prinsip yang dapat di

---

<sup>1</sup> Richardus Eko Indrajit, "Manajemen Sistem Informasi dan teknologi Informasi", PT. Elex Media komputindo, 2000. Hlm. 60.

<sup>2</sup> Badrulzaman, Mariam Darus, *E-Commerce Tinjauan dari Hukum Kontrak Indonesia*, Jurnal Hukum Bisnis. 2000. Hlm. 21.

adopsi dalam makalah ini. Konsepsi yang bisa diambil dari konvensi ini antara lain adalah:<sup>3</sup>

1. Kontrak tidak harus dalam bentuk tertulis (*in writing form*), tetapi kontrak tersebut bisa saja berbentuk lain bahkan hanya berdasarkan saksi. Berdasarkan aturan tersebut suatu kontrak dapat juga dalam bentuk data elektronik (misalnya dalam format data form yang di-sign dengan *digital signature*) tapi didalam UNCISG ini belum diatur secara spesifik mengenai *digital signature*. Berdasarkan hal tersebut diatas maka suatu kontrak jual-beli secara internasional yang menggunakan *digital signature* berdasarkan hukum internasional secara hukum mengikat (*legally binding*) atau mempunyai kekuatan hukum.

Mengenai sahnya suatu kontrak yang berbentuk *digital signature* ini sebaiknya diatur dalam perundang-undangan tersendiri seperti halnya yang dilakukan di Amerika (negara bagian Utah, California), Malaysia, Singapura.

2. CISG mencakup materi pembentukan kontrak secara internasional yang bertujuan meniadakan keperluan menunjukkan hukum negara tertentu dalam kontrak perdagangan internasional serta untuk memudahkan para pihak dalam hal terjadi konflik antar sistem hukum . CISG berlaku terhadap kontrak untuk penjualan barang yang dibuat diantara pihak yang tempat dagangnya berada di negara yang berlainan pasal (1(1)). Dengan demikian

---

<sup>3</sup> Grup Riset Digital Security & Electronic Commerce, *Aplikasi Teknologi Sekuriti Digital*, Fakultas Ilmu Komputer Universitas Indonesia.. 1999.

yang menentukan adalah tempat perdagangannya dan bukan kewarganegaranya. Dalam konteks *digital signature* tempat kedudukan dari Merchant yang adalah kedudukan hukum yang tercantum di digital certificate miliknya. Suatu kontrak yang dibuat berdasarkan CISG (misalnya berupa *digital signature*) atau yang tunduk kepada CISG harus ditafsirkan berdasarkan prinsip-prinsip yang tercantum dalam CISG dan kalau CISG belum menentukan, berdasarkan kaaidah-kaidah hukum : perdata internasional. Disamping itu, CISG menerima kebiasaan dagang serta kebiasaan antara para pihak sebagai dasar penafsiran ketentuan kontrak. Seperti halnya dalam hukum kontrak Indonesia, itikad baik dijadikan prinsip utama dalam penafsiran utama dalam penafsiran ketentuan dan pelaksanaan kontrak.

Berdasarkan hal-hal tersebut diatas maka hendaknya setiap bentuk kontrak perdagangan internasional dengan menggunakan *digital signature* selain didasarkan pada peraturan yang mengatur secara spesifik mengatur tentang *digital signature* juga didasarkan pada UNCISG karena CISG banyak dipakai oleh negara-negara di dunia.

3. Saat terbentuknya kontrak, Ini menyangkut kapan terjadinya kesepakatan terutama apabila kesepakatan ini terjadi tanpa kehadiran para peserta/pihak. Transaksi di internet kita analogikan sebagai transaksi yang dialukan tanpa kehadiran para pelaku di satu tempat (*betwen absent person*). CISG memberikan kepastian di dunia perdagangan internasional mengenai saat terjadinya suatu kontrak. kepastian ini akan memberikan dalam e-

*commerce* tanpa adanya kepastian ini, pertukaran antara suatu *digital signature* akan sulit menimbulkan hak dan kewajiban yang diakui oleh hukum kontrak. *E-mail* meskipun sifatnya menghubungkan para pihak dengan hampir seketika tetapi tetap saja terjadi kelambatan(*delay*) dalam masalah transmisinya. Juga harus dipertimbangkan adanya sistem yang tidak bekerja secara sempurna sehingga suatu *offer/acceptance* tidak dapat diterima secara seketika. Kontrak jual-beli dianggap sudah ada setelah adanya kesepakatan yang datang dari kedua belah pihak (lihat di atas cara melakukan *offer*).

*Digital signature* merupakan salah satu isu spesifik dalam *E-Commerce*. *Digital signature* ini pada prinsipnya berkenaan dengan jaminan untuk "message integrity" yang menjamin bahwa si pengirim pesan (*sender*) itu benar-benar orang yang berhak dan bertanggung jawab untuk itu (*the sender is the person whom they purport to be*). Hal ini berbeda dengan "real signature" yang berfungsi sebagai pengakuan dan penerimaan atas isi pesan/dokumen, persoalan hukum yang muncul seputar ini antara lain berkenaan dengan fungsi dan kekuatan hukum *digital signature*. Di Amerika saat ini telah ditetapkan satu undang-undang yang secara formal mengakui keabsahan *digital signature*.<sup>4</sup>

Maksud dari menandatangani secara digital adalah memberikan suatu ciri khas terhadap suatu pesan. *Message digest* adalah suatu besaran (*value*) yang berasal dari suatu data/pesan yang memiliki sifat yang unik yang menandai bahwa pesan tersebut mempunyai suatu besaran tertentu. *Messages digest* diciptakan

---

<sup>4</sup> Richardus Eko Indrajit, *Manajemen Sistem Informasi dan teknologi Informasi*, PT. Elex Media komputindo, 2000. Hlm.66.

dengan melakukan enkripsi terhadap suatu data dengan menggunakan menggunakan kriptografi satu arah (*one way cryptology*), yaitu suatu teknik kriptografi yang terhadapnya tidak dapat dilakukan proses pembalikan (*reversed*). Pada saat message digests dienkripsi dengan menggunakan kunci privat dari pengirim dan "ditambahkan" kepada data/pesan yang asli maka hasil yang didapat adalah *digital signature* dari pesan tersebut.

Penerima dari *digital signature* akan dapat mempercayai bahwa data/pesan benar berasal pengirim. Dan karena apabila terdapat perubahan suatu data/pesan akan menyebabkan akan merubah message digests dengan suatu cara yang tidak dapat diprediksi (*in unpredictable way*) maka penerima akan merasa yakin bahwa data/pesan tersebut tidak pernah diubah setelah *message digest* diciptakan.

Sebelum kedua belah pihak (pengirim/penerima) hendak melakukan komunikasi diantaranya dengan menggunakan kriptografi kunci publik, masing-masing pihak harus merasa yakin akan keberadaan mereka. Mereka kemudian akan melakukan otentifikasi terhadap keberadaan masing-masing pihak. Agar mereka dapat melakukan otentifikasi terhadap keberadaan mereka masing-masing maka mereka menunjuk pihak ketiga yang akan memberikan otentifikasi terhadap kunci publik mereka.

Pihak ketiga ini kita kenal sebagai *Certification Authority*. *Certification authority* ini kemudian akan memberikan suatu sertifikat (*certificate*) yang berisi identitas dari pengguna (misalnya Alice), sertifikat ini ditandatangani secara

digital oleh *Certification authority* tersebut. Isi dari sertifikat tersebut selain identitas ia juga berisi kunci publik dari pemiliknya.<sup>5</sup>

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

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 tersebut tidak mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang. Jaminan authenticity ini dapat dilihat dari adanya hash function dalam sistem digital signature, dimana penerima data (recipient) dapat melakukan perbandingan 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.

---

<sup>5</sup> Badruzaman, Mariam Darus, *E-Commerce Tinjauan dari Hukum Kontrak Indonesia*, Jurnal Hukum Bisnis. 2000. Hlm. 102.

Penggunaan *digital signature* maasih belum lazim digunakan, hal ini dikarenakan kurangnya akses masyarakat terhadap tata cara/operasional *digital signature* dan berbagai informasinya. Selain itu *digital signature* dinilai oleh para pelaku bisnis masih memiliki kelemahan pada tahap pembuktian, sehingga perlu dicari ketetapan untuk menjamin keabsahannya. Di Indonesia penggunaan *digital signature* masih belum umum digunakan. *Digital signature* masih dikaji secara mendalam dari sistem operasional hingga kemungkinan-kemungkinan distorsi yang bisa menghambat proses perdagangan.

## **B. Rumusan Masalah**

Berdasarkan uraian diatas dapat dirumuskan permasalahan:

1. Bagaimanakah opsional penggunaan *Digital Signature* dalam transaksi bisnis dengan sistem *e-commerce*?
2. Bagaimanakah kekuatan pembuktian *digital signature* dalam hukum acara di Indonesia?

## **C. Tujuan Penelitian**

Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Mengetahui sistem operasional *digital signature* dalam *e-commerce*
2. Mengetahui pembuktian dan aspek hukum yang mengatur *digital signature*

#### D. Tinjauan Pustaka

Pembuktian menurut Pitlo adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya. Subekti berpendapat bahwa yang dimaksud dengan membuktikan adalah meyakinkan hakim tentang kebenaran dalil atau dalil yang dikemukakan dalam suatu persengketaan. Sementara menurut ketentuan pasal 163 HIR (283 RBG) menyatakan setiap orang yang mendalilkan bahwa ia mempunyai suatu hak, atau guna menegukan haknya sendiri maupun membantah hak orang lain, menunjuk pada suatu peristiwa diwajibkan membuktikan adanya hak atau peristiwa tersebut. Dari sini ada dua aspek yang perlu diperhatikan dalam pembuktian yakni menyangkut dalil peristiwa dan adanya hak.

Proses pembuktian baru terjadi apabila ada sengketa di antara para pihak. Sengketa itu sendiri biasanya penyelesaiannya ditentukan oleh salah satu klausula dalam perjanjian. Umumnya penyelesaian itu dapat melalui lembaga litigasi atau non-litigasi. Khusus untuk pembahasan pembuktian ini diarahkan pada pola penyelesaian di lembaga peradilan.

Dalam konteks hukum Indonesia mengenai pembuktian mengacu pada hukum acara perdata. Dasar beracara dalam perkara perdata pengaturannya ditentukan dalam HIR (*Herzein Inlands Reglements*) atau RIB (Reglemen Indonesia yang diperbaharui).<sup>6</sup>

Dalam ensiklopedi wikipedia disebutkan bahwa *e-commerce* adalah sebagai berikut:

---

<sup>6</sup> Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. Hlm.17.

*Electronic commerce, e-commerce or ecommerce consists primarily of the distributing, buying, selling, marketing, and servicing of products or services over electronic systems such as the Internet and other computer networks. The information technology industry might see it as an electronic business application aimed at commercial transactions. It can involve electronic funds transfer, supply chain management, e-marketing, online marketing, online transaction processing, electronic data interchange, automated inventory management systems, and automated data-collection systems. It typically uses electronic communications technology such as the Internet, extranets, e-mail, Ebooks, databases, and mobile phones.*<sup>7</sup>

*"E-commerce is dynamics set of technologies, applications, and business process that link enterprises, consumers, and communities through electronic transactions and the electronic exchange of goods, service, and information".*<sup>8</sup>

Menurut Danan Mursito *Cyber Law* adalah aspek hukum yang istilahnya berasal dari *Cyberspace Law*, yang ruang lingkungnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai "online" dan memasuki dunia *cyber* atau maya. Pada negara yang telah maju dalam penggunaan internet sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju. Sebagai kiblat dari perkembangan aspek hukum ini, Amerika Serikat merupakan negara yang telah memiliki banyak perangkat hukum yang mengatur dan menentukan perkembangan *Cyber Law*.

Untuk dapat memahami sejauh mana perkembangan *Cyber Law* di Indonesia maka kita akan membahas secara ringkas tentang landasan fundamental yang ada didalam aspek yuridis yang mengatur lalu lintas internet sebagai sebuah

---

<sup>7</sup> <http://en.wikipedia.org/wiki/E-commerce>

<sup>8</sup> David Baum, "Business Link", *Oracle Magazine*, No. 3, Vol. XIII, May/June, 1999, Hlm. 36-44

rezim hukum khusus, dimana terdapat komponen utama yang meliputi persoalan yang ada dalam dunia maya tersebut, yaitu<sup>9</sup> :

1. Pertama, tentang yurisdiksi hukum dan aspek-aspek terkait; komponen ini menganalisa dan menentukan keberlakuan hukum yang berlaku dan diterapkan di dalam dunia maya itu;
2. Kedua, tentang landasan penggunaan internet sebagai sarana untuk melakukan kebebasan berpendapat yang berhubungan dengan tanggung jawab pihak yang menyampaikan, aspek *accountability*, tanggung jawab dalam memberikan jasa online dan penyedia jasa internet (*internet provider*), serta tanggung jawab hukum bagi penyedia jasa pendidikan melalui jaringan internet;
3. Ketiga, tentang aspek hak milik intelektual dimana adanya aspek tentang patent, merek dagang rahasia yang diterapkan serta berlaku di dalam dunia cyber;
4. Keempat, tentang aspek kerahasiaan yang dijamin oleh ketentuan hukum yang berlaku di masing-masing yurisdiksi negara asal dari pihak yang mempergunakan atau memanfaatkan dunia maya sebagai bagian dari sistem atau mekanisme jasa yang mereka lakukan;
5. Kelima, tentang aspek hukum yang menjamin keamanan dari setiap pengguna internet;

---

<sup>9</sup> Danan Mursito, Raya Reinhardt Sirait, Sukma Wardhana, *Pendekatan Hukum Untuk Keamanan Dunia Cyber Serta Urgensi Cyber Law Bagi Indonesia*, Program Studi Teknologi Informasi Program Magister Fakultas Ilmu Komputer, Universitas Indonesia, 2005.

6. Keenam, tentang ketentuan hukum yang memformulasikan aspek kepemilikan dalam internet sebagai bagian dari nilai investasi yang dapat dihitung sesuai dengan prinsip-prinsip keuangan atau akuntansi;
7. Ketujuh, tentang aspek hukum yang memberikan legalisasi atas internet sebagai bagian dari perdagangan atau bisnis usaha. Berdasarkan faktor-faktor tersebut di atas maka kita akan dapat melakukan penilaian untuk menjustifikasi sejauh mana perkembangan dari hukum yang mengatur sistem dan mekanisme internet di Indonesia.

Perkembangan internet di Indonesia mengalami percepatan yang sangat tinggi serta memiliki jumlah pelanggan atau pihak pengguna jaringan internet yang terus meningkat sejak paruh tahun 90'an. Salah satu indikator untuk melihat bagaimana aplikasi hukum tentang internet diperlukan di Indonesia adalah dengan melihat banyaknya perusahaan yang menjadi provider untuk pengguna jasa internet di Indonesia. Perusahaan-perusahaan yang memberikan jasa provider di Indonesia sadar atau tidak merupakan pihak yang berperan sangat penting dalam memajukan perkembangan *cyber law* di Indonesia dimana fungsi-fungsi yang mereka lakukan seperti :

1. Perjanjian aplikasi rekening pelanggan internet;
2. Perjanjian pembuatan desain home page komersial;
3. Perjanjian reseller penempatan data-data di internet server;
4. Penawaran-penawaran penjualan produk-produk komersial melalui internet; Pemberian informasi yang di update setiap hari oleh home page komersial;

5. Pemberian pendapat atau *polling online* melalui internet. Merupakan faktor dan tindakan yang dapat digolongkan sebagai tindakan yang berhubungan dengan aplikasi hukum tentang cyber di Indonesia. Oleh sebab itu ada baiknya didalam perkembangan selanjutnya agar setiap pemberi jasa atau pengguna internet dapat terjamin maka hukum tentang internet perlu dikembangkan serta dikaji sebagai sebuah hukum yang memiliki disiplin tersendiri di Indonesia.

#### **E. Metode Penelitian**

Metode dalam penelitian ini bersifat *juridis normatif*, yaitu mendasarkan pada peraturan perundang-undangan yang berlaku baik bersifat ketentuan nasional maupun internasional serta ketentuan-ketentuan lain yang tidak mengikat.

Sumber data yang dipergunakan dalam penelitian inilah adalah data sekunder, yaitu data yang diperoleh dari sumber secara tidak langsung yang berbentuk literatur dan dokumen hukum serta beberapa hasil penelitian-penelitian ilmiah. Sumber data tersebut terdiri dari:

1. **Bahan hukum primer**, yaitu bahan hukum yang mengikat (*legally and binding*), yang berhubungan dengan pokok masalah yang diteliti, seperti:
  - a) Kitab Undang-Undang Hukum Perdata
  - b) HIR
  - c) RBG
  - d) *UNCITRAL model law on Electronic Commerce*
  - e) Undang-undang No.8 Tahun 1997 tentang Dokumen Perusahaan

2. **Bahan hukum sekunder**, yaitu bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, seperti hasil-hasil penelitian sebelumnya dan artikel-artikel yang menyangkut dengan pokok masalah serta beberapa literatur.
3. **Bahan hukum tersier**, yaitu bahan hukum yang memberikan penjelasan atas bahan hukum primer dan sekunder, seperti kamus hukum dan ensklopedia.

Pengumpulan data dilakukan dengan studi pustaka melalui konsep-konsep, teori, pendapat ataupun doktrin baru yang berhubungan erat dengan masalah yang diteliti seperti peraturan perundang-undangan dan karya-karya ilmiah yang berhubungan. Disamping studi pustaka juga dilakukan pengumpulan fakta yang terjadi misalkan melalui surat kabar, tabloid, majalah dan media informasi lainnya.

Teknik analisa data yang digunakan dalam penelitian ini adalah analisa kualitatif dengan menyusun data secara sistematis guna menemukan kejelasan masalah yang akan diteliti. Menurut Maria Soemardjono data yang diperoleh dari penelitian atau studi pustaka dan dokumen dianalisis dengan menggunakan metode kualitatif, sehingga pendekatan yang digunakan dalam analisis bersifat *abstrak-teoritis*<sup>10</sup>. Secara umum analisa data ini dengan cara:

1. Penelitian Kepustakaan. Dari hasil studi kepustakaan akan dianalisis secara sistematis sehingga diperoleh gambaran yang menyeluruh mengenai asas-asas

---

<sup>10</sup> Maria Sumardjono SW, *Pedoman Pembuatan Usulan Penelitian*, Gramedia Pustaka Utama, Jakarta 1997. hlm. 40

hukum, kaidah-kaidah hukum dan pengertian hukum yang melingkupi persoalan perlindungan hukum nasabah penyimpan pada bank dengan berlakunya penjaminan dana nasabah melalui Lembaga Penjamin Simpanan dan persoalan yang muncul dengan berlakunya undang-undang Lembaga Penjamin Simpanan, bagi nasabah penyimpan pada bank.

2. Penelitian Lapangan. Data yang diperoleh dari penelitian ini dianalisis secara kualitatif, yaitu dengan memperhatikan faktor-faktor yang ada dalam praktek untuk melengkapi uraian yang diperoleh dari studi kepustakaan. Penelitian ini dilakukan terhadap responden atau narasumber dengan cara, baik melalui observasi maupun wawancara. Pemilihan instrument penelitian ini, tergantung dari berapa jumlah responden yang ada.

Metode pendekatan yang digunakan dalam penelitian ini adalah pendekatan normatif, yaitu metode pendekatan yang dipakai untuk menganalisa data kualitatif yang diperoleh berdasarkan peraturan perundang-undangan yang berlaku, sehingga diperoleh kesimpulan yang mengandung kebenaran obyektif.<sup>11</sup>

#### **F. Sistematika Penulisan**

Sistematika penulisan tesis ini terdiri dari 4 (empat) bab, pada pendahuluan merupakan Bab I yang berisikan latar belakang masalah, rumusan masalah, tujuan penelitian dan kerangka teori yang menjadi tolak ukur dalam pembahasan lebih lanjut serta metode penelitian yang dipakai dalam penelitian dan penulisa tesis ini.

---

<sup>11</sup> Soerjono Soekanto, *Pengantar Penelitian Hukum*, UI-Press, Jakarta 1986. hlm. 29

Bab II memaparkan secara umum tentang batasan *e-commerce*, sistem keamanan *e-commerce*, definisi kriptografi dan penggunaan kriptografi.

Bab III merupakan pembahasan atas rumusan masalah berdasarkan hasil penelitian. Pemaparan tentang operasional *digital signature*, mengenai pembuktian *digital signature*, pembuktian dalam peradilan Indonesia, pembuktian di luar badan peradilan selain *alternative dispute resolution*, dan aspek perlindungan konsumen

Bab IV merupakan bagian penutup dalam penulisan tesis ini yang memuat bagian kesimpulan dan saran.

## BAB II

### TRANSAKSI BISNIS DENGAN *E-COMMERCE* DAN SISTEM PENGAMANANNYA

Semakin konvergennya perkembangan Teknologi Informasi dan Telekomunikasi dewasa ini, telah mengakibatkan semakin beragamnya pula aneka jasa-jasa (*features*) fasilitas telekomunikasi yang ada, serta semakin canggihnya produk-produk teknologi informasi yang mampu mengintegrasikan semua media informasi. Ditengah globalisasi komunikasi yang semakin terpadu (*global communication network*) dengan semakin populernya Internet seakan telah membuat dunia semakin menciut (*shrinking the world*) dan semakin memudahkan batas-batas negara berikut kedaulatan dan tatananan masyarakatnya. Ironisnya, dinamika masyarakat Indonesia yang masih baru tumbuh dan berkembang sebagai masyarakat industri dan masyarakat Informasi, seolah masih tampak prematur untuk mengiringi perkembangan teknologi tersebut.

Perkembangan internet di Indonesia mengalami percepatan yang sangat tinggi serta memiliki jumlah pelanggan atau pihak pengguna jaringan internet yang terus meningkat sejak paruh tahun 90'an. Salah satu indikator untuk melihat bagaimana aplikasi hukum tentang internet diperlukan di Indonesia adalah dengan melihat banyaknya perusahaan yang menjadi provider untuk pengguna jasa internet di Indonesia. Perusahaan-perusahaan yang memberikan jasa provider di Indonesia sadar atau tidak merupakan pihak yang berperanan sangat penting

dalam memajukan perkembangan *cyber law* di Indonesia dimana fungsi-fungsi yang mereka lakukan seperti :

1. Perjanjian aplikasi rekening pelanggan internet;
2. Perjanjian pembuatan desain *home page* komersial;
3. Perjanjian reseller penempatan data-data di internet server;
4. Penawaran-penawaran penjualan produk-produk komersial melalui internet;
5. Pemberian informasi yang di update setiap hari oleh home page komersial;
6. Pemberian pendapat atau *polling online* melalui internet.

Merupakan faktor dan tindakan yang dapat digolongkan sebagai tindakan yang berhubungan dengan aplikasi hukum tentang cyber di Indonesia. Oleh sebab itu ada baiknya didalam perkembangan selanjutnya agar setiap pemberi jasa atau pengguna internet dapat terjamin maka hukum tentang internet perlu dikembangkan serta dikaji sebagai sebuah hukum yang memiliki disiplin tersendiri di Indonesia.

Pola dinamika masyarakat Indonesia seakan masih bergerak tak beraturan ditengah keinginan untuk mereformasi semua bidang kehidupannya ketimbang suatu pemikiran yang handal untuk merumuskan suatu kebijakan ataupun pengaturan yang tepat untuk itu. Meskipun masyarakat telah banyak menggunakan produk-produk teknologi informasi dan jasa telekomunikasi dalam kehidupannya, namun bangsa Indonesia secara garis besar masih meraba-raba dalam mencari suatu kebijakan publik dalam membangun suatu infrastruktur yang

handal (*National Information Infrastructure*) dalam menghadapi infrastruktur informasi global (*Global Information Infrastructure*).<sup>12</sup>

Komputer sebagai alat bantu manusia dengan didukung perkembangan teknologi informasi telah membantu akses ke dalam jaringan publik (*public network*) dalam melakukan pemindahan data dan informasi. Dengan kemampuan komputer dan akses yang semakin berkembang maka transaksi perniagaan pun dilakukan di dalam jaringan komunikasi tersebut.

Jaringan publik mempunyai keunggulan dibandingkan dengan jaringan privat dengan adanya efisiensi biaya dan waktu. Sesuai dengan *sifat jaringan publik yang mudah untuk diakses oleh setiap orang* menjadikan hal ini sebagai *kelemahan* bagi jaringan itu.

#### **A. Pengertian *E-commerce***

*Electronic Commerce* (Perniagaan Elektronik), sebagai bagian dari *Electronic Business* (bisnis yang dilakukan dengan menggunakan *electronic transmission*, oleh para ahli dan pelaku bisnis dicoba dirumuskan definisinya dari terminologi *E-Commerce* (Perniagaan Elektronik). Secara umum *e-commerce* dapat didefinisikan sebagai segala bentuk transaksi perdagangan/perniagaan barang atau jasa (*trade of goods and service*) dengan menggunakan media elektronik. Jelas, selain dari yang telah disebutkan di atas, bahwa kegiatan perniagaan tersebut merupakan bagian dari kegiatan bisnis.

---

<sup>12</sup> Badruzaman, Mariam Darus, 2000, *E-Commerce Tinjauan dari Hukum Kontrak Indonesia*, Jurnal Hukum Bisnis. Hlm. 76.

*Electronic Commerce* atau yang disingkat dengan *E-Commerce* adalah kegiatan-kegiatan bisnis yang menyangkut konsumen (*consumers*), manufaktur (*manufactures*), *services providers* dan pedagang perantara (*intermediateries*) dengan menggunakan jaringan-jaringan komputer (*computer network*) yaitu internet. Penggunaan sarana internet merupakan suatu kemajuanteknologi yang dapat dikatakan menunjang secara keseluruhan spektrum kegiatan komersial.<sup>13</sup>

Hal ini disebabkan internet merupakan jaringan komputerisasi yang sifatnya sangat global, yakni dapat diakses ke seluruh dunia pada waktu yang tidak terbatas atau dengan kata lain on-line 24 jam setiap hari dalam 7 hari seminggu. segala informasi dapat diakses kapan pun, di manapun dan saat apapun. Sehingga dengan kecanggihn jaringan komputer yang dinamakan internet ini dikreasikan oleh para usahawn dan provider dari internet untuk memanfaatkan lahan ini untuk ajang komerial, yakni menarik keuntungan yang sebesar besarnya. walaupun hal ini bisa dikatakan suatu hal yang klise, akan tetapi masing-maing provider internet akan menyingkapi usaha yang dijalankannya dengan sangat kreatif yakni berbelanja atau melakukan transaksi di duni maya yang dikenal dengan berbelanja di internet. berbelanja didunia internet inilah yang disebut *E\_Commerce*.

Istilah *E-Commerce* yang di definisikan oleh Julian Ding adalah sebagai berikut :

*“Electronic Commerce or E-Commerce as it also known, is a commercial transaction between avendor snd purchaser or parties in similar contractual*

---

<sup>13</sup> Haris, Freddy, *Aspek Hukum Transaksi Secara Elektronik di Pasar Modal*, Jakarta.2000.Hlm. 7.

*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 wideweb). The transaction concluded regardless of national boundaries or local requirement".<sup>14</sup>*

Dalam pengertian ini yang dimaksud *E-Commerce* merupakan suatu transaksi komersil yang dilakukan antara penjual dan pembeli atau 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 media network (sistem tertutup). dan sistem the 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 form of electronic, has become a popular prefix for other terms associated with electronic transaction.*<sup>15</sup>

Di sini dapat dikatakan bahwa pengertian *e-commerce* yang dimaksud adalah pembelian dan penjualan barang dan jasa dengan menggunakan jasa

---

<sup>14</sup>*Ibid.* Hlm. 32.

<sup>15</sup>*Black's Law Dictionary Seventh Edition*

konsumen online di internet. Model transaksi seperti ini dikenal dengan istilah *electronic transaction*.

Berdasarkan pengertian yang diberikan ECEG – Australia, maka pengertian e-commerce meliputi transaksi perdagangan melalui media elektronik. Dalam arti kata tidak hanya media internet yang dimaksud, tetapi juga meliputi semua transaksi perdagangan melalui media elektronika lainnya, seperti; facsimile, telex, EDI dan telephone.<sup>16</sup>

Istilah E-Commerce baru memperoleh perhatian beberapa tahun belakang ini ditandai dengan banyaknya seminar-seminar yang diadakan oleh beberapa institusi di bidang teknologi serta beberapa pengamat yang terkait dengan industri *e-commerce* seperti pengamat elektronik, pengamat teknologi informasi, pengamat hukum yang dihadirkan dalam membahas permasalahan yang akan timbul serta menyasati persoalan yang akan timbul, akan tetapi belum juga ditemukan jalan keluarnya, yang menjadi pokok bahasan yang sangat menarik di kalangan pembisnis pada umumnya.

*E-Commerce* sebagai lahan pembisnis dan para pelaku usaha menjadi tren yang sangat menarik perhatian publik. Kaitanya dengan periklanan, yang juga digeluti sebagai ajang promosi bagi perusahaan yang bergerak di bidang *e-commerce*, ini sangat menarik untuk diamati. Penggunaan peralatan elektronik untuk melakukan transaksi komersial yang telah dirancang sedemikian rupa membuat para peminat melupakan atau mengacuhkan implikasi-implikasi yang akan ditimbulkannya.

---

<sup>16</sup>Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. Hlm. 13.

Media elektronik yang dibicarakan di dalam tulisan ini untuk sementara hanya difokuskan dalam hal penggunaan media internet, mengingat penggunaan media internet yang saat ini paling populer digunakan oleh banyak orang, selain merupakan hal yang bisa dikategorikan sebagai hal yang sedang 'booming'. Perlu digarisbawahi, dengan adanya perkembangan teknologi di masa mendatang, terbuka kemungkinan adanya penggunaan media jaringan lain selain internet dalam *e-commerce*. Jadi pemikiran kita jangan hanya terpaku pada penggunaan media internet belaka.

Penggunaan internet dipilih oleh kebanyakan orang sekarang ini karena kemudahan-kemudahan yang dimiliki oleh jaringan internet<sup>17</sup>:

1. Internet sebagai jaringan publik yang sangat besar (huge/widespread network), layaknya yang dimiliki suatu jaringan publik elektronik, yaitu murah, cepat dan kemudahan akses.
2. Menggunakan electronic data sebagai media penyampaian pesan/data sehingga dapat dilakukan pengiriman dan penerimaan informasi secara mudah dan ringkas, baik dalam bentuk data elektronik analog maupun digital.

Dari apa yang telah diuraikan di atas, dengan kata lain; 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. Telah dikemukakan di

---

<sup>17</sup> Purbo, Onno W., Wahyudi, A.A., *Mengenal E-Commerce*, PT Elex Media Komputindo, Jakarta, 2001. Hlm. 87.

bagian awal tulisan, bahwa koneksi ke dalam jaringan internet sebagai jaringan publik merupakan koneksi yang tidak aman. Hal ini menimbulkan konsekuensi bahwa *E-commerce* yang dilakukan dengan koneksi ke internet adalah merupakan bentuk transaksi beresiko tinggi yang dilakukan di media yang tidak aman.

Kelemahan yang dimiliki oleh internet sebagai jaringan publik yang tidak aman ini telah dapat diminimalisasi dengan adanya penerapan teknologi penyandian informasi (*Cryptography*). Electronic data transmission dalam *e-commerce* disekuritisasi dengan melakukan proses enkripsi (dengan rumus algoritma) sehingga menjadi *cipher/locked* data yang hanya bisa dibaca/dibuka dengan melakukan proses reversal yaitu proses dekripsi sebelumnya telah banyak diterapkan dengan adanya sistem sekuriti seperti SSL, Firewall, dan sebagainya.

Perlu diperhatikan bahwa, kelemahan hakiki dari *open network* yang telah dikemukakan tersebut semestinya dapat diantisipasi atau diminimalisasi dengan adanya sistem pengamanan jaringan yang juga menggunakan kriptografi terhadap data dengan menggunakan sistem pengamanan dengan *Digital Signature*.

## **B. Macam Transaksi Bisnis Dengan Sistem *E-Commerce***

Perkembangan dunia bisnis dewasa ini dalam perkembangan perdagangan tidak lagi membutuhkan pertemuan secara langsung antar pelaku bisnis. Kemajuan teknologi memungkinkan unyuk dilaksanakannya hubungan-hubungan bisnis melalui perangkat teknologi yang disebut dengan internet. Permintaan apapun penawarannya melalui perangkat lunak yang ada dalam melakukan kegiatan

usaha di dalam cyberworld tersebut menjadi daya tarik sendiri bagi pelaku bisnis sendiri yang kini mempunyai kecenderungan memerlukan informasi yang cepat dan tidak memakan waktu yang lama. Segmentasi atau ruang lingkup e-commerce itu meliputi 3 sisi, yakni *e-commerce* yang terdiri dari segmentasi bisnis ke bisnis (*business to business*), bisnis ke konsumen (*business to consumer*) serta konsumen ke konsumen (*consumer to consumer*).

#### 1. Bisnis ke bisnis (*business to business*)

Bisnis ke bisnis merupakan sistem komunikasi bisnis antar pelaku bisnis atau dengan kata lain transaksi secara elektronik antar perusahaan (dalam hal ini pelaku bisnis) yang dilakukan secara rutin dan dalam kapasitas atau volume produksi yang besar. Aktivitas *e-commerce* dalam ruang lingkup ini ditunjukkan untuk menunjang kegiatan para pelaku bisnis itu sendiri.

Pembisnis yang mengadakan perjanjian tentu saja adalah para pihak yang bergerak dalam bidang bisnis yang dalam hal ini mengikatkan dirinya dalam suatu perjanjian untuk melakukan usaha dengan pihak pembisnis lainnya. Pihak-pihak yang mengadakan perjanjian dalam hal ini adalah *Internet Service Provider* (ISP) dengan website atau keybase (ruang elektronik, ISP itu sendiri adalah pengusaha yang menawarkan akses kepada internet. Sedangkan internet merupakan suatu jalan bagi komputer-komputer untuk mengadakan komunikasi bukan merupakan tempat akan tetapi merupakan suatu jalan untuk dilalui.

Karakteristik yang umum akan segmentasi bisnis ke bisnis adalah antara lain:

- a. *Trading Partners* yang sudah saling mengetahui dan antara mereka sudah terjalin hubungan yang berlangsung cukup lama. Pertukaran informasi berlangsung antara mereka dan sudah sangat mengenal, maka pertukaran informasi dilakukan atas dasar kebutuhan dan kepercayaan.
- b. Pertukaran yang dilakukan secara berulang-ulang dan berkala format data yang telah disepakati. Jadi service yang digunakan antara kedua sistem tersebut sama dan menggunakan standar yang sama pula.
- c. Salah satu pelaku tidak harus menunggu partners mereka lainnya untuk mengirimkan data
- d. Model yang umum digunakan adalah peer to peer dimana procesing intelegence dapat didistribusikan di kedua pelaku bisnis.

## 2. Bisnis ke konsumen (*business to consumer*)

Bisnis ke konsumen dalam e-commerce merupakan suatu transaksi bisnis secara elektronik yang dilakukan pelaku usaha dan pihak konsumen untuk memenuhi suatu kebutuhan tertentu dan pada saat tertentu. Sebagai contoh internet mal.

Transaksi ini produk yang diperjual belikan mulai produk barang dan jasa baik dalam bentuk berwujud maupun dalam bentuk elektronik atau digital yang telah siap digunakan atau dikonsumsi. Perkembangan segmentasi e-commerce khususnya pada ruang lingkup bisnis ke konsumen membawa keuntungan, bukan saja pada pihak pelaku usaha, pihak konsumen pun mendapat keuntungan yang

sama. Walaupun demikian tetap saja kemungkinan-kemungkinan penyimpangan di dunia maya dapat terjadi.

Kkesempatan salah satu pihak untuk melakukan penyimpangan karena dunia e-commerce di dalam dunia maya ini termasuk ruang transaksi yang belum terjangkau oleh hukum positif di Indonesia.

Keuntungan bagi pihak pelaku usaha dengan segmentasi ini, para pelaku usaha memiliki suatu lahan baru yang mempunyai potensi yang sangat besar untuk mendapatkan pendapatan yang lebih besar, dibandingkan dengan metode pemasaran secara konvensional. Melebarkan jangkauan pemasaran sehingga pelaku usaha dapat di hubungi oleh pelanggan dari seluruh dunia, merupakan keuntungan yang didapat dengan waktu operasional pemasaran yang tidak terbatas, yakni dilakukan dengan 24 jam nonstop setiap hari dan 7 hari perminggu. Selain hari operasional, biaya operasional para pelaku usaha pun menjadi sangat hemat karena tidak diperlukan ruang pameran (*show room*), staff operasional dalam jumlah besar maupun ruangan ataupun gudang yang besar.<sup>18</sup>

Konsumen mempunyai keuntungan-keuntungan diantaranya pembeli tidak perlu meluangkan waktu khusus untuk berbelanja keluar rumah cukup dengan membuka situs e-commerce yang diinginkan kapan saja selama 24 jam nonstop setiap hari dengan pilihan yang sangat beragam sesuai dengan keinginan produk atau jasa sekaligus dapat membandingkan produk yang ditawarkan dengan produk yang ditawarkan di pasar tradisional. Dan yang paling penting adalah kemudahannya perlu waktu banyak untuk bisa berbelanja di internet, cukup

---

<sup>18</sup> Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. Hlm. 43.

mengikuti prasyarat-prasyarat yang telah ditetapkan oleh masing-masing situs yang menawarkan produk barang atau jasa.

Umumnya jenis perjanjian dalam bisnis ke konsumen merupakan perjanjian on-line yang telah berbentuk perjanjian dan ditawarkan kepada pihak umum dalam bentuk take it or leave contract. Serta ada pula perjanjian dalam bentuk shrinkwrap contract dan click wrap contract yang merupakan perjanjian yang menawarkan kepada konsumen penggunaan produk dengan syarat-syarat yang menyertai produk tersebut, umumnya terjadi dalam perjanjian penggunaan suatu software komputer. Seorang pembeli seolah-olah telah menyetujui syarat-syarat yang di ajukan dalam tidakannya untuk menahan atau menggunakan produk tersebut setelah diberikan kesempatan untuk membacanya atau menulaknya.

Karakteristik yang umum untuk segmentasi bisnis ke konsumen diantaranya adalah sebagai berikut<sup>19</sup> :

- a. terbuka untuk umum, dimana informasi disebarakan secara umum pula.
- b. Service yang diberikan bersifat umum sehingga mekanismenya dapat digunakan oleh banyak orang sebagai contoh karena sistem web telah umum di kalangan masyarakat maka sistem yang digunakan sistem web pula.
- c. Service yang diberikan adalah berdasarkan permintaan. Konsumen berinisiatif sedangkan produsen harus siap merespon terhadap inisiatif konsumen tersebut.

---

<sup>19</sup>Onno W.Purbo & Anng Arif Wahyudi, *Mengenal e-Commerce*, PE. Elex Media Komputindo, 2001. Hlm. 24.

- d. Sering dilakukan pendekatan client-server dimana konsumen dipihak client menggunakan sistem yang manual (berbasis web) dan penyedia barang atau jasa (business procedure) berada pada pihak server.

### 3. Konsumen ke konsumen (*consumer to consumer*)

Konsumen ke konsumen merupakan transaksi bisnis elektronik yang dilakukan antar konsumen untuk memenuhi suatu kebutuhan tertentu dan pada saat waktu tertentu pula, segmentasi konsume ke konsumen ini sifatnya lebih khusus karena transaksi dilakukan oleh konsumen ke konsumen yang memerlukan transaksi.

Internet telah dilakukan sebagai sarana tukar menukar informasi tentang produk baik mengenai harga, kualitas dan pelayanannya. Selain itu antar customer juga dapat membentuk komunitas pengguna/penggemar produk tersebut. Ketidakpuasan customer dalam mengonsumsi suatu produk dapat segera tersebar luas melalui komunitas-komunitas tersebut. Internet telah menjadikan customer memiliki posisi tawar yang tinggi terhadap perusahaan dengan demikian menuntut pelayanan perusahaan menjadi lebih baik.

### **C. Keabsahan Kontrak Bisnis Dengan Menggunakan *E-Commerce***

Penerapan KUH Perdata secara analogi terhadap pengaturan perjanjian *e-commerce* sangat terkait dengan ketentuan mengenai hukum perjanjian. Didalam KUH Perdata Pasal 1313 menyatakan bahwa:

“Suatu perjanjian atau persetujuan adalah suatu perbuatan dengan mana satu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih”.

Ketentuan ini dapat dikatakan merupakan hal yang pokok atau hal yang sangat terpenting, oleh karena setiap perjanjian atau persetujuan melibatkan paling sedikit dua orang untuk mengikatkan dirinya dalam suatu ikatan perjanjian atau kontrak. Sebagai impletasi umum atas suatu perjanjian secara e-commerce juga dapat dikategorikan sebagai suatu bentuk perjanjian, walaupun perjanjian yang dilakukan tidak seperti perjanjian biasa, melainkan secara digital.

Perjanjian e-commerce merupakan bentuk perjanjian yang sedikit berbeda dengan perjanjian pada umumnya, yakni perjanjian menggunakan sarana atau media internet. Dan pihak-pihak yang bertransaksi secara e-commerce tidak saling bertemu atau bahkan tidak saling mengenal, karena mereka bertransaksi dalam dunia maya atau virtual.

Perjanjian walaupun wujud, bentuk dan sifat perjanjian itu berbeda dalam hal penandaan atau pernyataan kehendak, akan tetapi esensi atau inti dari pada isi perjanjian adalah sama secara umum, tiap-tiap perjanjian *e-commerce* pun dilahirkan karena Undang-undang dan persetujuan (sebagaimana yang ditetapkan dalam pasal 1233 KUH Perdata).<sup>20</sup>

Hukum Perdata Indonesia belum mengatur mengenai ketentuan perjanjian dengan metode *e-commerce* secara khusus. Ketika penulis melakukan survei terhadap isi dari perjanjian yang ada di situs on-line shopping semuanya memiliki kriteria yang hampir sama.

Karena negara kita masih baru dan awam terhadap hukum perjanjian dengan metode *e-commerce*, maka penulis mengambil kesimpulan bahwa ketentuan yang ada masih mengikuti ketentuan yang berlaku secara umum.

---

<sup>20</sup> Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. Hlm 60.

Perjanjian yang ada di dalam pada esensinya adalah sama yakni komponen para pihak peklaku usaha dan konsumen yang melakukan transaksi sama dengan perdagangan pada umumnya, walaupun pada media yang berbeda. Perjanjian atau kontrak e-commerce juga mencantumkan hak dan kewajiban sebagai mana yang yang ditetapkan dan berlaku secara konvensional yakni disatu pihak memberikan sesuatu, untuk berbuat sesuatu atau tidak berbuat sesuatu. Ketentuan ini sesuai dengan ketentuan yang terdapat di dalam Pasal 1234 KUH Perdata.

Untuk menilai sahnya suatu perjanjian dalam perjanjian penulis harus melihat ketentuan Pasal 1320 KUH Perdata yang mengatur syarat sahnya perjanjian, yaitu<sup>21</sup>:

1. sepakat bagi mereka yang mengikatkan diri

Dalam perjanjian kesepakatan telah tercapai pada saat pesan yang berisi penerimaan (*acceptance*) dari suatu penawaran (*offer*) masuk kembali kedalam sistem atau jaringan komputer pengirim (*offeror*) setelah dikirim kembali oleh penerima (*offere*). Penawaran tersebut akan memperoleh akseptasi bila konsumen mengklik suatu ilustrasi yang bertuliskan "setuju".

2. kecakapan untuk membuat suatu perjanjian

konsumen telah berusia 18 tahun atau pernah melangsungkan perkawinan (Pasal 1330 KUH Perdata jo Pasal 47 UU No. 1 Tahun 1974, tidak dibawah Pengampunan<sup>22</sup> dan tidak dilarang oleh undang-undang untuk melakukan perbuatan hukum tertentu. Pada dasarnya setiap orang yang

---

<sup>21</sup> *Ibid.* Hlm. 112.

<sup>22</sup> Pasal 1330 jo Pasal 433 KUH Perdata

sudah dewasa pikirannya adaklah cakap menurut hukum. Dan dalam perjanjian biasanya pihak konsumen mengisi terlebih dahulu data diri, sehingga dapat diketahui konsumen cakap atau tidak untuk mengadakan suatu perjanjian.

3. Suatu hal tertentu

perjanjian telah ditentukan jenis barang atau objek yang ditawarkan yakni buku, vcd dan majalah. Di lain pihak konsumen juga memiliki kebebasan untuk memilih berbagai jenis barang yang ditawarkan dengan membuka berbagai web-site dari pihak produsen.

4. suatu sebab yang halal

karena telah adanya perjanjian yang dapat dibaca secara langsung oleh pihak konsumen, maka konsumen dapat mengetahui apakah isi dari perjanjian tidak menyimpang dari undang-undang, norma-norma kesusilaan dan ketertiban umum.

Bisnis dalam jual beli yang diterapkan dapat saja dilakukan dengan konsumen yang berbeda kewarganegaraan atau beda negara, dalam penjelasan ini dikemukakan tiga teori yang memungkinkan dijadikan landasan untuk menentukan *lex loci contractus*.

Di negara civil law bilamana kedua belah pihak dalam suatu perjanjian tidak saling bertemu muka, maka digunakan teori deklarasi (*theory of declaration*). Menurut teori ini, penerimaan oleh yang ditawarkan harus dinyatakan (*declare*). Surat pernyataan penerimaan penawaran harus sampai kepada pihak yang menawarkan dan penerimaan penawaran tersebut harus diketahui oleh pihak yang menawarkan.

Di lain pihak di negara-negara *common law* teori yang digunakan *mail box theory*, yaitu salah satu pihak yang mengirimkan surat yang berisi penerimaan atas penawaran yang diajukan oleh pihak lainnya. Dengan mengacu pada teori ini.

Dua teori ini sebenarnya baru dapat diimpletasikan apabila para pihak dalam transaksi pembayaran di internet menganut pada sistem hukum yang sama. Persualanya sekarang bagaimana apabila para pihak berada dalam sistem hukum yang berbeda. Untuk menjawab pertanyaan ini, sebenarnya dapat dipergunakan teori *the most characteristic connection*. Dalam teori ini kewajiban untuk melakukan suatu prestasi yang paling karakteristik tolok ukur penentuan hukum yang akan mengatur perjanjian itu.

Dalam setiap perjanjian dapat dilihat pihak mana yang melakukan prestasi yang paling karakteristik dan hukum dari pihak yang melakukan prestasi yang paling karakteristik ini hukum yang harus dipergunakan, karena hukum inilah yang terberat dan yang paling sewajarnya dipergunakan. Maka berdasarkan pada teori ini dikaitkan dengan transaksi internet dalam masalah perlindungan konsumen. Sebenarnya hukum dalam penyediaan transaksi internetlah yang akan dipergunakan. Kalau penyedia jasa transaksi pembayaran internet ada Indonesia, di mana sistem hukumnya menganut sistem *civil law*, maka aturan-aturan hukum perjanjian Indonesialah yang akan dipakai sebagaimana telah dijelaskan di atas. Tetapi apabila penyedia jasa transaksi itu adalah pihak asing menganut sistem *common law*, maka hukum perjanjian yang berdasarkan *common law* itu yang akan dipergunakan. Karena berada di Indonesia maka hukum Indonesialah yang dipergunakan.

Khusus untuk Ekonomi Masyarakat Eropa, mereka telah menunjukkan garis-garis petunjuk kepada para negara anggotanya guna menjamin terlaksananya transaksi internet dengan tertib dan guna menghilangkan keraguraguan dalam proses terciptanya penawaran dan penerimaan dalam masalah perjanjian melalui media elektronik. Dikenal sebagai sistem "3 Klik". Pertama, setelah calon pembeli melihat dilayar komputernya adanya penawaran dari calon penjual (klik pertama), maka calon pembeli memberikan penerimaan terhadap penawaran tersebut (klik kedua).<sup>23</sup>

Di samping adanya proses (klik) penawaran dan penerimaan, masih disyaratkan adanya peneguhan dan persetujuan dari calon penjual kepada calon pembeli perihal diterimanya penerimaan dari calon pembeli (klik ketiga). Dengan demikian, adanya penawaran dan penerimaan melalui media elektronik dapat dikukuhkan.

Sebagai perbandingan lain, untuk kedepannya mengenai pengaturan perjanjian elektronik, maka dapat dilihat pada ketentuan *Model Law on Electronic Commerce* yang sudah dikeluarkan oleh PBB. Pasal 15 *Model Law on Electronic Commerce* menyatakan:

- 1 Kecuali diatur secara lain oleh originator dan addressee, saat suatu data message dikirim (*dispatch*) adalah pada saat ia memasuki suatu sistem informasi di luar kontrol dari originator atau orang lain yang mengirimkan data tersebut untuk kepentingan originator.

---

<sup>23</sup>Mertokusumo, Sudikno, *Hukum Acara Perdata Indonesia*, edisi ke empat, PT Liberty Yogyakarta 1993.

2 Kecuali diatur secara lain antara originator dan addresse, waktu diterimanya suatu data message ditentukan sebagai berikut:

a. Kalau seorang *addresse* sudah menentukan suatu informasi sebagai tujuan dikirimnya data message, saat diterimanya adalah :

- 1) Pada saat data message tersebut memasuki sistem informasi tertentu (*designated system information*) yang dituju; atau
- 2) Apabila suatu data message dikirimkan ke suatu informasi yang bukanya sistem informasi yang tertentu (*designated system information*), maka waktunya adalah pada saat pesan tersebut diterima oleh addresse;

b. Apabila suatu data tidak mempunyai suatu sistem informasi tertentu (*designated system information*), maka saat diteriam adalah pada saat data message memasuki sistem informasi dari addresse.

Perjanjian dalam bisnis tidak menjelaskan perjanjian yang dibuatnya untuk pada hukum apa tapi karena dia bertempat di Indonesia, maka hukum Indonesialah yang akan depergunakan dalam transaksi yang dilakukan.

Berdasarkan asas pokok dalam perjanjian sebagaimana yang diatur dalam KUH Perdata Pasal 1338 ayat 1 bahwa “semua perjanjian dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya”, merupakan suatu analogi terhadap perjanjian yang berlaku dalam ini. Hal ini terkait dengan sistem terbuka yang berlaku bagi setiap pihak yang hendak melakukan perjanjian. Perjanjian dapat dilihat bahwa apapun yangb diatur dalm perjanjian bersifat bebas. Dari pihak penjual memiliki kebebasan yang sangat luas untuk menentukan isi dari perjanjian asalkan tidak bertentangan dengan norma-norma kesusilaan dan

ketertiban umum, maka perjanjian atau kontrak e-commerce dapat diakui kebenarannya dan dapat diterima secara hukum yang berlaku di Indonesia khususnya.

Ketentuan mengenai jual beli yang diatur di dalam Pasal 1457 KUH Perdata yang terkait dengan perjanjian, pada prinsipnya memiliki prinsip yang sama dengan perjanjian konvensional yang lainnya. Yakni suatu jual beli yang mana pihak yang satunya mengikatkan dirinya untuk menyerahkan suatu kebendaan dan pihak yang lain membayar harga yang telah diperjanjikan, merupakan ketentuan mengenai jual beli yang berlaku secara umum.<sup>24</sup>

Perjanjian dimana jual beli atas suatu barang merupakan hal-hal yang sering dilakukan, maka seperti halnya pelaksanaan perjanjian yang telah diuraikan di atas, dalam perjanjian jual beli harus ada asas dan syarat suatu perjanjian. Berdasarkan hal tersebut maka jual beli dianggap terjadi setelah para pihak mencapai kesepakatan tentang kebendaan tersebut dan harganya. Meskipun kebendaan belum diserahkan atau harganya belum dibayar.<sup>25</sup>

Jadi jual beli dianggap telah terjadi pada saat barang yang diperjual belikan tersebut telah disepakati mengenai harga serta barang yang ditawarkannya, yaitu pada saat konsumen mengklik ilustrasi yang bertuliskan “setuju”, meskipun barang tersebut belum diserahkan atau harganya belum dibayar.

Dalam sistem pembayaran terbagi dalam 3 bagian yaitu COD (cash on delivery) atau ditempat yang hanya untuk wilayah DKI Jakarta saja, Transfer Bank dan *Credit Card*.

---

<sup>24</sup> Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. Hlm. 126.

<sup>25</sup> Pasal 1458 KUH Perdata

Dalam sistem pembayaran COD dan Trasfer bank hal itu tidak menjadi permasalahan, sama dengan jual beli secara umum tetapi dalam sistem pembayaranyang menggunakan credit card yang perlu mendapat perhatian, mengenai keamanan pembayarannya agar konsumen tidak merasa takut atau khawatir terjadinya kejahatan kartu kredit.

Pembayaran dengan kartu kredit dalam transaksi setelah order transaksi selesai dan pembeli memilih pembayarandengan kartu kredit maka pembeli akan terhubung ke Bank BII selaku payment gateway, pengisian semua data mengenai kartu kredit dilakukan pada payment gateway tersebut. Tugas sanur hanya men-  
chek apakah ada transaksi dengan CC dan cross chek dengan BII apakah CC yang digunakan valid.

Untuk kerahasiaan kartu kredit pelanggan, sistem keamanan diserahkan pada Bank BII selaku payment gateway dan mereka menjamin keamanannya.

Dalam sistem pembayaran ini penulis berpendapat sistem pembayaran kartu kredit dalm jual beli yang menggunakan BII sebagai Payment gegeway menggunakan Secure Socket Layer (SSL) untuk mengamankan pembayaran kartu kredit itu dan Certification Authority yang digunakan BII adalah VeriSign yang dikenal sebagai CA yang aman.

Dalam pengamanan transaksi itu sanur selaku merchant yang menggunakan BII sebagai Payment Gaateway memakai SSL 128 bit dan VeriSign sebagai Certification Authority yang membungkus kunci publiknya kedalam sertifikat digital dan setting pada browser yang memeriksa secara otomatis sertifikat digital dari website penjual, program tokol SSL selain menggunakan kunci publik, juga

menggunakan kunci simetrik untuk membungkus data sesungguhnya (dalam hal ini kartu kredit).

Walaupun transaksi ini menggunakan secure socket layer (SSL), namun sanur tidak dapat mengetahui informasi kartu kredit cardholder, karena sudah diserahkan pada pihak ke tiga (Bank BII) yang dipercaya sebagai Payment Gateway (gerbang pembayaran), seolah-olah sebagai kasir atau pos virtual.

Jadi pengamanan yang dipergunakan dengan mengkombinasikan three party payment system dengan teknologi SLL. Sampai saat ini, jenis transaksi ini yang relatif paling aman dan praktis untuk diimpletasikan. Jadi skenario ini mirip sekali dengan sekenario SET, hanya saja cardholder tidak perlu memiliki certification authority (CA) dan tidak perlu medownload aplikasi wallet untuk melakukan pembayaran.

Dalam skenario ini, cardholder tetap memilih barang-barang yang dibelinya dari website penjual. Setelah kumpul semua, penjual membuat slip pembelian. Kemudian, penjual meneruskan slip pembelian dengan teknik enkripsi sederhana ke payment gateway yang bertindak sebagai kasir.pada saat masuk payment gateway inilah, dibuat saluran kononikasi aman SSL antar pwymment gateway dengan cardholder.cardholder akan memberikan informasi kartu kreditnya kepada payment gateway dalam 'slip pembayaran'. Paymentgateway lah yang kemudian akan memberitaukan kepada penjual apakah suatu transaksi sudah berhasil diotorisasi atau belum. Jadi penjual tidak pernah membaca informasi kartu kredit cardholder. Salah satu ciri skenario perdagangan ini yang tampak pada browser yang dipakai cardholder adalah URL yang dipergunakan oleh payment gateway (saat memasukan informasi kartu kredit) berbeda dengan URL website sanur.

Perintah melalui kartu kredit (credit card orders), nasabah yang menggunakan web dengan perintah pengisian informasi nasabah dan menunjukkan nomer kartu kredit mereka. SSL sebagai teknologi yang melindungi nomor kartu.

BII dalam pengamanaan yang dilakukannya menggunakan SSL 128-bit encryption, menurut pendapat Onno W. Purbo seorang pakar Informatika SSL 128-bit RC4 dibutuhkan triliun miliar tahun dengan 120 komputer jalan paralel untuk menembus keamanan ini. Onno menjelaskan waktu yang diperlukan untuk membobol informasi yang menggunakan RC4 yang dipakai di SSL tergantung pada jumlah bi kunci yang digunakan.<sup>26</sup>

Pembobolan kunci mungkin saja terjadi. Besar kecilnya kemungkinan ini ditentukan oleh panjangnya kunci. Semakin panjang kunci makin semakin sulit pula untuk membobolnya.

Data tersebut merupakan penghitung pada tahun 1995 dengan menggunakan hardware khusus untuk menjebol kunci simetris DES. Sedangkan kunci asimetris dal kolom yang sama menunjukkan panjang kunci asimetris yang memiliki kekuatan yang sama dengan kunci asimetrisnya. Jadi untuk membobol kunci asimetris 512-bit membutuhkan waktu komputasi yang kurang lebih sama untuk membobol kunci simetris sepanjang 64-bit. Dengan asumsi kemampuan komputer menjadi berlipat ganda setiap 18 bulan dengan harga sama, maka pada tahun 1999 estimasi tersebut akan mejadi:

Berdasar data di atas terlihat bahwa resiko pembobolan kunci-kunci kriptografis, semakin tinggi sejalan dengan perjalanan waktu. Selain diperlukan

---

<sup>26</sup> Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. Hlm. 60.

protokol-protokol transaksi yang aman dari pencurian dan pembobolan, lembaga asuransi diharapkan dapat mengantisipasi kerugian yang mungkin terjadi di kemudian hari (Arrito Mukti Wibowo dkk, 1999:35).

Titik rawan yang lain adalah munculnya teknologi komputer yang baru yang 'melanggar' Moore's Law, sehingga dengan teknologi komputer yang baru itu, kecepatan komputer meningkat berlipat-lipat secara signifikan. Akibatnya sertifikat digital yang seharusnya berlaku lebih lama, akan kadaluarsa lebih cepat karena dapat dibobol dengan mudah.

Untuk menilai keamanan dalam bertransaksi yang harus diperhatikan adalah teknologi yang selalu berkembang dari waktu ke waktu karenanya dalam sistem keamanan harus memperhatikan perkembangan teknologi ini dan selalu disesuaikan pada keadaan pada saat itu, dalam pengamannya BII juga menggunakan Firewall sebagai pagar yang mencegah akses ilegal ke jaringan perbankan, yang mengintari sistem. Dalam pengamannya BII menggunakan VeriSign sebagai Certification Authority yang merupakan Certification Authority yang dapat dipercaya dan [www.jatis.com](http://www.jatis.com) yang menyediakan jasa sistem internet yang menghubungkan sanur dan BII dalam transaksi yang menggunakan kartu kredit.

Penggunaan BII sebagai payment gateway dalam transaksi yang menggunakan kartu kredit, menimbulkan kewajiban bagi BII untuk menjaga kerahasiaan kartu kredit konsumen, hal ini dapat penulis golongan sebagai rahasia jabatan bank, dari hasil wawancara penulis dengan Ibu Siti Sundari S. Arie, sebagai Deputy Gubernur Bank Indonesia (BI) bagian pengawasan, mengatakan bahwa kewajiban bank untuk menjaga kartu kredit itu. Karena

sebagai lembaga keuangan, bank harus mendapat kepercayaan dari masyarakat dan kepercayaan itu akan lahir apa bila semua data konsumen pada bank dapat tersimpan secara tertutup, rapi dan dirahasiakan. Hal ini membawa konsekuensi kepada bank, yaitu bank memikul kewajiban untuk menjaga rahasia konsumen sanur, sebagai timbal balik dari kepercayaan yang diberikan konsumen kepada bank BII selaku lembaga keuangan yang menjadi gerbang pembayaran.

BII sebagai payment gateway berkewajiban untuk menjaga kerahasiaan data kartu kredit konsumen sanur, apabila BII tidak menjaga kerahasiaan ini maka BII dapat dituntut baik secara perdata maupun pidana.

Dalam kesempatan ini akan dipertegas hubungan hukum yang ada dengan menggunakan kartu kredit sebagai alat pembayaran. Pada penggunaan kartu kredit, secara serentak bekerja 3 perjanjian yang satu sama yang lain sama terpisah, yaitu:

- a. perjanjian antara penjual dan pemegang kartu
- b. perjanjian antara penjual dengan perusahaan penerbit kartu, yang berdasarkan perjanjian itu penjual yang bersangkutan setuju untuk menerima pembayaran yang menggunakan kartu itu.
- c. Perjanjian antara penerbit kartu dan pemegang kartu atau pemegang rekening, yang berdasarkan perjanjian itu pemegang kartu menyetujui untuk melunasi pembayaran yang telah dilakukan oleh penerbit kartu kepada penjual barang dan atau jasa berkenaan dengan penggunaan kartu oleh pemegang kartu yang bersangkutan.

Perjanjian pengadaan pembayaran dengan kartu kredit merupakan perjanjian bisnis ke bisnis (business to business contract).

#### D. Sistem Pengamanan Transaksi Dengan Sistem *E-Commerce*

Pada awalnya, tahun 1980-an *e-commerce* telah menggunakan satu sistem keamanan yang dikenal dengan *Electronic Data Interchange* (EDI) yang digunakan terutama pada sektor industri manufaktur dan farmasi. Sistem ini masih belum mendapat perhatian kalangan pebisnis, karena sifat saling percaya masih sangat dominan melingkupi perdagangan elektronik ini. Namun perkembangan yang cepat terhadap *e-commerce* ini, pada tahun 1990-an menyebabkan para pebisnis mulai memfokuskan diri pada sistem keamanan informasi dan segala hal yang berkaitan dengan pentingnya pengakuan sah terhadap sesuatu (*legal significance*),<sup>27</sup> termasuk *online contract* dan *digital signature*.

Untuk kontrak elektronik terkait dengan bentuk tertulis diatas kertas, pilihan hukum dan yuridiksi hukum atas terjadinya kontrak, istilah dan syarat-syarat, penegakan dalam kontrak, identitas para pihak dan kekuatan mengikat kontrak elektronik.<sup>28</sup>

*Secure Electronic Commerce* atau dalam bahasa Indonesia bisa diterjemahkan menjadi sistem keamanan *e-commerce*, menurut Warwick Ford dan Michael S. Baum:

---

<sup>27</sup>Warwick Ford dan Michael S. Baum, *Secure Electronic Commerce: Building The Infrastructure for Digital-Signature and-Encryption*, Prentice Hall PTR Upper Saddle River, New Jersey 07458, 1997, hlm. 7.

<sup>28</sup>Ridwan Khairandy, *Pembaharuan Hukum Kontrak Sebagai Antisipasi E-Commerce*, Jurnal Hukum Bisnis, Vol. 16 November 2001. Hlm. 302.

" *Secure electronic commerce is electronic commerce that uses security procedures and techniques commensurate with anticipated risk.*<sup>29</sup>

Dengan demikian dapat dikatakan bahwa sistem keamanan *e-commerce* adalah *e-commerce* yang menggunakan prosedur sistem keamanan dan teknik-teknik untuk menghadapi segala resiko yang terjadi. Dalam prakteknya, *secure e-commerce* dapat dikatakan menjamin keamanan informasi bisnis antara para pelaku bisnis yang tidak bertemu muka dan menggunakan media internet yang tidak aman.

Sistem keamanan informasi (*information security*) yang merupakan bagian terpenting dari sistem keamanan *e-commerce* (*secure e-commerce*), didasari oleh empat macam tujuan yang sangat mendasar, yaitu:<sup>30</sup>

##### 5. *Confidentiality*

Upaya untuk menjamin agar informasi yang dikirim tersebut tidak dapat dibuka atau tidak dapat diketahui oleh orang lain yang tidak berhak. Untuk data yang teramat penting, dibutuhkan sekali tingkat kerahasiaan yang tinggi, yang hanya bisa diakses oleh orang-orang tertentu saja.

##### 6. *Integrity*

Menjamin konsistensi data tetap utuh sesuai aslinya atau palsu, sehingga upaya orang-orang yang tidak bertanggung jawab untuk melakukan duplikasi dan perusakan data bisa dihindari.

---

<sup>29</sup> Warwick Ford and Michael S. Baum, *Op. Cit.* Hlm. 7-9.

<sup>30</sup>*Ibid*, hlm. 94.

### 7. *Avability*

Menjamin pengguna yang sah agar bisa mengakses informasi dan sumber miliknya sendiri. Jadi tujuannya adalah untuk memastikan bahwa orang-orang yang memang berhak tidak ditolak untuk mengakses informasi yang memang menjadi haknya.

### 8. *Ligitimate Use*

Menjamin kepastian bahwa sumber tidak digunakan/diakses oleh orang-orang yang tidak bertanggung jawab dan tidak berhak.

Keempat tujuan diatas dapat terlaksana dengan adanya beberapa sistem keamanan, diantaranya: Pertama; Keamanan komunikasi (*communication security*), yang merupakan perlindungan terhadap informasi ketika dikirim dari sebuah sistem ke sistem lain. Kedua; Keamanan komputer (*computer security*), yaitu bentuk perlindungan terhadap sistem informasi itu sendiri, seperti keamanan pada *software* manajemen *data base* komputer. Ketiga; Keamanan secara fisik (*physical security*), seperti pemngamanan oleh penjaga keamanan, pintu yang terkunci, swistem kontrol fisik lainnya, dan sebagainya. Keempat; Keamanan personal (*personnel security*), dimana sistem ini meliputi kepribadian orang-orang yang mengoperasikan atau memiliki hubungan langsung dengan sistem tersebut. Kelima; Keamanan administratif (*administrative security*), dengan mengadakan kontrol terhadap perangkat-perangkat lunak yang dipakai, memeriksa kembali kejadian-kejadian yang telah diperikasa sebelumnya dan sebagainya. Keenam; Keamanan media yang digunakan (*media security*), yaitu meliputi pengontrolan terhadap media penyimpanan yang ada dan menjamin

bahwa media penyimpanan yang mengandung informasi sensitif tersebut tidak mudah hilang begitu saja.

## BAB III

### PENGGUNAAN *DIGITAL SIGNATURE* DALAM TRANSAKSI BISNIS DENGAN *E-COMMERCE*

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

#### A. Penggunaan *Digital Signature* Dalam Transaksi Bisnis Dengan *E-Commerce*

Dalam *Digital signature* suatu data/pesan akan dienkripsi dengan menggunakan kunci simetris yang diciptakan secara acak (*randomly generated symmetric key*). Kunci ini kemudian akan dienkripsi dengan menggunakan kunci publik dari calon penerima pesan. Hasil dari enkripsi ini kemudian dikenal/disebut sebagai "*digital envelope*" yang kemudian akan dikirimkan bersama pesan/data yang telah dienkripsi. Setelah menerima *digital envelope* penerima kemudian akan

membuka/mendekripsi dengan menggunakan kunci kunci pribatnya. Hasil yang ia dapatkan dari dekripsi tersebut adalah sebuah kunci simetris yang dapat digunakannya untuk membuka data/pesan tersebut.

Kombinasi antara *digital signature* dengan *message digest* menyebabkan seorang pengguna dapat "menandatangani secara digital" (*digitally sign*) suatu data/pesan. Maksud dari menandatangani secara digital adalah memberikan suatu ciri khas terhadap suatu pesan. *Message digest* adalah suatu besaran (*value*) yang berasal dari suatu data/pesan yang memiliki sifat yang unik yang menandai bahwa pesan tersebut mempunyai suatu besaran tertentu. *Messages digest* diciptakan dengan melakukan enkripsi terhadap suatu data dengan menggunakan menggunakan kriptografi satu arah (*one way cryptography*), yaitu suatu tehnik kriptografi yang terhadapnya tidak dapat dilakukan proses pembalikan (*reversed*).<sup>31</sup> Pada saat message digests dienkripsi dengan menggunakan kunci privat dari pengirim dan "ditambahkan" kepada data/pesan yang asli maka hasil yang didapat adalah *digital signature* dari pesan tersebut.<sup>32</sup>

Penerima dari *digital signature* akan dapat mempercayai bahwa data/pesan benar berasal pengirim. Dan karena apabila terdapat perubahan suatu data/pesan akan menyebabkan akan merubah message digests dengan suatu cara yang tidak

---

<sup>31</sup>Arrianto Mukti Wibowo, *Tanda tangan digital & sertifikat digital: Apa itu? 1998* Artikel ini muncul pada Infokomputer edisi Internet Juni 1998. Hlm.21.

<sup>32</sup>Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005.Hlm. 64.

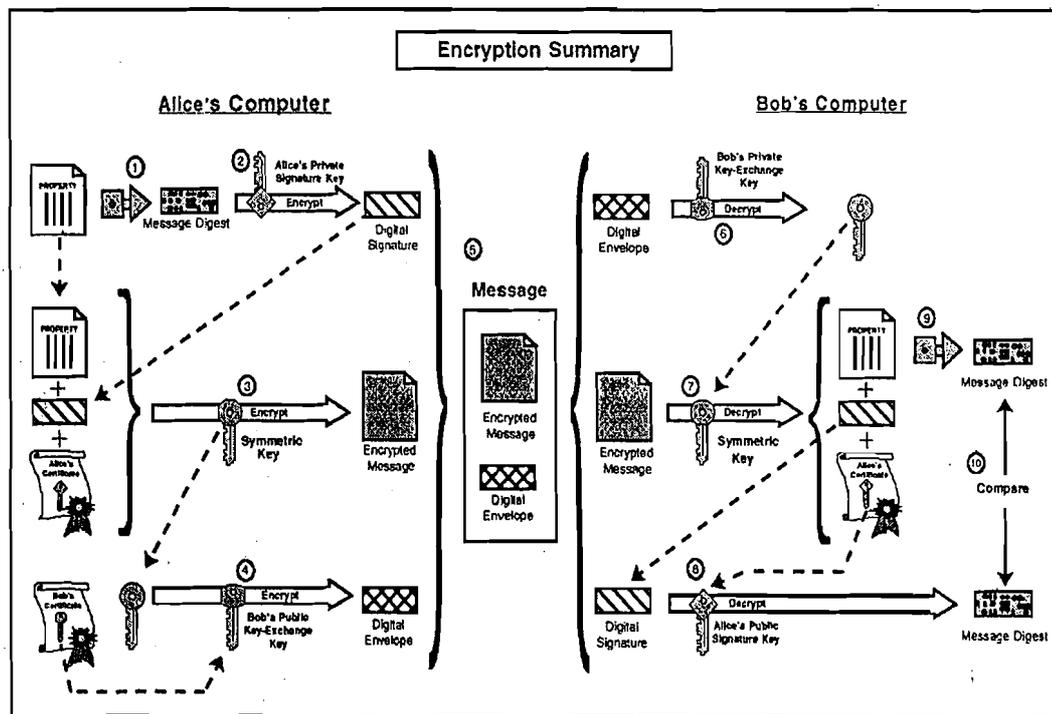
dapat diprediksi (*in unpredictable way*) maka penerima akan merasa yakin bahwa data/pesan tersebut tidak pernah diubah setelah *message digest* diciptakan.

Sebelum kedua belah pihak (pengirim/penerima) hendak melakukan komunikasi diantaranya dengan menggunakan kriptografi kunci publik, masing-masing pihak harus merasa yakin akan keberadaan mereka. Mereka kemudian akan melakukan otentifikasi terhadap keberadaan masing-masing pihak. Agar mereka dapat melakukan otentifikasi terhadap keberadaan mereka masing-masing maka mereka menunjuk pihak ketiga yang akan memberikan otentifikasi terhadap kunci publik mereka. Pihak ketiga ini kita kenal sebagai *Certification Authority*. *Certification authority* ini kemudian akan memberikan suatu sertifikat (*certificate*) yang berisi identitas dari pengguna (misalnya Alice), sertifikat ini ditandatangani secara digital oleh *Certification authority* tersebut. Isi dari sertifikat tersebut selain identitas ia juga berisi kunci publik dari pemiliknya.

Contoh dari penggunaan *digital signature* adalah sebagai berikut, Alice akan membuat *message digest* dari data/pesan yang hendak ia kirimkan. Kemudian *message digest* tersebut dienkripsi dengan menggunakan kunci privat yang ia punyai, hasil yang didapat adalah *digital signature* dari data tersebut. Ia kemudian mentransmisikan data dan *digital signature* itu kepada Bob. Bob pada saat menerima pesan itu akan melihat *message digest* dari pesan dan kemudian ia akan membandingkan hasilnya dengan hasil dari *digital signature*. Apabila hasil

yang didapat dari keduanya dalam sama maka Bob akan merasa yakin bahwa pesan yang telah ditandatangani oleh Alice dengan menggunakan kunci privatnya adalah tidak pernah berubah sejak dibuat.

Selanjutnya, diagram dibawah ini akan menunjukkan bagaimana suatu proses enkripsi berjalan apabila Alice ingin menandatangani suatu pesan dan mengirimkannya kepada Bob.



Gambar 3 : encryption summary

Gambar 3 menunjukkan proses kriptografi yang terjadi dalam digital signature, langkah-langkah dalam melakukan enkripsi ini adalah sebagai berikut:

1. Alice menjalankan (*runs*) data yang hendak ia kirimkan, melalui algoritma satu arah (*one way algorithm*) sehingga ia mendapat suatu nilai (*value*) yang unik dari data tersebut. Nilai ini disebut message digest. Nilai adalah semacam sidik jari bagi data tersebut dan akan digunakan dalam proses yang lebih lanjut untuk meneliti keutuhan (*integrity*) dari data tersebut.
2. Alice kemudian melakukan enkripsi terhadap *messages digest* tersebut dengan menggunakan kunci pribadinya sehingga ia akan mendapatkan *digital signature* dari data tersebut.
3. Kemudian, Alice membuat (*generates*) suatu kunci simetris secara acak (*random*) dan menggunakan kunci itu melakukan enkripsi terhadap data yang hendak ia kirimkan, tandatangan (*signature*) miliknya, dan salinan dari sertifikat digitalnya yang berisi kunci publiknya. Untuk mendekripsi data tersebut Bob membutuhkan salinan dari kunci simetris tersebut.
4. Alice harus memiliki terlebih dahulu sertifikat milik Bob, sertifikat ini berisi salinan (*copy*) dari kunci publik milik Bob. Untuk menjamin keamanan transmisi dari kunci simetris maka kunci tersebut dienkripsi dengan menggunakan kunci publik milik Bob. Kunci yang telah

dienkripsi yang dikenal sebagai amplop digital (*digital envelope*) akan dikirimkan bersama-sama dengan data yang telah dienkripsi.

5. Alice kemudian akan mengirimkan data (message) tersebut yang berisi data yang telah dienkripsi dengan kunci simetris, tandatangan dan sertifikat digital, serta kunci simetris yang telah dienkripsi dengan kunci asimetris (*digital envelope*).
6. Bob menerima pesan(messages) dari Alice tersebut dan kemudian mendekripsi amplop digital dengan kunci prifat yang dipunyainya, ia kemudian akan mendapatkan kunci asimetris
7. Bob kemudian menggunakan kunci simetris tersebut untuk mendekripsi data itu (property decryption), tandatangan Alice, dan sertifikat miliknya.
8. Ia kemudian mendekripsi *digital signature* milik Alice dengan menggunakan kunci publik milik Alice, yang didapat Bob dari sertifikat milik Alice. Dari dekripsi ini akan didapatkan *message digest* dari data tersebut.

9. Bob kemudian memproses (*run*) data itu dengan menggunakan algoritma satu arah yang sama yang digunakan Alice untuk message digest.

Akhirnya Bob akan membandingkan antara *message digest* yang didupatkannya dari proses dekripsi diatas dengan *message digest* yang didapatkan dari *digital signature* milik Alice. Kalau hasil yang didapat dari perbandingan itu adalah sama maka, Bob dapat merasa yakin bahwa data tersebut tidak pernah dirusak (*altered*) selama proses transmisi dan data itu ditandatangani dengan menggunakan kunci privat milik Alice.

Dengan memberikan *digital signature* pada data elektronik yang dikirimkan maka akan dapat ditunjukkan darimana data elektronis tersebut sesungguhnya berasal. Terjaminnya integritas pesan tersebut bisa terjadi karena keberadaan dari Digital Certificate. *Digital Certificate* diperoleh atas dasar aplikasi kepada Certification Authority oleh user/subscriber. *digital certificate* berisi informasi mengenai pengguna antara lain<sup>33</sup>:

- a. identitas
- b. kewenangan
- c. kedudukan hukum

---

<sup>33</sup> Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. Hlm. 21.

d. status dari user

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

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

*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 tersebut tidak

mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang. Jaminan authenticity ini dapat dilihat dari adanya hash function dalam sistem digital signature, dimana penerima data (recipient) dapat melakukan perbandingan 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.

*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 berbeda 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.

*Non repudiation* ini timbul dari keberadaan *digital signature* yang menggunakan enkripsi asimetris (*asymmetric encryption*). Enkripsi asimetris ini melibatkan keberadaan dari kunci privat dan kunci publik. Suatu pesan yang telah

dienkripsi dengan menggunakan kunci privat maka ia hanya dapat dibuka/dekripsi dengan menggunakan kunci publik dari pengirim. Jadi apabila terdapat suatu pesan yang telah dienkripsi oleh pengirim dengan menggunakan kunci privatnya maka ia tidak dapat menyangkal keberadaan pesan tersebut karena terbukti bahwa pesan tersebut dapat didekripsi dengan kunci publik pengirim. Keutuhan dari pesan tersebut dapat dilihat dari keberadaan hash function dari pesan tersebut, dengan catatan bahwa data yang telah di-sign akan dimasukkan kedalam *digital envelope*.

Pesan dalam bentuk data elektronik yang dikirimkan tersebut bersifat rahasia/confidential, sehingga tidak semua orang dapat mengetahui isi data elektronik yang telah di-sign 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 dari panjang kunci/*key* yang dipakai untuk melakukan enkripsi. Pada saat ini standar panjang kunci yang digunakan adalah sebesar 128 bit.<sup>34</sup>

Kriptografi merupakan seni dan ilmu yang mempelajari bagaimana membuat suatu pesan (data) yang dikirim pengirim (*originator*) dapat disampaikan kepada penerima (*addressee*) dengan aman. Kriptografi dapat juga diartikan sebagai suatu cabang dari matematika terapan mengenai perubahan bentuk pesan kedalam

---

<sup>34</sup>Dimitri Mahayana, *Menjempuk Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global*, PT. Remaja Rosdakarya, 1999. Hlm.98.

bentuk yang tidak dapat dipahami dan mengubahnya lagi ke bentuk semula.<sup>35</sup> Teknik ini digunakan untuk mengkonversi/mengubah data ke dalam bentuk kode-kode tertentu, dengan tujuan informasi yang disimpan maupun ditransmisikan melalui jaringan yang tidak aman (misalnya internet) tidak dapat dibaca oleh siapapun kecuali oleh orang-orang yang berhak.

Pada umumnya, kriptografi modern sebagai suatu teknik menyediakan beberapa fungsi dalam bidang keamanan informasi, yaitu:<sup>36</sup>

- a. Fungsi enkripsi (*encryption*), yang terdiri dari tiga metode enkripsi, yaitu konvensional (dengan menggunakan kunci simetris), menggunakan kunci publik dan gabungan keduanya.
- b. Tanda tangan digital (*digital signature*)
- c. Protokol (aturan) dalam pembentukan kunci.

Fungsi-fungsi tersebut digunakan untuk memenuhi kebutuhan umum terhadap suatu transaksi mengenai:

- a. Kerahasiaan (*confidentiality*)
- b. Keutuhan (*integrity*)
- c. Jaminan atas identitas dan keabsahan (*authenticity*)
- d. Transaksi dapat dijadikan bukti yang tidak bisa disangkal (*non-repudiation*)

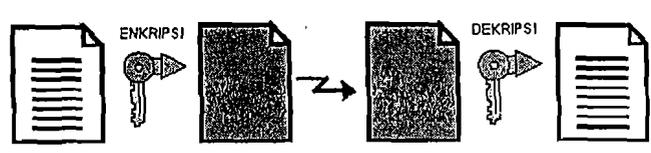
*Secret key cryptography* atau yang dikenal sebagai kriptografi simetris, menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi terhadap

---

<sup>35</sup> *Information Security Committee*, [www.abanet.org/scitech/ec/isc/dsg-tutorial.html](http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html).

<sup>36</sup> *Ibid.*

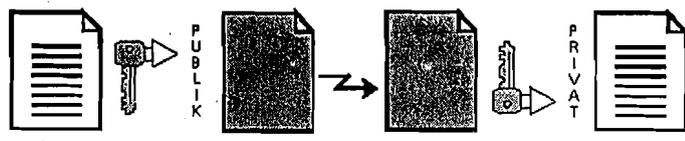
suatu pesan (message), disini pengirim dan penerima menggunakan kunci yang sama sehingga mereka harus menjaga kerahasiaan (*secret*) terhadap kunci tersebut. Salah satu algoritma yang terkenal dalam kriptografi simetris ini adalah *Data Encryption standard* (DES).



Gambar 1 : kriptografi simetris<sup>37</sup>

Public key *cryptology*, atau dikenal juga sebagai kriptografi simetris, menggunakan dua kunci (*key*) : satu kunci digunakan untuk melakukan enkripsi terhadap suatu pesan (*messages*) 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 didekripsi 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. Salah satu algoritma yang terbaik yang dikenal selama ini adalah RSA (dinamakan sesuai dengan nama penciptanya Rivest, Shamir, Adleman).



Gambar 2 : kriptografi dengan menggunakan kunci publik<sup>38</sup>

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 ditransmisikan dengan aman melalui jaringan yang relatif tidak aman (melalui internet).

---

<sup>38</sup> *Ibid.*

Penerima dari *digital signature* akan dapat mempercayai bahwa data/pesan benar berasal pengirim. Dan karena apabila terdapat perubahan suatu data/pesan akan menyebabkan akan merubah message digests dengan suatu cara yang tidak dapat diprediksi (*in unpredictable way*) maka penerima akan merasa yakin bahwa data/pesan tersebut tidak pernah diubah setelah *message digest* diciptakan.

Sebelum kedua belah pihak (pengirim/penerima) hendak melakukan komunikasi diantaranya dengan menggunakan kriptografi kunci publik, masing-masing pihak harus merasa yakin akan keberadaan mereka. Mereka kemudian akan melakukan otentifikasi terhadap keberadaan masing-masing pihak. Agar mereka dapat melakukan otentifikasi terhadap keberadaan mereka masing-masing maka mereka menunjuk pihak ketiga yang akan memberikan otentifikasi terhadap kunci publik mereka. Pihak ketiga ini kita kenal sebagai *Certification Authority*. *Certification authority* ini kemudian akan memberikan suatu sertifikat (*certificate*) yang berisi identitas dari pengguna (misalnya Alice), sertifikat ini ditandatangani secara digital oleh *Certification authority* tersebut. Isi dari sertifikat tersebut selain identitas ia juga berisi kunci publik dari pemiliknya.

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

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 tersebut tidak mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang. Jaminan authenticity ini dapat dilihat dari adanya hash function dalam sistem digital signature, dimana penerima data (recipient) dapat melakukan perbandingan 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.

Penggunaan *digital signature* yang diaplikasikan pada pesan/data elektronik yang dikirimkan dapat menjamin bahwa pesan/data elektronik tersebut tidak mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang. Jaminan authenticity ini dapat dilihat dari adanya hash function dalam sistem

digital signature, dimana penerima data (recipient) dapat melakukan perbandingan 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.<sup>39</sup>

*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 berbeda 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.

*Non repudiation* ini timbul dari keberadaan *digital signature* yang menggunakan enkripsi asimetris (*asymmetric encryption*). Enkripsi asimetris ini melibatkan keberadaan dari kunci pribadi dan kunci publik. Suatu pesan yang telah dienkripsi dengan menggunakan kunci pribadi maka ia hanya dapat dibuka/dekripsi

---

<sup>39</sup> Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. Hlm. 27.

dengan menggunakan kunci publik dari pengirim. Jadi apabila terdapat suatu pesan yang telah dienkripsi oleh pengirim dengan menggunakan kunci pribadinya maka ia tidak dapat menyangkal keberadaan pesan tersebut karena terbukti bahwa pesan tersebut dapat didekripsi dengan kunci publik pengirim. Keutuhan dari pesan tersebut dapat dilihat dari keberadaan hash function dari pesan tersebut, dengan catatan bahwa data yang telah di-sign akan dimasukkan kedalam *digital envelope*

Pesan dalam bentuk data elektronik yang dikirimkan tersebut bersifat rahasia/confidential, sehingga tidak semua orang dapat mengetahui isi data elektronik yang telah di-sign 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 dari panjang kunci/*key* yang dipakai untuk melakukan enkripsi. Pada saat ini standar panjang kunci yang digunakan adalah sebesar 128 bit.<sup>40</sup>

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

---

<sup>40</sup>Dimitri Mahayana, *Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global*, PT. Remaja Rosdakarya, 1999. Hlm.98.

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.

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.

## **B. Kekuatan Pembuktian *Digital Signature* Dalam Sistem Hukum Indonesia**

Pembuktian menurut Pitlo adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya. Subekti berpendapat bahwa yang dimaksud dengan membuktikan adalah meyakinkan hakim tentang kebenaran dalil atau dalil yang dikemukakan dalam suatu persengketaan. Sementara menurut ketentuan pasal 163 HIR (283 RBG) menyatakan setiap orang yang mendalilkan bahwa ia mempunyai suatu hak, atau

guna menegukan haknya sendiri maupun membantah hak orang lain, menunjuk pada suatu peristiwa diwajibkan membuktikan adanya hak atau peristiwa tersebut. Dari sini ada dua aspek yang perlu diperhatikan dalam pembuktian yakni menyangkut dalil peristiwa dan adanya hak.

Proses pembuktian baru terjadi apabila ada sengketa di antara para pihak. Sengketa itu sendiri biasanya penyelesaiannya ditentukan oleh salah satu klausula dalam perjanjian. Umumnya penyelesaian itu dapat melalui lembaga litigasi atau non-litigasi. Khusus untuk pembahasan pembuktian ini diarahkan pada pola penyelesaian di lembaga peradilan.

Dalam konteks hukum Indonesia mengenai pembuktian mengacu pada hukum acara perdata. Dasar beracara dalam perkara perdata pengaturannya ditentukan dalam HIR (*Herzein Inlands Reglements*) atau RIB (Reglemen Indonesia yang diperbaharui).

Hukum Pembuktian (yang tercantum dalam buku keempat dari BW (Burgerlijk Wetboek)/Kitab Undang-Undang Hukum Perdata), mengandung segala aturan-aturan pokok pembuktian dalam perdata. Pembuktian dalam BW semata-mata hanya berhubungan dengan perkara saja. Ada beberapa definisi yang dikemukakan oleh para ahli hukum yang dapat dijadikan acuan. Menurut Pitlo, Pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya.<sup>41</sup> Menurut Subekti yang dimaksudkan

---

<sup>41</sup>Arrianto Mukti, Edwon Makarim, Leny Helena dkk, *Kerangka Hukum Tanda Tangan Digital Dalam Electronic Commerce Untuk Indonesia* tahun 2000.Hlm.54.

dengan 'membuktikan' adalah meyakinkan hakim tentang kebenaran dalil atau dalil-dalil yang dikemukakan dalam suatu persengketaan.

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

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

Dengan melakukan pembuktian maka akan dapat dilakukan suatu membenaran/penyangkalan terhadap suatu dalil yang dikemukakan oleh para pihak yang terlibat dalam perkara.

## Pembuktian dalam Peradilan (Indonesia)

Pada prinsipnya, menurut KUHPer, bentuk suatu perjanjian adalah bebas, tidak terikat pada bentuk tertentu. Namun, bila undang-undang menentukan syarat sahnya perjanjian seperti bila telah dibuat secara tertulis, atau bila perjanjian dibuat dengan akta notaris, perjanjian semacam ini di samping tercapainya kata sepakat terdapat kekecualian yang ditetapkan undang-undang berupa formalitas-formalitas tertentu. Perjanjian semacam ini dikenal dengan perjanjian formil, apabila formalitas-formalitas tersebut tidak dipenuhi, maka perjanjian tersebut akan terancam batal (seperti pendirian PT atau pengalihan hak atas tanah).

Untuk pengaturan *e-commerce* kita menerapkan KUHPer secara analogi, dimana terhadap ketentuan-ketentuan dari *e-commerce* diterapkan ketentuan dari Buku II tentang Hukum Perikatan dan KUHDagang). Dalam KUHPerdata ditentukan bahwa suatu persetujuan adalah suatu perbuatan dengan mana suatu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih.<sup>42</sup> Untuk sahnya suatu kontrak maka kita harus melihat kepada syarat-syarat yang diatur di dalam pasal.1320 KUHPer yang menentukan bahwa syarat sahnya suatu perjanjian adalah sebagai berikut:

- i. kesepakatan para pihak;
- ii. kecakapan untuk membuat perjanjian;
- iii. suatu hal tertentu; dan

---

<sup>42</sup>Pasal 1313 KUHPer

iv. suatu sebab yang halal.

Dalam hal tidak terpenuhinya unsur pertama (kesepakatan) dan unsur kedua (kecakapan) maka kontrak tersebut dapat dibatalkan. Sedangkan apabila tidak terpenuhinya unsur ketiga (suatu hal tertentu) dan unsur keempat (suatu sebab yang halal) maka kontrak tersebut adalah batal demi hukum.

Suatu persetujuan tidak hanya mengikat apa yang dengan tegas ditentukan di dalamnya melainkan juga segala sesuatu yang menurut sifatnya persetujuan dituntut berdasarkan keadilan, kebiasaan atau undang-undang (ps.1339 KUHPer). Syarat-syarat yang selalu diperjanjikan menurut kebiasaan, harus dianggap telah termasuk dalam suatu persetujuan, walaupun tidak dengan tegas dimasukkan di dalamnya.<sup>43</sup>

Saat ini, dengan makin pesatnya kemajuan teknologi informasi, dimana dengan adanya kemajuan tersebut orang dapat melakukan transaksi-transaksi perdagangan dengan tanpa kehadiran para pihak, seperti transaksi perdagangan dilakukan dengan *online trading*.

Menurut ajaran yang lazim dianut sekarang, perjanjian harus dianggap lahir pada saat pihak yang melakukan penawaran (*offerte*) menerima jawaban yang termaktub dalam surat tersebut, sebab detik itulah yang dapat dianggap sebagai detik lahirnya kesepakatan. Walaupun kemudian mungkin yang bersangkutan tidak membuka surat itu, adalah menjadi tanggungannya sendiri. Sepantasnyalah

---

<sup>43</sup> pasal.1347 KUHPer

yang bersangkutan membaca surat-surat yang diterimanya dalam waktu yang sesingkat-singkatnya, karena perjanjian sudah lahir. Perjanjian yang sudah lahir tidak dapat ditarik kembali tanpa izin pihak lawan. Saat atau detik lahirnya perjanjian adalah penting untuk diketahui dan ditetapkan, berhubung adakalanya terjadi suatu perubahan undang-undang atau peraturan yang mempengaruhi nasib perjanjian tersebut, misalnya dalam pelaksanaannya atau masalah beralihnya suatu risiko dalam suatu perjanjian jual beli.

Tempat tinggal (domisili) pihak yang mengadakan penawaran (*offerte*) itu berlaku sebagai tempat lahirnya atau ditutupnya perjanjian. Tempat inipun menjadi hal yang penting untuk menetapkan hukum manakah yang akan berlaku.

Sampai saat ini sistem pembuktian hukum privat masih menggunakan ketentuan yang diatur di dalam KUHPer, HIR (untuk Jawa Madura) dan RBg (untuk luar Jawa Madura). Dalam hukum pembuktian ini, alat-alat bukti dalam perkara perdata terdiri dari: bukti tulisan, bukti saksi-saksi, persangkaan-persangkaan, pengakuan dan bukti sumpah.<sup>44</sup>

Sementara itu, dengan pesatnya Teknologi Informasi melalui internet sebagaimana telah dikemukakan, yaitu telah mengubah berbagai aspek kehidupan, diantaranya mengubah kegiatan perdagangan yang semula dilakukan dengan cara kontak fisik, kini dengan internet kegiatan perdagangan dilakukan secara elektronik (*Electronic Commerce* atau *E-Commerce*) atau di Bursa Efek dikenal dengan *online trading*.

---

<sup>44</sup> pasal.1866 KUHPer atau 164 HIR

Keadaan tersebut di atas belum mendapat pengaturan dalam sistem hukum pembuktian, karena sampai saat ini hukum pembuktiannya masih menggunakan ketentuan hukum yang lama (KUHPer,HIR, dan RBg). Namun demikian, keberadaan Undang-undang No.8 Tahun 1997 tentang Dokumen Perusahaan (UU Dokumen Perusahaan) telah mulai menjangkau ke arah pembuktian data elektronik.<sup>45</sup>

Memang, UU Dokumen Perusahaan tidak mengatur masalah pembuktian, namun UU ini telah memberi kemungkinan kepada dokumen perusahaan yang telah diberi kedudukan sebagai alat bukti tertulis otentik untuk diamankan melalui penyimpanan dalam mikro film. Selanjutnya, terhadap dokumen yang disimpan dalam bentuk elektronik (*paperless*) ini dapat dijadikan sebagai alat bukti yang sah. Di samping itu dalam pasal.3 UU Dokumen Perusahaan telah memberi peluang luas terhadap pemahaman atas alat bukti, yaitu: "dokumen keuangan terdiri dari catatan, bukti pembukuan, dan data pendukung administrasi keuangan, yang merupakan bukti adanya hak dan kewajiban serta kegiatan usaha perusahaan". Selanjutnya, ps.4 UU tersebut menyatakan: "dokumen lainnya terdiri dari data atau setiap tulisan yang berisi keterangan yang mempunyai nilai guna bagi perusahaan meskipun tidak terkait langsung dengan dokumen perusahaan". Berdasarkan uraian tersebut, maka tampaknya UU ini telah memberi kemungkinan dokumen perusahaan untuk dijadikan sebagai alat bukti.

---

<sup>45</sup> Mertokusumo, Sudikno, *Hukum Acara Perdata Indonesia*, edisi ke empat, PT Liberty Yogyakarta 1993. Hlm. 11.

Dalam pasal 164 HIR (284 RBG) dan 1866 KUH Perdata ada lima alat bukti yang dapat diajukan dalam proses persidangan. Alat bukti itu adalah:

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

Apabila melihat pada ketentuan ini dan kemungkinan *digital signature* digunakan sebagai alat bukti tidak dimungkinkan atau akan ditolak baik oleh hakim maupun pihak lawan. Hal ini karena pembuktian yang dikehendaki berdasarkan pada ketentuan di atas mensyaratkan baha alat bukti itu berupa tulisan, sementara *digital signature* sifatnya tanpa kertas bahkan merupakan *scripless transaction*.<sup>46</sup>

Sebenarnya dalam sistem hukum juga sudah dikenal konsep keamanan untuk perdagangan yang agak mirip dengan konsep kriptografi kunci publik (penekanan pada konsep pasangan / pairs). Zaman dahulu, untuk keperluan otentifikasi dengan mitra dagang, dipergunakan tongkat 96 kayu yang dipatahkan menjadi dua. Jika orang hendak melakukan pencacahan atas suatu transaksi, orang menorehkan sebuah goresan yang menggores sambungan kedua tongkat (yang berpasangan) tersebut. Untuk mencocokkan, cukup dengan menyambungkan

---

<sup>46</sup>Hanitijo Soematri, *Metodologi Penelitian Hukum dan Jurimetri*, PT Ghalia Indonesia, Jakarta.Hlm. 88.

kedua tongkat tersebut dan melihat apakah goresan ini 'melintas' sambungan / patahan tongkat dengan baik.

Hal ini dapat dilihat pada bunyi Pasal 1887 Kitab Undang-undang Hukum Perdata (KUHP Perdata) yang berbunyi:

“Tongkat-tongkat berkelar yang sesuai dengan kembarnya’ harus dipercaya, jika dipergunakan antara orang-orang yang biasa membuktikan penyerahan-penyserahan barang yang dilakukannya atau diterima dalam jumlah-jumlah kecil, dengan cara yang demikian itu”.

Namun menurut pendapat penulis, penggunaan pasal tersebut untuk tanda tangan elektronik kurang kuat. Seperti yang telah dijelaskan sebelumnya bahwa suatu tulisan, 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.

Yang menjadi masalah, apakah tanda tangan digital tersebut mempunyai makna atau fungsi atau bahkan kekuatan hukum yang sama dengan tanda tangan konvensional? Ada dua point yang harus diperhatikan sebelum menjawab pertanyaan ini:

- a. Bahwa fungsi hakiki dari tanda tangan konvensional dalam suatu dokumen (perjanjian) adalah untuk membuktikan keberadaan dari para pihak yang terlibat dalam perjanjian. Maksudnya kalau ada sengketa (atau permasalahan yang berkenaan dengan dokumen tersebut), maka dapat dibuktikan keberadaan para pihak yang menandatangani

dokumen tersebut dan menjadi suatu perwujudan kesepakatan terhadap isi dokumen yang bersangkutan.

- b. Kemudian, sebenarnya yang diinginkan adalah agar tanda tangan elektronik memiliki kesamaan keberadaan hukum dengan tanda tangan konvensional pada kertas.

Ada beberapa cara yang dapat diusulkan untuk membuktikan keberadaan tanda tangan elektronik sehingga mendapatkan pengakuan awal sebelum proses pengadilan berlangsung. Artinya, keaslian tanda tangan elektronik itu langsung dapat diakui di pengadilan (*presumption*) kecuali ada yang bisa membuktikan sebaliknya (pembuktian terbalik) salah satu cara yang banyak digunakan berbagai negara adalah dengan cara melakukan audit dan memberikan lisensi pemerintah terhadap infrastruktur yang dipergunakan untuk 'membuat' tanda tangan elektronik. Lisensi tersebut memberikan jaminan bahwa infrastruktur tersebut telah diaudit dan memenuhi syarat minimum yang ditetapkan pemerintah.

Dalam banyak kasus yang diberikan lisensi adalah CA-nya. Oleh karena itulah, tanda tangan yang dihasilkan oleh infrastruktur kunci publik yang disediakan oleh CA yang berlisensi seharusnya dapat langsung diterima di pengadilan tanpa perlu dibuktikan keasliannya.

Ketidakmungkinan *digital signature* dipakai sebagai alat bukti tidaklah absolut, namun relatif sifatnya. Sebab menurut hukum acara perdata Indonesia, apabila ada sengketa, kemudian sengketa itu diserahkan pada hakim dalam penyelesaiannya, maka hakim tidak boleh menolak perkara tersebut dengan alasan

tidak ada hukumnya (*asas ius curia novit*). Artinya jika terjadi sengketa dalam transaksi pembayaran elektronik antara para pihak, maka hakim pun wajib untuk menerimanya.

Dengan alasan ini pula sebenarnya hakim di Indonesia diberi keleluasaan untuk menemukan hukum. Seandainya terjadi sengketa dalam transaksi pembayaran, maka sebenarnya dengan metode penemuan hukum hakim dapat saja menganggap bahwa *digital signature* sebagai alat bukti. Dengan catatan hakim harus dibekali pengetahuan yang cukup mengenai skema sistem pembayaran elektronik. Setidaknya mengetahui mekanisme sistem pembayaran elektronik yang secara keseluruhan tidak berbasis kertas. Metode yang digunakan adalah metode interpretasi analogis dan interpretasi ekstensif.

Interpretasi analogis merupakan penemuan hukum yang dilakukan oleh hakim dengan cara memberi penafsiran pada suatu peraturan hukum dengan memberi kias pada kata-kata dalam peraturan tersebut sesuai dengan asas hukumnya, sehingga suatu peristiwa yang sebenarnya tidak dapat dimasukkan kemudian dianggap sesuai dengan bunyi peraturan tersebut. Contohnya analogi mengenai aliran listrik dan data elektronik. Dalam kaitan ini *digital signature* sebagai data elektronik belum ada peraturannya secara khusus, maka dalam proses pembuktiannya dapat dilakukan melalui metode interpretasi analogis.

Interpretasi ekstensif dilampaui batas-batas yang ditetapkan oleh interpretasi gramatikal. Melalui metode interpretasi ekstensif ini, maka makna

tertulis sebagaimana yang dimaksudkan dalam ketentuan alat bukti menurut hukum acara Indonesia dapat diperluas.

Metode interpretasi ekstensif ini seharusnya diawali dulu dengan memberikan penjelasan terhadap kata tertulis. Berdasarkan pasal 1904 KUH Perdata dikenal pembagian katagori tertulis terdiri dari:

- a Otentik
- b Bawah tangan

Pengaturan lebih lanjut berkaitan dengan kata tertulis ini terdapat juga pada pasal 1905-1920 KUH Perdata yang membaginya lagi dalam dua bagian:

- a Akta
- b Bukan Akta

Pengaturan / pembagian kata tertulis ini dalam hukum Indonesia masih ada kerancuan, namun demikian untuk menengahi perbedaan ini dapatlah dikemukakan pendapat Pitlo, salah satu sarjana Hukum asal Belanda yang memadukan perbedaan di atas. Menurutny katagori tertulis itu meliputi;

- 1) Akta Otentik
- 2) Akta bawah tangan
- 3) Bukan Kata<sup>47</sup>

Katagori yang akan dijelaskan di sini hanyalah menyangkut poin satu, yakni akta otentik. Suatu dapat dikatakan akta otentik apabila akta tersebut dibuat berdasarkan undang-undang dan dihadapan seorang pejabat yang berwenang.

---

<sup>47</sup> Onno W.Purbo & Anng Arif Wahyudi, *Mengenal e-Commerce*, PE. Elex Media Koputindo, 2001. Hlm.32.

Dalam hal sistem pembayaran elektronik, tidak ada alat bukti lain yang dapat digunakan selain data elektronik / digital berupa *digital signature*. Untuk dapat diklasifikasikan dalam bentuk tertulis banyak cara yang dapat dilakukan. Salah satu cara tersebut dengan membuat suatu *printout* atau *copy* dari pesan yang masih berbentuk elektronik. Hukum Indonesia ternyata belum memungkinkan untuk menggunakan cara ini. Namun, hukum Indonesia malah merupakan kebalikannya, peralihan itu terjadi dari yang tertulis ke bentuk data elektronik. Hal ini dapat ditemukan pada pasal 12 UU No. 8 tahun 1987 tentang Dokumen Perusahaan yang berbunyi:

- a) Dokumen perusahaan dapat dialihkan ke dalam *mikrofilem* atau media lainnya.
- b) 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;
- c) Dalam mengalihkan dokumen perusahaan sebagaimana 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;
- d) 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 dilakukan untuk menjadikan dokumen perusahaan ini mempunyai kekuatan alat bukti, maka perlu ada proses legalisasi. Pengaturan legalisasi ini terdapat pada ketentuan pasal 13 dan pasal 14 UU No. 8 Tahun 1997 tentang Dokumen Perusahaan berbunyi: "Setiap pengalihan dokumen perusahaan sebagaimana dimaksud dalam pasal 12 ayat (1) wajib dilegalisasi." Pasal 14 UU No. 8 Tahun 1997 berbunyi:

- 1) Legalisasi sebagaimana dimaksud dalam pasal 13 dilakukan oleh pimpinan perusahaan atau pejabat yang ditunjuk di lingkungan perusahaan yang bersangkutan, dengan dibuat beserta acara:
- 2) Berita acara yang dimaksud dalam ayat (1) sekurang-kurangnya memuat:
  - a. Keterangan tempat, hari, tanggal, bulan dan tahun dilakukannya legalisasi;
  - b. Keterangan bahwa pengalihan dokumen perusahaan yang dibuat di atas kertas ke dalam *mikrofilm* atau media lainnya telah dilakukan sesuai dengan aslinya;
- 3) Tandatangan 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:

- (i) Dokumen perusahaan yang telah dimuat dalam *mikrofilm* atau media lainnya sebagaimana dimaksud dalam pasal 12 ayat (1) dan atau hasil cetaknya merupakan alat bukti yang sah;
- (ii) 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.

Meskipun dapat saja hakim mengatakan bahwa *digital signature* dapat dijadikan sebagai alat bukti sah melalui metode interpretasi, tetapi, untuk kepentingan jangka panjang sangat diperlukan sekali aturan hukum yang mengatur secara tegas berhubungan dengan *digital signature*.

Untuk memformulasikan aturan hukum, model *law on electronic commerce* layak untuk dijadikan acuan dalam pengaturan *digital signature* ini. Pasal 5 *Unictral Model law on Electronic Commerce* menyatakan bahwa *data messages* mempunyai kekuatan hukum dan dapat dijalankan secara hukum. Hal ini dikarenakan pesan-pesan ini mempunyai sifat-sifat yang dimiliki oleh perjanjian-perjanjian konvensional yang biasa dikenal. Sehingga berdasarkan pasal ini *data messages* ini mempunyai kekuatan yuridis. Seluruh *data messages* dikirim oleh para pihak dengan menggunakan *digital signature*. Pesan ini senantiasa dapat diakses (dapat dilihat), dapat diperiksa orisinalitasnya (dengan mengecek *messages digest*), dapat mengidentifikasi penandatannya (ditandatangani dengan menggunakan kunci privat penandatannya).

Model Law menyatakan beberapa persyaratan agar suatu pesan dapat masuk ke dalam kriteria “*writing*”. Kriteria yang dipakai adalah:

- i) Adanya bukti yang cukup yang dapat membuktikan adanya kata sepakat dari para pihak;
- ii) Memberitahukan kepada para pihak bahwa perbuatan yang dilakukannya ini mempunyai akibat hukum;
- iii) Mempertahankan keberadaan dokumen tersebut (dokumentasi) untuk suatu jangka waktu tertentu;
- iv) Kemungkinan dilakukannya otentifikasi terhadap dokumen tersebut dengan menggunakan tandatangan yang ada;
- v) Memudahkan verifikasi yang dilakukan oleh pemerintah atau untuk kepentingan pengadilan;
- vi) Untuk memudahkan para pihak menutup perjanjian (*finalize*) dan menyediakan bukti telah adanya kesepakatan itu;
- vii) Untuk memastikan data atau informasi yang ada belum pernah diubah / dirusak sejak ia pertama kali dibuat (dengan kata lain disini ditekankan pada faktor *integrity* dari data tersebut);
- viii) *Digital signature* yang terdapat dalam pesan atau data *messages* ini adalah dibuat dalam suatu jangka waktu yang terdapat di dalam *certificate*. Jadi selama *certificate* itu masih valid (sah). *Digital signature* tersebut dibuat dengan menggunakan kunci privat, yaitu pasangan kunci dari kunci publik yang terdapat dalam *certificate*

tersebut. Jangka waktu dari berlakunya *certificate* itu dapat dilihat dari *certificate Practice Statement* (CPS) milik *issuer* dari *certificate* tersebut, sedangkan untuk mengetahui apakah *certificate* tersebut masih valid atau tidak dapat dilihat di *certificate Revocation List* (CRL). Keberadaan CPS dan CRL adalah sangat penting dalam proses penandatanganan suatu dokumen karena ia akan menentukan apakah dokumentasi tersebut valid atau tidak;

- ix) Untuk memudahkan pendokumentasian data dalam bentuk tertentu (*intangible form*);
- x) *Digital signature* tersebut milik dari orang yang dianggap telah menandatangani (di sini ditekankan pada prinsip otensitas). Berdasarkan hal ini, maka sangat penting untuk menjaga keberadaan kunci privat agar jangan sampai digunakan oleh orang lain yang tidak berhak. Apabila kunci privat itu hilang atau dicuri orang, maka *certificate* pasangannya harus segera di – *revoke*. Pemilik kunci yang asli mempunyai kewajiban untuk segera melaporkan peristiwa ini, karena ia dapat diminta pertanggungjawaban atas penggunaan kunci yang tidak pada tempatnya;
- xi) *Digital signature* yang digunakan oleh pemiliknya, digunakan dengan kesadaran yang penuh dari penandatanganan. Penandatanganan tersebut harus bebas dari unsur tekanan, paksaan ataupun kekhilafan;

xii) Untuk menunjang dilakukannya kontrol dan audit untuk kepentingan akuntansi, pajak dan ketentuan perundangan yang berlaku lainnya.<sup>48</sup>

Pasal 6 menekankan pada keuntungan dari sifat tertulis (*writing*) untuk maksud dan tujuan itu saja dan bukan secara umum. Pasal ini menekankan adanya alat bukti untuk kepentingan pajak dan peraturan perundang-undangan lainnya. Pasal ini juga menekankan bahwa *data message* tersebut dapat dibaca dan digunakan untuk berbagai tujuan. Untuk menentukan sah dan tidaknya suatu dokumen maka diperlukan suatu lembaga yang menentukannya (Lembaga Sertifikasi Tanda Tangan Digital) yang berfungsi sebagai lembaga yang diberi kewenangan untuk mengeluarkan sertifikat tanda tangan digital yang diberikan oleh negara jadi fungsi lembaga ini sama dengan notaris di dunia nyata yang mereka itu mensahkan setiap transaksi sehingga mempunyai kekuatan pembuktian yang sempurna, namun sampai sekarang Indonesia belum mengakui lembaga ini.

Dari perspektif hukum, *digital signature* adalah sebuah pengaman pada data digital yang dibuat dengan kunci tanda tangan pribadi (*private signature key*), yang penggunaannya tergantung pada kunci publik (*public key*) yang menjadi pasangannya. Eksistensi *digital signature* ini ditandai oleh keluarnya sebuah sertifikat kunci tanda tangan (*signature key certificate*) dari suatu badan pembuat sertifikat (*certifier*). Dalam sertifikat ini ditentukan nama pemilik kunci tanda

---

<sup>48</sup> Dalam; Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005. 66.

tangan dan karakter dari data yang sudah ditandatangani, untuk kekuatan pembuktian.<sup>49</sup>

Beberapa masalah yang mungkin timbul dari sistem *digital signature* ini terkait dengan sistem hukum yang sudah ada. Pada banyak negara, disyaratkan bahwa suatu transaksi haruslah disertai dengan bukti tertulis, dengan pertimbangan kepastian hukum.

Permasalahannya, bagaimana sebuah dokumen elektronik yang ditandatangani dengan sebuah *digital signature* dapat dikategorikan sebagai bukti tertulis? Di Inggris, bukti tertulis haruslah berupa tulisan (*typing*), ketikan (*printing*), litografi (*lithography*), fotografi, atau bukti-bukti yang mempergunakan cara-cara lain, yang dapat memperlihatkan atau mengolah kata kata dalam bentuk yang terlihat secara kasat mata. Definisi dari bukti tertulis itu sendiri sudah diperluas hingga mencakup juga "telex, telegram, atau cara-cara lain dalam telekomunikasi yang menyediakan rekaman dan perjanjian" (UNCITRAL Model Law on Internatinal Commercial Arbitration, art.7 (2)).

Sebenarnya, dari fakta-fakta tersebut dapatlah ditarik kesimpulan bahwa dokumen elektronik yang ditandatangani dengan sebuah *digital signature* dapat dikategorikan sebagai bukti tertulis. Tetapi, terdapat suatu prinsip hukum yang menyebabkan sulitnya pengembangan penggunaan dan dokumen elektronik atau

---

<sup>49</sup> German Draft *Digital signature Law*, 1996

*digital signature*, yakni adanya syarat bahwa dokumen tersebut harus dapat dilihat, dikirim dan disimpan dalam bentuk kertas.

Masalah lain yang dapat timbul berkaitan dengan dokumen elektronik dan *digital signature* ini adalah masalah cara untuk menentukan dokumen yang asli dan dokumen salinan. Berkaitan dengan hal ini sudah menjadi prinsip hukum umum bahwa:

- a. dokumen asli mestilah dalam bentuk perjanjian tertulis yang ditandatangani oleh para pihak yang melaksanakan perjanjian;
- b. dokumen asli hanya ada satu dalam setiap perjanjian; dan
- c. semua reproduksi dari perjanjian tersebut merupakan salinan.

Suatu pembuktian lazimnya baru dilakukan apabila ada suatu perselisihan. Suatu perselisihan diselesaikan di badan peradilan Indonesia, apabila telah disepakati oleh kedua belah pihak atau telah ada di dalam suatu kontrak yang di dalamnya terdapat suatu klausul yang menyebutkan bahwa setiap perselisihan yang timbul akan diselesaikan menurut hukum Indonesia dan diselenggarakan di Peradilan Indonesia.

Di dalam badan peradilan di Indonesia, dikenal suatu hukum acara yang fungsinya mengatur hal-hal yang diselenggarakan di dalam proses peradilan. Di dalam hal ini, hukum positif (hukum yang berlaku saat ini) yang ada adalah HIR (Herzien Inlands Reglement) atau yang dikenal dengan sebutan RIB (Reglemen Indonesia yang diperBaharui), yaitu undang-undang yang termuat dalam

Staatsblaad 1941 No.44. Mungkin terpikir oleh awam, inilah yang sering didengarkan oleh para ahli hukum di Indonesia, mengenai produk hukum Belanda yang masih berlaku sampai sekarang ini. Hal ini benar adanya, sebagaimana adanya kekosongan hukum dan keberlakuan dari HIR ini, juga hanya diatur dalam UU Darurat.

Kenyataan inilah yang harus kita hadapi bersama, mengingat sebagai produk lama maka besar pula kemungkinan dimana kita hanya menemui peraturan hukum yang mengatur mengenai hal-hal yang sifatnya tidak atau belum up to date, apalagi dalam hal ini kita membicarakan mengenai kegiatan sehubungan dengan *e-commerce* dengan penggunaan Digital Signature, sesuatu yang baru dan belum terpikirkan oleh pembentuk undang-undang ini pada waktu dibuatnya. Sebagaimana diatur dalam 164 HIR (283 RBG) dan 1903 BW, hanya dikenal 5 (lima) macam alat bukti yang dapat dihadirkan di persidangan khususnya dalam acara perdata, di antaranya:

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

## 5 Sumpah

Sedangkan khusus dalam acara pidana, dikenal adanya barang bukti dan alat bukti. Dalam doktrin ilmu hukum pidana, barang bukti dapat dikategorikan dalam tiga antara lain:

- a) barang yang digunakan untuk melakukan perbuatan pidana,
- b) barang yang digunakan untuk membantu terjadinya perbuatan pidana dan
- c) barang yang menjadi hasil perbuatan pidana.

Sedangkan alat bukti dalam acara pidana (Pasal 184 KUHAP) dengan alat bukti dalam acara perdata secara umum adalah sama.<sup>50</sup>

*Digital Signature* sebagai suatu data elektronik di dalam hal ini mempunyai masalah apabila diajukan sebagai alat bukti di dalam beracara di Badan Peradilan Indonesia. *Digital Signature* yang digunakan dalam transaksi *e-commerce* secara keseluruhan adalah merupakan *paperless*, bahkan *scriptless transaction*. Sesuai apa yang diatur dalam pasal tersebut, maka dalam hal ini berarti bukti-bukti berupa data elektronik yang diajukan akan dianggap tidak mempunyai kekuatan

---

<sup>50</sup>Sudikno Mertokusumo, *Hukum Acara Perdata Indonesia*, edisi ke empat, PT Liberty Yogyakarta 1993.Hlm. 103.

hukum pembuktian. Kemungkinan juga besar, terhadap ditolakny hal ini sebagai alat bukti oleh hakim maupun pihak lawan.

Hukum Acara yang ada dan berlaku sekarang (hukum acara positif) dalam hal ini perlu ditinjau ulang untuk adanya kemungkinan dilakukannya suatu revisi, mengingat adanya kebutuhan yang mendesak ini. Masalah *e-commerce* sudah ada di depan mata dan adanya kemungkinan munculnya suatu kasus perselisihan/dispute tinggal menunggu waktu saja. Apabila hal ini terjadi maka akan dapat diduga munculnya permasalahan pembuktian yang kompleks. Hal-hal yang telah disebutkan di atas hanyalah merupakan sebagian dari keseluruhan permasalahan.

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

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

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

Penafsiran (interpretasi) yang dapat dilakukan oleh hakim maupun ahli hukum antara lain dapat melalui interpretasi analogis maupun interpretasi ekstentif. Interpretasi analogis dapat dilakukan apabila belum ada suatu peraturan hukum yang mengatur mengenai data elektronik/digital, terutama dalam hal ini yang berkaitan dengan digital signature, belum ada. Jadi hakim dapat mengambil norma-norma yang ada di masyarakat untuk melakukan interpretasi analogis. Interpretasi ekstentif dapat dilakukan apabila telah ada peraturan hukumnya, tetapi

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

Definisi Surat diberikan oleh para ahli hukum pembuat BW, yaitu pembawa tanda tangan bacaan yang berarti, yang menterjemahkan suatu isi pikiran. Atas bahan apa dicantumkan tanda bacaan ini, adalah tidak penting (PITLO, dalam buku *Bewijs en Verjaring naar het Nederlands Burgerlijk Wetboek*). Jadi tidak memandang ditulisnya di atas lembaran kertas, di atas bungkus sigaret, maupun di atas buah semangka, tetap merupakan surat.<sup>51</sup> Dalam permasalahan yang kita hadapi ini berkaitan dengan penggunaan data elektronik sebagai media penyampaian pesan. Bisakah kita analogikan hal tersebut dalam penulisan surat di atas media elektronik? Hal ini akan kita lihat lebih lanjut nantinya.

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

- a. Otentik
- b. bawah tangan

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

---

<sup>51</sup> Arrianto Mukti, Edwon Makarim, Leny Helena dkk, *Kerangka Hukum Tanda Tangan Digital Dalam Electronic Commerce Untuk Indonesia*, tahun 2000. Hlm. 25.

a. Akta

b. Bukan Akta

Terdapat kerancuan mengenai hal ini, kenapa sampai ada dua pembagian ketentuan hukum yang berbeda mengenai kualifikasi tertulis. Terdapat teori yang dikemukakan oleh Pitlo, Sarjana Hukum Belanda, yang mengambil jalan tengah, yaitu menggabungkan unsur dan mengelompokkannya sesuai urutan kekuatannya<sup>52</sup>:

a. Akta Otentik

b. Akta Bawah Tangan

c. Bukan Akta

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

---

<sup>52</sup>Arrianto Mukti Wibowo, Tanda tangan digital & sertifikat digital: Apa itu? 1998 Artikel ini muncul pada Infokomputer edisi Internet Juni 1998. Hlm. 71.

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

Ada tiga macam kekuatan dari suatu akta otentik, yaitu<sup>53</sup>:

- a. Membuktikan antara para pihak, bahwa mereka sudah menerangkan apa yang ditulis dalam akta tersebut (pembuktian formal)
- b. Membuktikan antara para pihak yang bersangkutan, bahwa sungguh-sungguh peristiwa yang disebutkan di sini telah terjadi (pembuktian mengikat)

---

<sup>53</sup> Grup Riset Digital Security & Electronic Commerce, *Aplikasi Teknologi Sekuriti Digital*, Fakultas Ilmu Komputer Universitas Indonesia.. 1999.

- c. Membuktikan tidak saja antara para pihak yang bersangkutan tetapi juga terhadap pihak ketiga, bahwa pada tanggal tersebut dalam akta, kedua belah pihak tersebut telah menghadap di muka pegawai umum dan menerangkan apa yang ditulis dalam akta tersebut. (pembuktian keluar)

Sebelum mengulas mengenai kekuatan pembuktian yang sama tersebut, kita tinjau terlebih dahulu mengenai surat otentik. Dikatakan sebagai suatu akta/surat otentik apabila mengandung unsur-unsur sebagai berikut ini sebagaimana diatur dalam Pasal 1905 BW: Akta otentik adalah akta yang dibuat menurut bentuk Undang-Undang oleh dan dihadapan seorang pegawai umum yang berwenang di tempat itu. Dapat disarikan di luar definisi sebagai berikut: bentuknya tertulis, dibuat oleh atau dihadapan pejabat/pegawai umum yang berwenang. Pejabat yang dimaksudkan di sini adalah orang yang berwenang karena atas dasar jabatannya yang diangkat oleh negara, contohnya profesi notaris atau PPAT (Pejabat Pembuat Akta Tanah).

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

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

Ketentuan yang ada dalam pasal-pasal tersebut menyebutkan, bahwa suatu bentuk tertulis nyata (dalam hal ini segala tulisan yang dibuat berkenaan dengan kegiatan perusahaan) dapat diubah ke bentuk lain (contohnya mikrofilm atau CD) setelah sebelumnya dilakukan suatu verifikasi dan legalisasi yang dalam hal ini dilakukan oleh pimpinan perusahaan atau pejabat yang ditunjuk di lingkungan perusahaan dengan dibuatkan suatu berita acara. Setelah ada verifikasi dan legalisasi bahwa kedua bentuk dokumen tersebut isinya sama secara keseluruhan

maka sebagaimana disebutkan dalam Pasal 15 ayat (1) maka media hasil transformasi tersebut dan atau hasil cetaknya merupakan alat bukti yang sah.

### **C. Aspek Perlindungan Konsumen Dalam *Digital Signature***

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

1. *Certificate Authority (CA)*
2. *Subscriber*

Hubungan ini menunjukkan kaitan antara CA sebagai penyelenggara jasa dan subscriber sebagai konsumen. Sebagai penyelenggara jasa, CA harus menjamin hak-hak *subscriber* antara lain<sup>54</sup>:

#### **1. *Privacy***

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

---

<sup>54</sup>*Ibid.*

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

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

Pelanggaran terhadap prinsip-prinsip perlindungan data dapat menyebabkan tanggung jawab pidana, adapun prinsip-prinsip tersebut antara lain:<sup>55</sup>

- a. Informasi yang dimuat dalam data pribadi harus diperoleh, dan data pribadi itu harus diproses, secara jujur dan sah.
- b. Data pribadi harus dipegang hanya untuk satu tujuan atau lebih yang spesifik dan sah.
- c. 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.
- d. 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
- e. Data pribadi harus akurat dan, jika diperlukan, selalu *up-to date*.

---

<sup>55</sup>Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005.Hlm. 28.

f. 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.

g. 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.

h. Seorang individu akan diberikan hak untuk:

1. Dalam jangka waktu yang wajar dan tanpa kelambatan serta tanpa biaya:

(a) Diberi penjelasan oleh pihak pengguna data tentang apakah pihaknya menguasai data pribadi di mana individu yang bersangkutan menjadi subyek data; dan

(b) Untuk akses pada suatu data demikian yang dikuasai oleh pihak pengguna data.

2. 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 subscriber. CA mempunyai peluang yang besar untuk bisa menemukan kunci pasangan dari subscriber karena CA mempunyai komputer yang lebih canggih untuk menemukannya.<sup>56</sup>

Selain itu harus ada jaminan bahwa pencipta kartu yang berisikan kunci privat juga tidak akan menyebarkan 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.

---

<sup>56</sup> David Baum, "Business Link", *Oracle Magazine*, No. 3, Vol. XIII, May/June, 1999, Hlm. 34.

## **2. Accuracy**

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

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

## **3. Property**

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

#### 4. *Accessibility*

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

Hak-hak konsumen untuk tercapainya perlindungan konsumen sudah tercantum atau dituangkan dalam bentuk Undang-Undang, yaitu UU No 8 tahun 1999. Maka artinya hak-hak tersebut sudah diakui keberadaannya dan memiliki kepastian hukumnya yang diatur dalam Undang-Undang positif. Upaya hukum yang dilakukan oleh konsumen yang merasa dirugikan bisa menggunakan pasal-pasal dalam UU No 8 tahun 1999 ini.

Dalam kaitannya dengan penggunaan *digital signature*, CA dalam kedudukan yang lebih kuat harus bisa menjamin hak-hak konsumen. Terutama dalam perjanjian adhesi antara CA dan subscriber. Perjanjian diajukan sebaiknya tidak hanya berat sebelah, sehingga subscriber tidak mempunyai posisi penawaran (*bargaining power*). Untuk menutup resiko atas produk-produk yang cacat CA dapat mengasuransikan resiko tersebut. Hal ini untuk mengurangi beban yang harus ditanggung oleh CA apabila suatu saat ada konsimen (*subscriber*) yang menuntut CA karena merasa dirugikan.

## **BAB IV**

### **PENUTUP**

#### **KESIMPULAN**

Bahwa dari apa yang telah diuraikan di atas, dengan kata lain dalam *e-commerce* para pelaku/ pihak melakukan kegiatan perdagangan/ perniagaan hanya berhubungan melalui jaringan publik (*publik network*). *Digital signatur* dalam *e-commerce* belum dapat dijadikan alat bukti dalam hukum perdata Indonesia karena belum ada undang – undang yang mengaturnya, tetapi dengan adanya *digital signature* adalah menggunakan petunjuk dalam membuktikan adanya perjanjian dalam *e-commerce*. *e-commerce* menggunakan transaksi beresiko tinggi dalam perniagaan/ perdagangan walaupun demikian telah diminimalisir dengan adanya *cryptography*.

#### **SARAN**

Perlu diperhatikan bahwa kelemahan hakiki dari *open network* yang telah dikemukakan tersebut semestinya dapat diantisipasi atau diminimalisir dengan adanya sistem pengamanan jaringan yang juga menggunakan *cryptography* terhadap data dengan menggunakan sistem pengamanan dengan *digital signature*. Indonesia secara mental masih belum siap sedangkan di lain sisi, hal ini sifatnya sangat urgent. Kenapa hal ini dikemukakan, karena jujur saja, kalangan masyarakat Indonesia yang selama ini telah melakukan kegiatan dalam ruang lingkup *e-commerce*, setidak – tidaknya yang mengetahui atau concern mengenai

masalah ini hanya terbatas pada kalangan yang selama ini akrab dengan internet (walaupun telah disebutkan sebelumnya kemungkinan *e-commerce* di luar internet). Sedangkan kalangan ini hanya sebagian kecil dari masyarakat. Selain karena pengguna komputer (yang secara tidak langsung berpengaruh) masih sedikit. Dengan perkataan lain, masyarakat Indonesia harus segera menyikapi diri menghadapi masalah ini sesegera mungkin, mengingat negara lain sudah menyiapkan diri dalam mensikapi perdagangan secara elektronik, dengan adanya kemudahan – kemudahan yang dibawanya.

Perlu dipikirkan adanya sosialisasi *e-commerce* kepada seluruh masyarakat Indonesia. Belum siapnya beberapa peraturan hukum Indonesia. Telah dikemukakan, prinsip yang kita pegang haruslah "*transform the medium, not the instrument*". Kegiatan – kegiatan dalam *e-commerce* secara general masih dapat dikategorikan sebagai tindakan perdagangan/ perniagaan biasa, walaupun terdapatnya hal – hal yang signifikan yang membedakannya seperti media elektronik yang menggantikan *paper-based transaction*. Dapat dikatakan beberapa peraturan hukum yang telah ada sekarang ini sudah dapat mencukupi, baik dengan cara melakukan penafsiran secara analogis terhadap tindakan yang ada dalam *e-commerce* (terdapat aturan yang belum ada) maupun melakukan penafsiran ekstensif dengan cara memberlakukan peraturan hukum pada hal – hal yang secara esensi adalah sama (contohnya : listrik dan data elektronik). Dalam hal – hal yang khusus di bidang *digital signature* sebagai pengamanan *e-commerce*, karena dalam bidang ini tidak dapat dilakukan penafsiran untuk menghindarkan kesalah pengertian mengenai esensi dari *digital signature*.

Perlu diperhatikan lebih lanjut bahwa perangkat hukum di Indonesia khususnya hukum perdata pada dasarnya telah mampu menjangkau permasalahan – permasalahan yang timbul. Hukum perdata ini secara umum. (secara general) :norma sudah mampu, tetapi kita masih butuh pengaturan yang lebih spesifik untuk menjamin kepastian hukum bagi setiap perbuatan hukum perdata khususnya di bidang *e-commerce*.

Untuk sementara, menghadapi kekosongan hukum di Indonesia, diperlukan peran hakim dan para aparat penegak hukum termasuk penasehat hukum, dan kepolisian serta kejaksaan. Hakim juga dituntut untuk melakukan *rechtsvinding* (penemuan hukum) selain melakukan penafsiran analogis maupun penafsiran ekstensif yang telah dikemukakan di atas.

Peran dari para konsultan hukum yang mewakili pihak yang melakukan suatu perbuatan hukum di bidang *e-commerce* sangat besar. Untuk sementara, yang dilakukan mereka adalah mencari norma – norma perlu dibentuk suatu tim khusus di bidang hukum/ regulasi *e-commerce* sesegera mungkin. Tim khusus ini perlu segera dibentuk untuk mempersiapkan peraturan hukum di bidang *e-commerce* khususnya *digital signature*. Kedudukan tim ini di bawah beberapa departemen, seperti sekretariat negara, departemen perdagangan dan industri, departemen kehakiman, departemen bidang telekomunikasi dan beberapa departemen lainnya yang berkaitan erat dengan masalah ini. Tim khusus ini dapat bekerja secara inter departemen sehingga segala permasalahan dapat dicakup secara luas.

## DAFTAR PUSTAKA

### BUKU

Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis e-Commerce, Studi Sistem dan Hukum di Indonesia*, Pustaka Pelajar, 2005.

Arrianto Mukti, Edwon Makarim, Leny Helena dkk, **Kerangka Hukum Tanda Tangan Digital Dalam Electronic Commerce Untuk Indonesia** tahun 2000.

Arrianto Mukti Wibowo, **Tanda tangan digital & sertifikat digital: Apa itu?** 1998 Artikel ini muncul pada Infokomputer edisi Internet Juni 1998.

Dimitri Mahayana, **“Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global”**, PT. Remaja Rosdakarya, 1999.

Badruzaman, Mariam Darus, *E-Commerce Tinjauan dari Hukum Kontrak Indonesia*, Jurnal Hukum Bisnis. 2000

Hanitijo Soematri, Ronny, **Metodologi Penelitian Hukum dan Jurimetri**, PT Ghalia Indonesia, Jakarta.

Haris, Freddy, *Aspek Hukum Transaksi Secara Elektronik di Pasar Modal*, Jakarta.2000.

Hasil penelitian oleh group riset Digital dan security dan electronic yang pernah dipresentasikan di hadapan Masyarakat Telekomunikasi.

Jerry Honeycutt, **“Knowledge Management Strategies”**, Microsoft Corporation, 2000.

- Mertokusumo, Sudikno, **Hukum Acara Perdata Indonesia**, edisi ke empat, PT Liberty Yogyakarta 1993.
- Onno W.Purbo & Anng Arif Wahyudi, "**Mengenal e-Commerce**", PE. Elex Media Komputindo", 2001.
- Purbo, Onno W., Wahyudi, A.A., *Mengenal E-Commerce*, PT Elex Media Komputindo, Jakarta, 2001.
- Richardus Eko Indrajit, "**Manajemen Sistem Informasi dan teknologi Informasi**", PT. Elex Media komputindo, 2000.
- Sukanto, Surjono, **Pengantar Penelitian Hukum**, cetakan pertama, Penerbit Universitas Indonesia, 1981.
- Satjipto Rahardjo, **Pembangunan Hukum di Negara-negara sedang Berkembang: Dilema Pasca-Kolonialisme**, makalah, 1995 Sunaryati Hartono, C.F.G., *In Search of New Legal Principles*, Bina Cipta, Bandung, 1982.
- Sunaryati Hartono, C.F.G., **Tentang Metode Penelitian Perbandingan Hukum**, **Pusat Studi Hukum**, Universitas Katolik Parahyangan, Bandung, 1988
- Sunggono, Bambang, **Metodologi penelitian hukum**, PT Raja Grafindo Persada Jakarta 1997.

---

**Undang-Undang Nomor 8 Tahun 1997** tentang Peraturan dan perundang-undangan, *Jurnal Hukum Bisnis*, Yayasan Pengembangan Hukum Bisnis, vol 1 tahun 1997.

## INTERNET

Mukti Fajar, *Commerce* dalam perspektif hukum Indonesia, makalah 2000 Onno W. Purbo, artikel, 10 pertanyaan tentang *E-commerce* lihat <http://www.mastel.or.id/indonesia/artikel10.htm>.

-----, *E-com* di Indonesia awal tahun 2000, MikroData media pengemar komputer Volume 3 seri 15.

Indonesia pada bulan juni 1999 di Pusat Ilmu Komputer Universitas Indonesia, Depok Jawa barat, kerangka hukum *digital signature* dalam *Electronic commerce*, 1999 lihat ><http://www.geocities.com/amwibowo/resource/.htm>

*Indonesia Infocom Bussiness* <http://www.i2bc.org/news/i2bcnews4.html> date access December 2005.

Richard hill and Ian Walden *The Draft UNCTRAL Model Law for Electronic Commerce ; issues and solutions*, terjem. Oleh M. fajar dipublikasikan maret 1996. lihat >[http://www.Banet.com/\\_ricard\\_hill](http://www.Banet.com/_ricard_hill).

## MAJALAH

Warta Ekonomi No. 9, 5 Maret 2001 Judul : Perangkat hukum di Indonesia dalam mengatasi kejahatan komputer, halaman 12-14 Web site Insecure.org at <http://insecure.org/nmap/> date access December 2005.

Majalah interaksi acuan hukum dan masyarakatan, website : <http://berita.kafedago.com/kirimkomentar.asp>, date access December 2005.

Asosiasi Jasa Penyelenggara Internet Indonesia, *website* :

<http://www.apji.or.id/news/> date access December 2005.

Majalah Gatra edisi Oktober 2004, Judul : *Cybercrime di era digital*, *website* :

<http://www.gatra.com/2004-10-13/> date access December 2005.