

# PENGAKUAN TANDA TANGAN ELEKTRONIK DALAM HUKUM PEMBUKTIAN INDONESIA

Oleh :  
Julius Indra Dwipayono Singara, S.H., D.E.A.<sup>1</sup>

*“Semper in obscuris inspici debet quod versimilis  
est aut quod plerumque fieri solet”<sup>2</sup>*

## **Abstrak**

Persatuan antara teknologi komunikasi dan teknologi informatika menciptakan Internet yang saat ini menjadi tulang punggung dari teknologi informasi. Berkat jaringan Internet, tidak ada lagi perbatasan antar suatu negara. Ia meningkatkan keefisienan serta kecepatan dalam pelaksanaan perdagangan elektronik (*e-commerce*) dan pemerintahan elektronik (*e-gouvernance*). Indonesia sebagai negara berkembang tidak luput dari perkembangan teknologi informasi yang semakin hari semakin digunakan dan menjadi salah satu “kebutuhan primer” dari sektor perdagangan. Namun di Indonesia, perkembangan teknologi berjalan lebih cepat dan seakan-akan tidak terkejar oleh hukum yang ada, padahal salah satu tujuan hukum adalah memberikan kepastian hukum. Seperti yang dikatakan Doktor Eric Caprioli, “keamanan dan kehandalan teknik harus sepadan dengan kepastian hukum sebab hukum menciptakan kepercayaan para pengguna terhadap teknologi informasi” sebab tanpa kepercayaan ini, perdagangan elektronik dan pemerintahan elektronik yang sedang digalakkan Pemerintah Indonesia tidak akan berkembang dan tidak akan memberikan kontribusi yang baik pada pembangunan Indonesia. Kepercayaan ini dapat dicapai dengan memberikan kepastian hukum terhadap tulisan elektronik.

## **Pendahuluan**

Persatuan antara teknologi komunikasi dan teknologi informatika menciptakan Internet yang saat ini menjadi tulang punggung dari teknologi informasi. Berkat jaringan Internet, tidak ada lagi perbatasan antar suatu negara. Ia meningkatkan keefisienan serta kecepatan dalam pelaksanaan perdagangan elektronik (*e-commerce*) dan pemerintahan elektronik (*e-gouvernance*), kondisi yang demikian pada satu pihak membawa manfaat bagi masyarakat, karena memberikan kemudahan-mudahan dalam melakukan berbagai aktifitas terutama yang terkait dengan pemanfaatan informasi. Akan tetapi, di sisi lain, fenomena tersebut dapat memicu lahirnya berbagai bentuk konflik di masyarakat sebagai akibat penggunaan yang tidak bertanggung jawab<sup>3</sup>.

Di Indonesia, perkembangan teknologi informasi semakin pesat dan penggunaannya pun semakin banyak, tetapi perkembangan ini tidak diimbangi dengan perkembangan produk

<sup>1</sup> Kandidat doktor di Fakultas Hukum-Université Montpellier I, Perancis.

<sup>2</sup> Haruslah selalu mengintepretasi sesuatu yang tidak terang agar menjadi terang dengan mendasarkan interpretasi tersebut terhadap hal-hal yang dapat diterima dengan akal atau terhadap nilai-nilai hukum yang hidup dalam masyarakat

<sup>3</sup> Penjelasan umum RUU ITE.

hukum sehingga timbullah berbagai macam sengketa hukum antara para penggunanya baik di tingkat nasional maupun di internasional. Padahal, kehandalan dan keamanan teknologi informasi harus seimbang dengan perlindungan hukum. Seimbang dalam artian hukum bukan berperan sebagai penghambat perkembangan teknologi, melainkan sebagai penyeimbang dari perkembangan teknologi dengan memberikan jaminan hukum bagi para penggunanya.

Kedudukan sederajat antara perlindungan hukum, kehandalan dan keamanan teknologi informasi akan menciptakan suatu “kepercayaan” kepada para penggunanya, tanpa kepercayaan ini perdagangan elektronik dan pemerintahan elektronik yang saat ini digalakkan oleh pemerintah Indonesia tidak akan berkembang. Kepercayaan ini dapat diperoleh dengan memberikan pengakuan hukum terhadap tulisan elektronik.

Hingga hari ini hukum positif Indonesia menentukan bahwa hanya satu cara untuk memberikan kekuatan hukum dan akibat hukum terhadap suatu akta, yaitu dengan tanda tangan manuskrip. Namun, dalam praktek perdagangan khususnya, tanda tangan manuskrip sudah kian tergeser dengan penggunaan tanda tangan elektronik yang melekat pada akta terdematerialisasi atau dengan kata lain “akta elektronik”, sehingga timbul perdebatan tentang pengakuan, kekuatan hukum dan akibat hukum dari sebuah tanda tangan elektronik.

Saat ini para ahli hukum dan teknologi informasi di Indonesia telah “menelorkan” sebuah Rancangan Undang-Undang yang di “baptis” dengan nama “Informasi dan Transaksi Elektronik” (selanjutnya disingkat RUU ITE), kiranya rancangan undang-undang ini akan segera dibahas oleh Dewan Perwakilan Rakyat (selanjutnya disingkat DPR) periode 2004-2009. RUU ITE akan membawa sebuah revolusi besar-besaran terhadap hukum pembuktian yang berlaku di Indonesia dengan demikian kebingungan hukum terhadap tulisan elektronik akan terjawab<sup>4</sup>.

Pasal 11 RUU ITE menentukan, “Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama **memenuhi ketentuan dalam undang-undang ini**”, artinya, selama dapat dipastikannya keterkaitan antara tanda tangan elektronik dengan Penandatanganan yang bersangkutan, dan tanda tangan elektronik tersebut dibuat dan disimpan dalam kondisi yang menjamin integritas dengan akta yang dilekatinya, maka sebuah tanda tangan elektronik mempunyai nilai hukum yang sama dengan tanda tangan manuskrip.

Tanda tangan elektronik dapat menjadi sebuah instrumen dasar pada hubungan-hubungan kontraktual, asalkan identitas penggunanya, dan integritasnya dengan akta yang dilekatinya dapat dijamin. Tentunya keamanan terhadap hubungan kontraktual ini harus dijamin, marilah melihat bagaimana keamanan ini dijamin dengan melihat pelaksanaan teknik dari tanda tangan elektronik (1) dan instrumen hukumnya (2).

---

<sup>4</sup> Lihat Pasal 3 RUU ITE tentang tujuan dari pemanfaatan teknologi informasi.

## 1. Pelaksanaan teknik tanda tangan elektronik

Hukum positif Indonesia belum pernah memberikan definisi terhadap kata “tanda tangan” yang sesungguhnya mempunyai dua fungsi hukum dasar, yaitu : (1) tanda identitas Penandatanganan, dan (2) sebagai tanda persetujuan dari Penandatanganan terhadap kewajiban-kewajiban yang melekat pada akta. Berdasarkan kedua fungsi hukum ini maka dapat ditarik suatu definisi sebagai berikut, “tanda tangan adalah sebuah identitas yang berfungsi sebagai tanda persetujuan terhadap kewajiban-kewajiban yang melekat pada akta”.

Tentunya definisi “tanda tangan elektronik” seharusnya tidak jauh dari definisi di atas; RUU ITE mendefinisikannya sebagai berikut, “Informasi elektronik yang dilekatkan, memiliki hubungan langsung atau terasosiasi pada suatu informasi elektronik lain yang ditujukan oleh pihak yang bersangkutan untuk menunjukkan identitas dan status subyek hukum<sup>5</sup>”. RUU ITE memberikan definisi lebih ke sudut teknik, padahal sebuah tanda tangan mempunyai tujuan untuk menerima/menyetujui secara meyakinkan isi dari sebuah tulisan. Hal ini sangat logis, di mana tanda tangan elektronik mempunyai dua fungsi hukum dasar<sup>6</sup>. Oleh karenanya, Penulis mencoba untuk memberikan definisi sebagai berikut, “tanda tangan elektronik adalah sebuah identitas elektronik yang berfungsi sebagai tanda persetujuan terhadap kewajiban-kewajiban yang melekat pada sebuah akta elektronik. Dia terbuat dari prosedur identifikasi handal dan mampu menjamin hubungan antara akta elektronik dan tanda tangan elektronik. Prosedur ini dianggap handal, kecuali terbukti sebaliknya, selama memenuhi ketentuan-ketentuan yang diatur oleh undang-undang ini”.

Untuk mendapatkan kekuatan hukum dan akibat hukum yang sama dengan tanda tangan manuskrip, sebuah tanda tangan elektronik harus mampu memberikan jaminan integritas dari akta elektronik (1.1.), dan mampu mengidentifikasi si Penandatanganan dari akta elektronik ini (1.2.).

### 1.1. Jaminan integritas dari akta elektronik

Pasal 11 RUU ITE menentukan bahwa, “Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi ketentuan dalam undang-undang ini”, ketentuan-ketentuan yang dimaksud dimuat dalam Pasal 13 RUU ITE yang salah satunya adalah tanda tangan elektronik tersebut harus menjamin integritas dari suatu akta elektronik yang dilekatinya. Jaminan ini dapat dicapai hanya dengan menggunakan teknik kriptologi. Kriptologi (*cryptologie*) berasal dari bahasa Yunani, yaitu “*kryptos*”(disembunyikan) dan “*logos*” (ilmu) yang artinya adalah ilmu dari penulisan-penulisan rahasia, dan dokumen-dokumen terenkripsi<sup>7</sup> dengan kata lain kriptologi merupakan kombinasi dari kriptografi<sup>8</sup> (*cryptographie*) dan kriptanalisis<sup>9</sup>(*cryptanalyse*).

<sup>5</sup> Pasal 1 butir 5, RUU ITE.

<sup>6</sup> Eric CAPRIOLI, *Le juge et la preuve électronique*, 10 januari 2000, [www.juriscom.net](http://www.juriscom.net)

<sup>7</sup> Julius SINGARA, *Memoire : la cryptologie et la preuve électronique de la France à l'Indonésie*, D.E.A. Informatique et Droit, Université Montpellier I, année universitaire 2003-2004, Montpellier, h. 13.

Teknik kriptologi bukanlah sebuah teknik baru, ia telah digunakan sejak jaman Julius Cesar, tetapi pada jaman ini, teknik kriptologi yang digunakan masih konvensional. Pengkodean pesan rahasia yang digunakan adalah algoritma yang berasal dari penggeseran abjad-abjad. Kunci rahasia untuk mendekripsi pesan rahasia ini adalah jumlah karakter yang digeser. Contohnya, kata "LQGRQHVL D" merupakan kata rahasia dari INDONESIA, sehingga hanya orang-orang yang mengetahui kunci "penggeseran 3 huruf" yang dapat mengerti tulisan tersebut.

Tentunya di jaman teknologi informasi ini, teknik kriptologi modern yang digunakan. Berkaitan dengan keamanan pesan rahasia, teknik kriptologi modern menjamin sedikitnya lima keamanan minimal, yaitu<sup>10</sup> :

- (a) Keotentikan (*l'authenticité*), penerima pesan harus mengetahui siapa pengirim pesan tersebut dan harus benar-benar yakin bahwa pesan tersebut berasal dari pengirim;
- (b) Integritas (*l'intégrité*), penerima harus yakin bahwa pesan tersebut tidak pernah dirubah, atau dipalsukan oleh pihak beritikad tidak baik;
- (c) Kerahasiaan (*la confidentialité*), pesan tersebut harus tidak dapat dibaca oleh pihak yang tidak berkepentingan;
- (d) Tidak dapat disangkal (*la non repudiation*), pengirim tidak dapat menyangkal bahwa bukan dia yang mengirim pesan tersebut ;
- (e) Kontrol akses (*le contrôle d'accès*), sistem kriptologi mempunyai kemampuan untuk memberikan otorisasi ataupun melarang atas setiap akses ke pesan-pesan tersebut.

Ada dua bentuk kriptologi<sup>11</sup> yang paling dikenal, yaitu kriptologi simetris dan kriptologi asimetris (1.1.1.) tetap hanya bentuk terakhir yang digunakan pada tanda tangan elektronik (1.1.2.).

### **1.1.1. Dua bentuk yang paling dikenal dalam teknik kriptologi**

Kriptografi simetris hanya menggunakan sebuah kunci rahasia untuk mengenkripsi dan mendekripsi sebuah pesan. Salah satu algoritma simetris yang digunakan adalah *Data Encryption Standard* (selanjutnya disebut DES) yang mempunyai panjang kunci 64 bit. Teknik ini sudah semakin ditinggalkan karena tingkat kebocorannya sangat tinggi. Bila kunci rahasia tersebut diketahui oleh pihak ketiga maka dia dapat menggunakannya untuk

---

<sup>8</sup> Kesatuan teknik dari pengkodean/pengenkripsian. M. VIVANT, C. LE STANC, *Lamy Droit de l'Informatique et des Réseaux*, 18ème éd., éd. 2003. éd. Lamy, Paris, 2003, N° 3112, h. 1784.

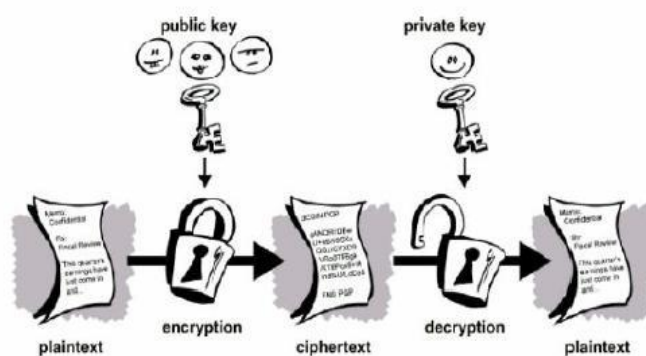
<sup>9</sup> Ilmu yang menganalisa bagaimana memecahkan sebuah tulisan/dokumen terenkripsi menjadi jelas atau dapat diketahui isinya tanpa mengetahui kunci rahasia yang digunakan dalam proses enkripsi. Pretty Good Privacy, *An introduction to cryptographie*, Juni 2004, h. 71.

<sup>10</sup> Julius SINGARA, *op.cit.*, h. 16.

<sup>11</sup> Lihat pula kajian lengkapnya di (bahasa Perancis) Julius SINGARA, *ibid.*, p. 13-25., dan di (bahasa Indonesia) Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan Jakarta dan Lembaga Kajian Hukum Teknologi-Fakultas Hukum Universitas Indonesia (LKHT-UI), *Naskah akademik Rancangan Undang-Undang tentang Tanda Tangan Elektronik dan Transaksi Elektronik*, Laporan penelitian tahap pertama versi 1.04, Jakarta, 2001.

mendekripsi, membaca bahkan memalsukan pesan rahasia tersebut. Untuk keluar dari kesulitan ini digunakanlah sebuah teknik pengkodean yang disebut kriptologi asimetris.

Tahun 1976, dua ahli matematika Diffie dan Hellman memperkenalkan sebuah sistem kriptologi asimetris atau kriptologi kunci publik, teknik ini menggunakan dua buah kunci. Konsep ini kemudian diaplikasikan oleh Rivest, Shamir dan Adleman, dengan membuat sebuah algoritma asimetris RSA pada tahun 1977. Sebuah kunci RSA mempunyai panjang kunci yang bervariasi mulai dari 40 bits hingga 2048 bits<sup>12</sup>. Berkat algoritma ini, Phil Zimmerman mampu membuat sebuah piranti lunak yang diberi nama *Pretty Good Privacy* (selanjutnya disebut PGP). Karena piranti lunak ini didistribusikan secara bebas dan gratis<sup>13</sup> maka penyebaran piranti lunak ini sangat cepat di kalangan pengguna pribadi.



Gambar I : kriptologi asimetris<sup>14</sup>

Proses ini melibatkan dua buah kunci, yang disebut kunci privat dan kunci publik. Kunci privat digunakan untuk mengenkripsi pesan rahasia sedangkan kunci publik digunakan untuk mendekripsi pesan rahasia tersebut agar dapat dibaca. Begitupun sebaliknya, kunci publik digunakan untuk mengenkripsi sebuah pesan rahasia dan kunci privat digunakan untuk mendekripsikan pesan tersebut.

Sekalipun secara matematis, dua kunci ini saling berhubungan tetapi tidak dimungkinkan menemukan kunci privat dengan menggunakan kunci publik<sup>15</sup>, sehingga sangat

<sup>12</sup> Prinsipnya semakin panjang kunci tersebut (semakin besar “bit” dari kunci) maka akan semakin sulit untuk membobol kunci kriptologi. Di Indonesia, panjang kunci ini dapat dibuat sebarang, tetapi tidak di Perancis, Pasal 28 Undang-undang Perancis Nomor 90-1170 tentang reglementasi telekomunikasi yang telah dimodifikasi oleh Undang-undang Nomor 2004-575 tentang kepercayaan dalam perdagangan elektronik, memberikan batasan-batasan yang tegas terhadap panjang maksimum dari sebuah kunci, misalnya untuk keperluan pribadi, panjang kunci 40-128 bits tidak membutuhkan otorisasi pemerintah, bila lebih dari 128 maka membutuhkan otorisasi dari pemerintah (kajian lebih lanjut “*un nouveau régime de la cryptologie : une liberté encore timide*”, lihat di Julius SINGARA, *ibid.*, h. 25-49.)

Untuk saat ini, panjang kunci 128 bits dipandang sudah tepat dan ideal untuk menjamin keamanan dari pesan rahasia tersebut. Panjang kunci yang lebih dari 128 bits, misalnya 256 bits, justru tidak menguntungkan bagi penggunanya. Lihat juga estimasi membobol kunci kriptologi di Grup Riset Digital Security and Electronic Commerce, *Kerangka hukum digital signature dalam e-commerce*, Fakultas Ilmu Komputer Universitas Indonesia, Jakarta, 1999.

<sup>13</sup> Kunjungi : <http://www.pgpi.org/products/pgp/versions/freeware/>

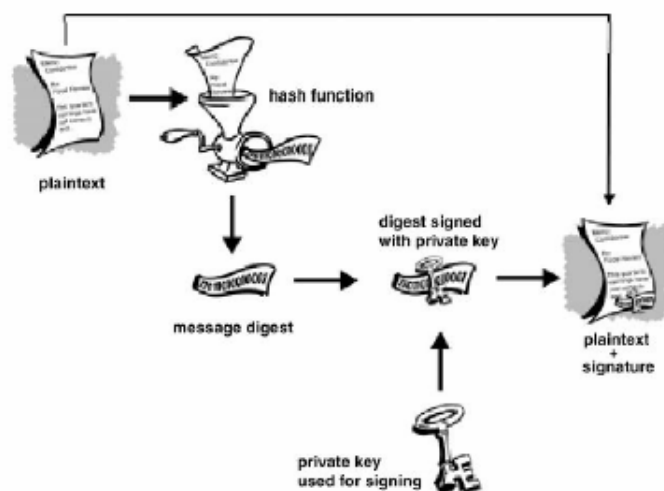
<sup>14</sup> Gambar diambil dari *Pretty Good Privacy*, *op.cit.*, h. 13.

<sup>15</sup> Sebaliknya, kunci publik berasal dari kunci privat sehingga ia dapat dibuat lagi bila kunci publik tersebut hilang.

dimungkinkan untuk mendistribusikan seluas-luasnya kunci publik. Namun sebaliknya, kunci privat harus disimpan dan dijaga kerahasiaannya. Teknik kriptologi asimetris ini merupakan dasar dari pembuatan tanda tangan elektronik.

### 1.1.2. Proses tanda tangan elektronik

Untuk menandatangani secara elektronis sebuah pesan, dengan bantuan piranti lunak, pengirim akan membuat pertama-tama sebuah *message digest*<sup>16</sup> dari pesan yang asli dengan menggunakan *fonction de hachage*<sup>17</sup> (*hash* dalam bahasa Inggris). *Message digest* dari setiap pesan asli adalah unik layaknya “sidik jari”, sehingga perubahan sekecil-kecilnya pada sebuah *message digest* akan mengakibatkan perubahan “sidik jarinya” pula. Keuntungannya, baik sang Pengirim maupun Penerima dapat mengetahui keintegritasan pesan tersebut.



Gambar II : Tanda tangan elektronik<sup>18</sup>

Selanjutnya *message digest* tersebut akan ditanda tangani dengan menggunakan kunci privat pengirim, dengan kata lain tanda tangan elektronik adalah *message digest* yang dienkripsi oleh kunci privat Pengirim. Kemudian pesan asli dan tanda tangan elektronik dikirim bersama-sama ke tujuan yang diinginkan. Berkat kunci publik dari Pengirim yang dikomunikasikan terlebih dahulu ke penerima pesan, Penerima dapat mendekripsi tanda tangan elektronik tersebut, katakanlah hasilnya D1, selanjutnya penerima akan membuat *message digest* pada pesan asli yang diterima, katakanlah hasilnya D2. Maka langkah terakhir adalah membandingkan keduanya, yaitu D1 dan D2. Bila keduanya memiliki “sidik jari” yang sama, maka dapat dipastikan bahwa itu pesan asli dan belum pernah dirubah (lihat lampiran I dan II tentang penggunaan tanda tangan elektronik). Sekalipun begitu, proses ini tidak dapat mengotentifikasi identitas penulis pesan tersebut.

<sup>16</sup> Merupakan “DNA” dari pesan asli. bila terjadi perubahan satu karakter saja maka “DNA” nya akan berubah, dengan kata lain, satu pesan akan mempunyai satu “DNA” unik.

<sup>17</sup> Algoritma yang digunakan antara lain, *Secure Hash Algorithm-1* (selanjutnya disebut SHA-1) atau *Message Digest 5* (selanjutnya disebut MD-5).

<sup>18</sup> Gambar diambil dari *Pretty Good Privacy, op.cit.*, h. 18.

### **1.2. Pengidentifikasian penulis akta elektronik**

Pasal 13 ayat (1) butir (a) dan (b) RUU ITE menentukan sebagai berikut :

- (a) Data pembuatan tanda tangan terkait hanya kepada Penandatanganan saja;
- (b) Data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penandatanganan;
- (c) [...]
- (e) Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangannya;
- (f) Terdapat cara tertentu untuk menunjukkan bahwa Penandatanganan telah memberikan persetujuan terhadap informasi elektronik yang terkait.

Ketentuan-ketentuan Pasal 13 merupakan syarat-syarat minimal<sup>19</sup> yang harus dipenuhi sebuah tanda tangan elektronik sebelum menikmati “asas praduga kehandalan” (*présomption de fiabilité*) yang memberikan kekuatan hukum dan akibat hukum yang sama dengan tanda tangan manuskrip. Menurut Penulis, penggunaan kata “data pembuatan tanda tangan elektronik” hendaklah disederhanakan menjadi “tanda tangan elektronik”, agar lebih jelas dan mudah dimengerti karena tidak ada tanda tangan elektronik tanpa data.

Selain itu, menurut Penulis, butir (f) sebaiknya dihapus karena dari sudut pandang teknis, butir (e) sudah cukup untuk membuktikan bahwa Penandatanganan telah memberikan persetujuannya dengan menandatangani akta elektronik tersebut dengan tanda tangan elektronik miliknya. Namun, untuk membuktikan apakah persetujuan Penandatanganan tersebut datang tanpa unsur paksaan, digunakanlah fakta-fakta hukum dalam proses peradilanlah, bukan piranti lunak yang digunakan.

Kesempurnaan prosedur identifikasi Penandatanganan sangat penting dalam penggunaan tanda tangan elektronik. Jika Hakim meragukan kehandalan prosedur ini, maka ia akan menolak secara tegas validitas dari akta elektronik yang ditandatangani secara elektronis. Pengidentifikasian Penandatanganan dari sebuah akta elektronik dan hubungan antara kunci publik dan subyek hukum membutuhkan bantuan dari pihak ketiga yaitu, Penyelenggara Sertifikasi Tanda Tangan Elektronik (1.2.2.) dengan bantuan sebuah sertifikat elektronik (1.2.1.).

#### **1.2.1. Sertifikat elektronik**

Sertifikat elektronik menduduki peran layaknya “paspor elektronik”, ia tidak dapat dipisahkan dari praktek tanda tangan elektronik, ia membawa kekuatan hukum yang kuat karena dapat meyakinkan identitas Penandatanganan. Sertifikat elektronik mempunyai sebuah struktur internal, artinya ada beberapa bagian yang diwajibkan untuk diinformasikan atau dilekatkan pada sertifikat tersebut untuk memberikan kekuatan hukum pada sertifikat tersebut<sup>20</sup>.

<sup>19</sup> Syarat-syarat ini akan diatur lebih lanjut di Peraturan Pemerintah berdasarkan Pasal 13 ayat (2) RUU ITE.

<sup>20</sup> Julien ESNAULT, *Memoire : la signature électronique*, D.E.S.S. du droit du Multimédia et de l'Informatique, Université de Paris II Pantheon-Assas, Paris, Année universitaire 2002-2003, h. 11.

Struktur internal ini didefinisikan oleh sebuah norma internasional yang disebut *recommendation X-509 V.3 de l'Union internationale des télécommunications*. Norma internasional ini kemudian dikembangkan oleh *Internet Engineering Task Force* untuk diaplikasikan pada teknologi tanda tangan elektronik. Sebuah sertifikat elektronik, menurut norma X-509 V.3 hendaknya memuat minimal keterangan-keterangan sebagai berikut :

- (a) Versi sertifikat;
- (b) Nomor seri sertifikat;
- (c) Algoritma yang dipergunakan;
- (d) Nama pemilik sertifikat digital, termasuk didalamnya keterangan tentang negara asal, organisasi dan seterusnya;
- (e) Nama lembaga yang menerbitkan sertifikat elektronik;
- (f) Ektensi, disesuaikan dengan kebutuhan.

RUU ITE tidak mempresisikan keterangan-keterangan apa saja yang harus dimuat dalam sebuah sertifikat elektronik, tetapi RUU menyerahkan kepada Peraturan Pemerintah untuk menentukan lebih lanjut mengenai penyelenggaraan sertifikasi elektronik<sup>21</sup>.

Namun ada baiknya kita “melirik” Dekrit Komisi Negara Perancis 2001-272 tanggal 30 Maret 2001 tentang “aplikasi Pasal 1316-4 *Code civil* dan tentang tanda tangan elektronik”. Pasal 6 dekrit ini menentukan keterangan-keterangan yang harus dimuat dalam sebuah sertifikat elektronik terqualifikasi adalah sebagai berikut :

- (a) Keterangan yang mengindikasikan bahwa sertifikat ini dikeluarkan sebagai sertifikat elektronik terqualifikasi;
- (b) Identitas dari Penyelenggara Sertifikasi Tanda Tangan Elektronik serta Negara di mana ia berada;
- (c) Nama Penandatanganan atau nama aliasnya, disertai dengan bukti-bukti identitas Penandatanganan ;
- (d) Bila keadaan memungkinkan, keterangan kualitas si Penandatanganan sesuai dengan penggunaan daripada tujuan pemakaian sertifikat elektronik itu ditujukan;
- (e) Data-data pemeriksa kebenaran/keabsahan tanda tangan elektronik yang sesuai dengan data-data pembuatan tanda tangan elektronik;
- (f) Indikasi awal berlaku dan berakhirnya validitas dari sertifikat elektronik;
- (g) Kode identitas dari sertifikat elektronik;
- (h) Tanda tangan elektronik “*sécurisée*”<sup>22</sup> dari Penyelenggara Sertifikasi Tanda Tangan Elektronik yang mengeluarkan sertifikat elektronik tersebut ;

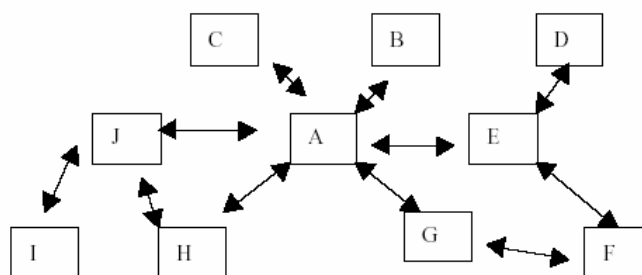
<sup>21</sup> Pasal 16 (2), RUU ITE.

<sup>22</sup> Peraturan perundang-undangan Perancis tentang tanda tangan elektronik membedakan antara tanda tangan elektronik sederhana “*simple*” dengan tanda tangan elektronik “*securisée*”, di mana yang terakhir ini harus memenuhi ketentuan-ketentuan yang ditetapkan oleh dekrit 30 Maret 2001. Tentunya kekuatan pembuktiannya lebih kuat daripada sebuah tanda tangan elektronik sederhana.

- (i) Bila keadaan memungkinkan, disertakan kondisi-kondisi penggunaan sertifikat elektronik, khususnya besarnya transaksi maksimal yang dapat dilakukan dengan menggunakan sertifikat elektronik tersebut<sup>23</sup>.

Sistem sertifikasi tanda tangan elektronik dengan cara-cara di atas memakan biaya yang tidak murah dan tampaknya “hanya” ditujukan kepada kaum profesional saja, sehingga para pengamat berusaha untuk mengurangi biaya tersebut dan memasyarakatkan penggunaan sertifikat elektronik dengan mengembangkan sebuah model sertifikasi yang dikenal dengan nama *web of trust*<sup>24</sup>.

Model sertifikasi *web of trust* yang dikembangkan oleh PGP tidak lain adalah model kepercayaan kumulatif. Dalam sistem ini, setiap orang dapat bertindak sebagai “pemberi sertifikat elektronik”, dan setiap orang dapat mensertifikasi kunci publik dari pengguna lainnya. Cara kerjanya sebagai berikut, I dapat bertransaksi dengan A karena ada jalur kepercayaan melalui J. Sedangkan antara I dan J telah saling mempercayai kunci publik satu dengan yang lainnya, bila J menandatangani kunci publik I maka A dapat mempercayai I<sup>25</sup>.



Gambar III : *web of trust*<sup>26</sup>

Peraturan Pemerintah tentang penyelenggaraan sertifikasi elektronik kelak sebaiknya mengatur secara spesifik mengenai sistem sertifikasi yang digunakan. Penulis bertanya-tanya, bagaimana validitas juridis dari sebuah prosedur identifikasi dengan menggunakan sistem ini? Bagaimanakah pengguna dapat yakin bahwa setiap orang di jaringan ini *capable* untuk menjalankan perannya sebagai “pemberi sertifikat elektronik” ? Bagaimana pengguna bisa

<sup>23</sup> Mengurangi resiko-resiko kepada penerima yang menerima sertifikat elektronik tersebut dan kepada pemberi sertifikat yang dapat diminta pertanggungjawabannya.

<sup>24</sup> *Web of trust* merupakan perpaduan antara model sertifikasi hirarkis “*hierarchial trust tree*” dan *direct end-entity trust*, artikel anonim berbahasa perancis di <http://parodie.com/monetique/signelec>

<sup>25</sup> Lihat pula tentang macam-macam model-model jaringan kepercayaan “*web of trust*” di laporan berbahasa indonesia dari Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan Jakarta dan Lembaga Kajian Hukum Teknologi-Fakultas Hukum Universitas Indonesia (LKHT-UI), *op.cit.* dan thesis berbahasa Perancis dari Julius SINGARA, *La cryptologie et la prevue électronique*, h. 24 dan Pretty Good Privacy, *op.cit.*, h. 27.

<sup>26</sup> Gambar diambil dari Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan Jakarta dan Lembaga Kajian Hukum Teknologi-Fakultas Hukum Universitas Indonesia (LKHT-UI), *ibid.*, h. 44.

yakin atas kebenaran identitas Penandatanganan jika *certification path*<sup>27</sup> telah berada terlalu jauh dari pengguna, misalnya I dan D (lihat gambar III).

Sistem ini memang cukup “berani” tapi masih bersifat “utopi”, dia tidak dapat memberikan jaminan apapun untuk meyakinkan identitas seseorang. Sistem ini juga hanya berjalan di jaringan Internet, sehingga proses sertifikasi ini tidak di bawah kontrol nyata dan serius<sup>28</sup>. Salah satu karakter dari Internet adalah hilangnya perbatasan (*frontier*) suatu negara, sehingga individu-individu yang berperan sebagai “penyelenggara sertifikasi elektronik” dapat berada di negara manapun. Sebaliknya, hukum mengenal *frontier* sehingga bila terjadi sengketa hukum, pihak-pihak yang dirugikan akan menemui kesulitan untuk meminta tanggung jawab individu-individu “penyelenggara sertifikasi elektronik” yang tinggal di luar negeri. Karena hal ini lah, sistem *web of trust* belum diaplikasikan secara menyeluruh di dunia.

Selain itu, Peraturan Pemerintah kelak sebaiknya menegaskan kembali, apakah dapat sebuah perusahaan mempunyai sertifikat elektronik yang dikeluarkan dari perusahaan itu sendiri, artinya ia sekaligus berperan sebagai “Penyelenggara Sertifikasi Tanda Tangan Elektronik”. Contoh konkritnya<sup>29</sup>, P.T. Telkom Indonesia menyediakan jasa penyertifikasian tanda tangan elektronik, apakah dimungkinkan P.T. Telkom sebagai “pemberi sertifikat” mengeluarkan sertifikat elektronik untuk dirinya sendiri ? Seperti yang diketahui, pembuatan sertifikat elektronik diawali dengan kata sepakat (*overeensteming*) dari para pihak atas kewajiban-kewajiban yang melekat dalam sebuah kontrak penggunaan sertifikat elektronik, dalam kasus ini, “para pihak” yang bersepakat adalah P.T. Telkom dengan dirinya sendiri.

Secara yuridis di Perancis, tidak ada larangan pada perusahaan untuk menjadi penyelenggara sertifikasi tanda tangan elektroniknya sendiri, seperti yang didefinisikan, oleh Dekrit 2001-272 tanggal 30 Maret 2001, bahwa penyelenggara sertifikasi elektronik adalah semua entitas atau manusia atau badan hukum yang menerbitkan sertifikat-sertifikat dan yang menyediakan servis-servis yang berkaitan dengan tanda tangan elektronik<sup>30</sup>. Namun, praktek ini beresiko menimbulkan proses pembuktian yang rumit di pengadilan, bahkan akan melemahkan nilainya sebagai alat bukti karena yurisprudensi Perancis, berdasarkan Pasal 1315 *Code civil* Perancis, menegaskan bahwa “tidak seorang pun dapat membuat sebuah bukti atas dirinya”.

Di Indonesia, menurut Penulis, RUU ITE tampaknya tidak mengizinkan praktek tersebut di atas, marilah lihat Pasal 1 butir 8 yang dikatakan penyelenggara sertifikasi elektronik adalah subyek hukum yang berfungsi sebagai pihak ketiga [...] <sup>31</sup>, sedangkan dari sudut pandang *ius constitutum* (hukum positif), P.T. Telkom, berdasarkan ilustrasi di atas,

<sup>27</sup> *The certification path* artinya rantai sertifikasi dari pangkal pemberi sertifikat ke subyek, di mana antara keduanya bisa ada pemberi-pemberi sertifikat lainnya.

<sup>28</sup> Julien ESNAULT, *op.cit.*, h. 14.

<sup>29</sup> Lihat <http://www.telkom.co.id/multimedia/index.asp?menucat=itrust&headcat=>

<sup>30</sup> Pasal 1 butir 11, Dekrit 2001-272 tanggal 30 Maret 2001.

<sup>31</sup> Pasal 1 butir 8, RUU ITE.

tidak dapat mengikatkan diri atas namanya sendiri ataupun meminta ditetapkannya suatu janji dari pada untuk dirinya sendiri<sup>32</sup>.

Seperti yang diuraikan di atas bahwa kombinasi antara teknik kriptologi dan sertifikasi tanda tangan elektronik melahirkan sebuah solusi keamanan yang lebih lengkap dan meyakinkan dalam mengidentifikasi para pihak yang bertransaksi dengan menggunakan akta elektronik dan tanda tangan elektronik. Oleh karena itu, Penulis berharap, Peraturan Pemerintah tentang penyelenggaraan sertifikasi tanda tangan elektronik diatur dengan secara mendalam sehingga terjadi keseimbangan antara jaminan integritas dari sebuah akta elektronik dengan jaminan pengidentifikasian Penandatanganan, yang pada akhirnya akan memberikan kekuatan hukum, berdasarkan asas *présomption de fiabilité*, kepada tanda tangan elektronik.

Peraturan perundang-undangan di Perancis, Malaysia, Singapura maupun RUU ITE mensyaratkan adanya pihak ketiga yang layak dipercaya untuk menerbitkan sertifikat elektronik, pihak ini yang dikenal dengan nama “penyelenggara sertifikasi tanda tangan elektronik<sup>33</sup>”

### **1.2.2. Penyelenggara Sertifikasi Tanda Tangan Elektronik**

Penyelenggara sertifikasi elektronis, menurut RUU ITE, adalah subyek hukum yang berfungsi sebagai pihak ketiga yang layak dipercaya, yang menyelenggarakan tanda tangan elektronik untuk Penandatanganan dan memastikan identitas dan status subyek hukum Penandatanganan tersebut selama keberlakuan tanda tangan elektronik<sup>34</sup>. Definisi ini mengaburkan tujuan utama yang diperankan oleh “penyelenggara sertifikasi elektronis” yaitu menerbitkan sertifikat elektronik atas tanda tangan elektronik, karena identitas dan status subyek hukum Penandatanganan dipastikan ketika diterbitkannya sertifikat elektronik.

Selain tujuan utama ini, penyelenggara sertifikasi elektronis dapat menyediakan pelayanan-pelayanan lainnya yang bertujuan untuk menunjang penyelenggaraan tanda tangan elektronik agar mampu mengikuti evolusi teknologi, misalnya dengan menyediakan jasa “*horodatage*<sup>35</sup>” (dalam bahasa inggris, *time stamping*), jasa pembuatan kunci publik, pengarsipan elektronis<sup>36</sup> dan lain-lainnya. Sehingga, menurut Penulis, lebih tepat Pasal 1 butir

---

<sup>32</sup> Pasal 1315, Kitab Undang-Undang Hukum Perdata.

<sup>33</sup> Prestataire de Service de Certification (bahasa Perancis) atau Certificate Authority (bahasa inggris).

<sup>34</sup> Pasal 1 butir 8, RUU ITE.

<sup>35</sup> Sebuah teknik untuk membubuhkan keterangan waktu pada dokumen elektronik. Teknik ini merupakan salah satu teknik untuk mengetahui waktu terjadinya kesepakatan dalam kontrak. Dokumen-dokumen yang telah ditandatangani secara elektronis dikirim ke *server* utama dari *horodatage* (dalam bahasa inggris, *time stamp server*). *Server* ini sendiri yang akan memberikan keterangan waktu yang tepat pada dokumen-dokumen tersebut. Lihat pula “*les incertitudes sur les dates des actes électroniques*” di Julius SINGARA, *op.cit.* h. 80.

<sup>36</sup> Berdasarkan peraturan perundang-undangan, akta-akta tertentu harus dikonservasi untuk jangka waktu yang sangat panjang. Pengarsipan akta-akta elektronik harus korespon dengan ide kelangsungan sebuah informasi yang terkandung dalam sebuah akta hukum untuk jangka waktu yang lama. Dengan demikian, harus ada teknik dan media handal untuk meyakinkan bahwa arsip-arsip elektronik ini identik dengan aslinya. Teknik dan media yang dapat digunakan antara lain teknik kriptologi, *Compact*

(8) ini didefinisikan sebagai berikut, “subyek hukum yang berfungsi sebagai pihak ketiga yang layak dipercaya, yang menerbitkan sertifikat elektronik dan yang menyediakan pelayanan-pelayanan yang berkaitan dengan penyelenggaraan tanda tangan elektronik ».

Setelah melihat aspek-aspek teknik dari tanda tangan elektronik, pembahasan ini akan masuk pada aspek-aspek juridis dari tanda tangan elektronik.

## 2. Landasan juridis tanda tangan elektronik

Teknologi-teknologi dan media-media baru semakin luas dipergunakan dalam praktik perdagangan, baik di tingkat nasional maupun di tingkat internasional<sup>37</sup>, sehingga Organisasi-organisasi internasional semakin memikirkan pengakuan hukum terhadap akta terdematerialisasi dan tanda tangan elektronik. Akhirnya, dorongan datang dari Komisi Perserikatan Bangsa-Bangsa untuk hukum dagang internasional (selanjutnya disebut UNCITRAL) yang mengeluarkan *UNCITRAL Model Law on Electronic Commerce* pada tanggal 16 Desember 1996.

*Model law* ini sesungguhnya ditujukan untuk menawarkan model hukum kepada negara-negara yang sudah ataupun belum mempunyai peraturan perundang-undangan terhadap materi ini. Namun *model law* sifatnya bebas, artinya negara-negara dibiarkan bebas mau mengikutinya atau tidak. Berkat *model law* ini, banyak negara di dunia berbenah-benah diri, mereka memandang bahwa hukum pembuktian tradisional tidak mampu lagi beradaptasi dengan model perdagangan elektronik, pemerintahan elektronik serta pertukaran yang terdematerialisasi<sup>38</sup>. Oleh karena itu, sangat dibutuhkannya produk hukum yang bertujuan untuk meningkatkan keamanan dari transaksi-transaksi elektronik melalui jaringan elektronik, serta untuk memberikan pengakuan terhadap kekuatan hukum dari alat bukti elektronik dan tanda tangan elektronik, misalnya Komunitas Eropa dengan *Directive communautaire 1999/93/CE du 13 décembre 1999* tentang “tanda tangan elektronik”, Perancis dengan *Loi du 13 mars 2001* tentang “pengadaptasian hukum pembuktian dalam *Code civil français* terhadap teknologi informasi dan tentang tanda tangan elektronik”, Malaysia dengan *Digital signature act 1997*, Singapura dengan *Electronic transaction act 1998* dan *Electronic signatures in global and National Commerce Act 30 juin 2000*.

Bagaimana dengan Indonesia ? Hukum acara positif Indonesia baik hukum acara perdata maupun hukum acara pidana belum mengakui alat bukti elektronik dan tanda tangan elektronik padahal dalam transaksi perdagangan elektronik, bahkan pemerintahan elektronik,

---

*Disc-Read Only Memory* (CWROM) ataupun *Write-One-Read-Many* (WORM). Penyelenggara pengarsipan elektronis memainkan peran yang penting layaknya penyelenggara sertifikasi tanda tangan elektronik. Hukum positif Indonesia telah mengatur cara peralihan dokumen-dokumen konvensional perusahaan ke dalam media lainnya serta penyimpanannya pada Undang-undang Nomor 8 tahun 1997 tentang dokumen perusahaan. Lihat pula “*la conservation des actes électroniques*” dan “*tiers archiveur*” di Julius SINGARA, *ibid.*, h. 81.

<sup>37</sup> Eric CAPRIOLI, *Le juge et la preuve électronique*.

<sup>38</sup> Sepintas sejarah *la loi 2000-230 du 13 mars 2000*, <http://www.foruminternet.org/documents/lois/lire.phtml?id=21>

secara keseluruhan dilakukan tanpa kertas (*paperless*). Berdasarkan Pasal 164 *Herzien Inlands Reglements* (selanjutnya disingkat HIR) dan 1903 Kitab Undang-undang Hukum Perdata (selanjutnya disingkat KUHPerdata) ada 5 alat bukti, yaitu :

- (a) Bukti tulisan;
- (b) Bukti dengan saksi;
- (c) Persangkaan-persangkaan;
- (d) Pengakuan;
- (e) Sumpah

Bertolak dari ketentuan di atas, jelaslah pengajuan tanda tangan elektronik yang melekat pada akta elektronik di muka pengadilan sebagai alat bukti akan menemukan hambatan dan mengalami proses pembuktian yang rumit, bahkan Hakim dan pihak lawan kemungkinan besar akan menolaknya. Akibatnya, timbul ketidakpastian hukum terhadap akta elektronik dan tanda tangan elektronik, yang ironisnya, berbanding terbalik dengan semakin meluasnya penggunaan akta elektronik dan tanda tangan elektronik dalam transaksi elektronik baik dalam negeri maupun dengan luar negeri.

Revisi hukum pembuktian tentu saja membutuhkan waktu yang tidak singkat, karena itu sambil menunggu disahkannya RUU ITE, maka peranan suatu yurisprudensi tetap sangat dibutuhkan dalam mengisi *recht-vacuum*<sup>39</sup>, seperti yang dikemukakan oleh Van Apeldoorn, “Bilamana sesuatu peraturan yang tercantum dalam keputusan Hakim tetapi diturut, jadi, pada kenyataannya peraturan itu telah menjadi bagian dari keyakinan-hukum umum, yakni apabila tentang soal yang bersangkutan telah ditimbulkan suatu yurisprudensi tetap, maka peraturan itu telah menjadi hukum<sup>40</sup>”.

Yurisprudensi tetap dapat tercipta, asalkan ahli hukum dan ahli teknologi informasi mampu memberikan sesuatu pemahaman yang mendalam kepada masyarakat pada umumnya, dan kepada para Hakim pada khususnya. Pemahaman yang membawa keyakinan bahwa akta elektronik dan tanda tangan elektronik dapat diterima sebagai alat bukti elektronik, dalam artian ia mempunyai kekuatan hukum yang sama dengan alat bukti tradisonal, selama alat bukti elektronik ini menggunakan proses yang handal yang mampu memberikan jaminan secara meyakinkan identitas pembuat/penulisnya dan integritas dari akta elektronik tersebut.

Dalam sub-bab berikut akan dibahas tinjauan juridis baik dari sudut hukum positif maupun *ius constituendum* terhadap pelaksanaan tanda tangan elektronik (2.1.) dan juga pelaksanaan penyelenggara sertifikasi elektronik (2.2.).

## **2.1. Tinjauan juridis tanda tangan elektronik**

### **2.1.1. Tanda tangan elektronik sebagai alat bukti dan kekuasaan Hakim**

<sup>39</sup> Aloysius WISNUBROTO, *Kebijakan hukum pidana dalam penanggulangan penyalahgunaan komputer*, cetakan pertama, Penerbitan Universitas Atma Jaya Yogyakarta, 1999, h. 195.

<sup>40</sup> E. UTRECHT dan Moh. Saleh DJINDANG, *Pengantar dalam hukum Indonesia*, cetakan kesebelas, penerbit P.T. Ichtiar Baru dan Penerbit Sinar Harapan, Jakarta, 1989, h.162, angka 174.

Berdasarkan Pasal 4 ayat (1) RUU ITE, informasi elektronik<sup>41</sup> memiliki kekuatan hukum sebagai alat bukti yang sah, bila informasi elektronik ini dibuat dengan menggunakan sistem elektronik yang dapat dipertanggungjawabkan sesuai dengan perkembangan teknologi informasi<sup>42</sup>. Bahkan secara tegas, Pasal 6 RUU ITE menentukan bahwa “Terhadap semua ketentuan hukum yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli selain yang diatur dalam Pasal 4 ayat (4)<sup>43</sup>, persyaratan tersebut telah terpenuhi berdasarkan undang-undang ini jika informasi elektronik tersebut dapat terjamin keutuhannya dan dapat dipertanggungjawabkan, dapat diakses, dapat ditampilkan sehingga menerangkan suatu keadaan”.

Jika RUU ITE telah menjadi hukum positif, saat itu juga akta elektronik dianggap sama dengan akta konvensional, begitu pula dengan tanda tangan elektronik akan dianggap sama dengan tanda tangan manuskrip. Namun dengan hukum acara perdata yang ada saat ini, apakah akta elektronik dapat dianggap sama dengan alat bukti tertulis klasik ? Apakah kekuatan hukum dari akta elektronik tersebut sama dengan kekuatan hukum alat bukti tertulis dalam acara perdata ?

Sesungguhnya pandangan yang mengatakan tanda tangan elektronik tidak dapat menjadi alat bukti tertulis tidaklah mutlak, karena sangat tidak relevan di jaman teknologi tetap memandang alat bukti tertulis dengan cara pandang tahun 1848 ! Disinilah Hakim dituntut untuk berani melakukan terobosan hukum, karena dia yang paling berkuasa dalam memutuskan suatu perkara dan karena dia juga yang dapat memberi suatu *vonnis van de rechter*<sup>44</sup> yang tidak langsung dapat didasarkan atas suatu peraturan hukum tertulis atau tidak tertulis. Dalam hal ini, Hakim harus membuat suatu peraturan sendiri (*eigen regeling*)<sup>45</sup>. Tindakan seperti ini, menurut Pasal 14 Undang-Undang Nomor 14 Tahun 1970 tentang kekuasaan kehakiman, dibenarkan karena seorang Hakim tidak boleh menolak untuk memeriksa, mengadili dan memutuskan suatu perkara dengan alasan peraturan perundang-undangan yang tidak menyebutkan, tidak jelas, atau tidak lengkap (*asas ius curia novit*). Bila

<sup>41</sup> Penjelasan Pasal 4 ayat 1 RUU ITE menjelaskan bahwa, “Informasi elektronik dapat berupa catatan elektronik, dokumen elektronik, kontrak elektronik, surat elektronik, atau tanda tangan elektronik”.

<sup>42</sup> Pasal 4 ayat (3) RUU ITE.

<sup>43</sup> Ketentuan mengenai informasi elektronik sebagaimana dimaksud dalam ayat (1) dan ayat (3) tidak berlaku untuk :

- (a) pembuatan dan pelaksanaan surat wasiat ;
- (b) pembuatan dan pelaksanaan surat-surat terjadinya perkawinan dan putusnya perkawinan ;
- (c) surat-surat berharga yang menurut undang-undang harus dibuat dalam bentuk tertulis ;
- (d) perjanjian yang berkaitan dengan transaksi barang tidak bergerak;
- (e) dokumen-dokumen yang berkaitan dengan hak kepemilikan; dan
- (f) dokumen-dokumen lain yang menurut peraturan perundang-undangan yang berlaku mengharuskan adanya pengesahan notaris atau pejabat yang berwenang.

Lihat kajian lebih lanjut terhadap Pasal ini di “*des exceptions aux dispositions de l’acte électronique* », Julius SINGARA, *op.cit.*, h.75-79.

<sup>44</sup> Keputusan Hakim.

<sup>45</sup> E. UTRECHT dan Moh. Saleh DJINDANG, *op.cit.*, h. 121.

keputusan Hakim yang memuat *eigen regeling* ini dianggap tepat dan dipakai berulang-ulang oleh Hakim-hakim lainnya, maka keputusan ini akan menjadi sebuah sumber hukum bagi peradilan (*rechtspraak*)<sup>46</sup>.

Dengan dasar-dasar di atas, seorang Hakim diberikan keleluasan untuk menemukan hukum (*rechtsvinding*), baik dengan cara melakukan interpretasi hukum (*wetinterpretatie*), maupun dengan menggali, mengikuti dan memahami nilai-nilai hukum yang hidup dalam masyarakat. Metoda interpretasi yang dapat digunakan dalam pencarian kekuatan hukum dari akta elektronik dan tanda tangan elektronik khususnya adalah interpretasi analogi, interpretasi ekstensif dan interpretasi sosiologis<sup>47</sup>. Metoda interpretasi analogis<sup>48</sup> dilakukan dengan memberi ibarat terhadap suatu kata-kata sesuai dengan asas hukumnya, sehingga suatu peristiwa yang pada awalnya tidak dapat dimasukkan, lalu dianggap sesuai dengan ketentuan peraturan tersebut, misalnya menyambung aliran listrik dianggap mencuri/mengambil aliran listrik sebagaimana yang ditegaskan dalam yurisprudensi tetap *Hoge Raad der Nederlanden* (pengadilan tertinggi di Belanda). Berdasarkan asas konkordansi, pengadilan Indonesia menggunakan yurisprudensi ini untuk menjawab kebingungan Hakim dalam menyelesaikan kasus penyalahgunaan/pencurian listrik<sup>49</sup>.

Berkaitan dengan tanda tangan elektronik, seorang Hakim dapat menggunakan metode interpretasi analogis dengan memperhatikan pandangan dari Pitlo dan definisi yang diberikan oleh *Code civil* Perancis. KUHPerdara dan HIR tidak memberikan definisi yang jelas apa yang dimaksud dengan “tulisan”. Pitlo dalam bukunya *Bewijs en Verjaring naar het Nederlands Burgerlijk Wetboek* mendefinisikannya sebagai berikut “surat sebagai, pembawa tanda tangan bacaan yang berarti, yang menterjemahkan suatu isi pikiran. Atas bahan apa

---

<sup>46</sup> Pasal 21 *Algemene Bepalingen van Wetgeving voor Indonesie* (selanjutnya disingkat AB) menentukan bahwa seorang Hakim dilarang membuat peraturan umum (*arrets de reglement*) sebab hanya lembaga legislatiflah yang membuat peraturan yang berlaku umum. Namun tidak dapat dikatakan bahwa yurisprudensi adalah peraturan umum karena Hakim yang memutuskan suatu perkara dengan menggunakan yurisprudensi tidak karena suatu perintah dari Hakim lainnya untuk tunduk atas yurisprudensi tersebut. Lihat lebih lanjut tentang “yurisprudensi” di E. UTRECHT dan Moh. Saleh DJINDANG, *ibid.*, h. 121-128.

<sup>47</sup> Lihat “Penemuan hukum (*rechtsvinding*) : menentukan mana yang merupakan hukum mana yang tidak” di E. UTRECHT dan Moh. Saleh DJINDANG, *ibid.*, h. 203.

<sup>48</sup> Sesungguhnya penggunaan interpretasi analogi dalam hukum pidana masih mengundang pro-kontra, salah satu alasan yang kontra sebagaimana diungkapkan oleh Lemaire bawah undang-undang pidana tidak boleh ditafsirkan secara analogi, karena pengadilan pidana berwenang membuat keputusan hukum (*rechtsbeslissing*) yang sungguh-sungguh membatasi hak-hak manusia (seperti hukuman mati, hukuman penjara). Membuat keputusan semacam itu, apalagi dalam hal analogi, tidak boleh diadakan menurut kehendak Hakim belaka. Lemaire mengkhawatirkan ada kemungkinan diadakan suatu tindakan Hakim yang sewenang-wenang, apabila Hakim itu diberi wewenang untuk menjalankan undang-undang secara analogi. Sedangkan dari kelompok yang pro, diungkapkan oleh Taverne bahwa peradilan pidana modern, yang bidangnya telah sangat luas dalam suatu masyarakat yang berbelit-belit, tidak dapat menolak analogi. E. UTRECHT dan Moh. Saleh DJINDANG, *ibid.*, h. 401.

<sup>49</sup> Keputusan Hakim kadang-kadang mempunyai kekuatan yang sama dengan kuatnya suatu perubahan undang-undang (*vonnis van de rechter is soms net zo sterk als een wetswijziging*). E. UTRECHT dan Moh. Saleh DJINDANG, *op.cit.*, h. 127.

yang dicantumkannya tanda bacaan ini, adalah tidak penting<sup>50</sup>”, serupa dengan Pitlo, Pasal 1316 *Code civil* Perancis menentukan, “*la preuve littérale, ou preuve par écrit, résulte d’une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d’une signification intelligible, quels que soient leur support et leurs modalités de transmission*” (yang dimaksud dengan alat bukti dengan huruf, atau alat bukti tertulis adalah urutan dari huruf-huruf, tanda-tanda, angka-angka, atau semua tanda-tanda atau simbol-simbol yang dapat difahami, bagaimana pun bentuk medianya, dan bagaimana pun cara transmisinya).

Dengan demikian, terlihat bahwa di mana pun tulisan itu ditulis dapat menjadi alat bukti, selama tulisan tersebut dapat dibuktikan dengan siapa tulisan itu terkait, dan keintegritasannya terjamin. Sehingga, Hakim dapat menganggap bahwa akta elektronik dan tanda tangan elektronik termasuk dalam alat bukti. Penggunaan interpretasi analogis terhadap akta elektronik dan tanda tangan elektronik menuntut Hakim untuk membekali dirinya dengan pengetahuan tentang sistem transaksi elektronik, ataupun mekanisme transaksi elektronik. Referensi-referensi berkaitan dengan alat bukti elektronik sudah mudah dijumpai, dengan semakin berkembangnya doktrin-doktrin<sup>51</sup> dari ahli hukum dan laporan-laporan penelitian mengenai adaptasi hukum pembuktian Indonesia terhadap teknologi informasi

Bentuk interpretasi lainnya adalah interpretasi ekstensif<sup>52</sup> (*extensieve uitleg*), yaitu memberikan suatu penafsiran dengan memperluas arti kata-kata yang terdapat dalam ketentuan-ketentuan undang-undang tersebut, sehingga suatu peristiwa yang tidak dapat dimasukkan menjadi dapat dimasukkan. Berdasarkan metoda ini, makna “tertulis” dalam hukum acara perdata dapat diperluas seperti yang diungkapkan oleh Pitlo di atas.

Menurut Ter Haar, seorang Hakim harus mencari *maatschappelijke werkelijkheid* (realitas kemasyarakatan), oleh karenanya penafsiran undang-undang menurut bahasa harus diakhiri dengan penafsiran sosiologis agar sebuah keputusan Hakim itu sesuai dengan realitas masyarakat<sup>53</sup>. Hukum pembuktian dalam acara perdata yang digunakan saat ini sudah berumur lebih dari satu abad. Sehingga seperti yang dikatakan oleh, E. Utrecht dan Moh. Saleh Djindang, *de positiviteit dekt niet meer de realiteit* (positivitas tidak lagi meliputi realitas). Di jaman ini, pendapat dari Montesquieu bahwa Hakim adalah *la bouche qui*

---

<sup>50</sup> Grup Riset Digital Security and Electronic Commerce, *Kerangka hukum digital signature dalam e-commerce*, Fakultas Ilmu Komputer Universitas Indonesia, Jakarta, 1999.

<sup>51</sup> Secara teori, Hakim tidak terpengaruh oleh doktrin, sangat jarang ada yurisprudensi yang menggunakan doktrin sebagai referensinya, sebaliknya di Spanyol. Namun hal ini tidak berarti bahwa doktrin tidak “menarik” karena sesungguhnya banyak pula Hakim-Hakim yang menggunakan doktrin sebagai referensi khususnya doktrin berkaitan dengan suatu domain khusus/spesial, misalnya domaine hukum dari teknologi baru dan komunikasi. Serge BORRIES, *Jurimetrie*, D.E.A. Informatique et Droit, Université Montpellier I, tahun akademik 2003-2004.

<sup>52</sup> Penjelasan Pasal 4 ayat (1) RUU ITE menjelaskan bahwa, “Informasi elektronik dan dokumen elektronik merupakan alat bukti baik dalam perkara perdata, pidana maupun tata usaha negara dan merupakan perluasan dari alat bukti yang diatur dalam Hukum Acara yang berlaku di Indonesia”.

<sup>53</sup> E. UTRECHT dan Moh. Saleh DJINDANG, *op.cit.*, h. 217.

*prononce les paroles de la loi* (corongnya undang-undang) sudah tidak dapat diterima lagi baik di lingkungan hukum perdata maupun pidana.

Sehingga seorang Hakim harus mencari tujuan sosial baru dari hukum pembuktian, dengan menggali, mengikuti, dan memahami nilai-nilai hukum yang hidup dalam masyarakat<sup>54</sup> saat ini. Penafsiran sosiologis sesungguhnya merupakan suatu alat untuk menyelesaikan perbedaan-perbedaan antara positivitas hukum dan realitas hukum<sup>55</sup>. Dengan metoda penafsiran sosiologis ini, Hakim dapat menafsirkan maksud dari hukum pembuktian tahun 1848 dari sudut pandang hukum pembuktian di abad 21. Dengan demikian, hukum akan tetap dinamis dan mampu mengikuti perkembangan jaman.

Saran terakhir dari Penulis kepada para pengguna akta elektronik dan tanda tangan elektronik dalam bertransaksi melalui jaringan *digital* yaitu memuat sebuah klausula khusus dalam kontrak yang menentukan bahwa para pihak yang terikat pada perjanjian tersebut menyatakan kesepakatannya untuk menerima akta elektronik dan tanda tangan elektronik sebagai alat bukti tertulis yang sah. Klausula ini dimungkinkan dengan berpijak pada asas kebebasan berkontrak, di mana para pihak pada dasarnya dapat membuat perjanjian dengan isi yang bagaimana pun juga, asalkan tidak bertentangan dengan peraturan perundang-undangan yang berlaku dan yang bersifat memaksa (*dwigned recht*).

Pada dasarnya hukum perjanjian dalam hukum perdata merupakan hukum pelengkap (*aanvullendrecht*), artinya bahwa para pihak dapat membuat suatu perjanjian yang menyimpang dari ketentuan-ketentuan undang-undang tentang hukum perjanjian, kecuali beberapa sifat yang memaksa<sup>56</sup>, seperti yang ditentukan oleh Pasal 1338 KUHPperdata, "Semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya" (*pacta sunt servanda*). Dengan demikian, para pihak dapat bersepakat dan menetapkan bahwa akta elektronik atau tanda tangan elektronik yang digunakan dalam bertransaksi digunakan sebagai alat bukti sah, dan perjanjian ini mengikat para pihak dan mempunyai kekuatan hukum seperti halnya undang-undang.

Pencantuman klausula khusus mengenai "pembuktian dengan alat bukti elektronik" telah banyak diterapkan oleh pelaku bisnis terutama sektor perbankan yang menggunakan *internet system banking*. Salah satunya adalah *Internet Banking Bank Central Asia* (selanjutnya disingkat BCA) yang mencantumkan sebuah klausula tentang "pembuktian"

---

<sup>54</sup> Pasal 27, Undang-undang Nomor 14 Tahun 1970 tentang Kekuasaan Kehakiman.

<sup>55</sup> E. UTRECHT dan Moh. Saleh DJINDANG, *loc.cit*.

<sup>56</sup> J. Satrio mengatakan bahwa, "Undang-undang sendiri tidak memberikan patokan yang pasti untuk menetapkan mana undang-undang yang bersifat memaksa dan mana yang bersifat menambah. Pada umumnya orang mentafsirkan dari sebuah ketentuan yang bersangkutan, dihubungkan dengan tuntutan masyarakat. Namun jangan dikira, bahwa ketentuan yang bersifat memaksa dapat langsung dikenali karena adanya ancaman batal terhadap pelanggarannya; kenyataannya, pelanggarannya seringkali hanya mengakibatkan, bahwa tindakan hukum yang bersangkutan dapat dibatalkan, atau dikabulkannya tuntutan pemotongan/*inkorting* (dalam hukum waris) dan lain-lain. Tetapi tindakan hukum yang bersifat melanggar tata-krama yang baik (*goede zeden*) dan ketertiban umum selalu mengakibatkan kebatalan yang mutlak. J. Satrio, *Hukum perikatan : perikatan pada umumnya*, cetakan ke-3, Penerbit P.T. Alumni, Bandung, 1999, h. 37.

yang menentukan bahwa, “(1) setiap instruksi transaksi finansial dari Nasabah yang tersimpan pada pusat data BCA dalam bentuk apapun, termasuk namun tidak terbatas pada catatan, *tape/cartridge, print out* komputer, komunikasi yang ditransmisi secara elektronik antara BCA dan Nasabah, merupakan alat bukti yang sah, kecuali Nasabah dapat membuktikan sebaliknya. (2) Nasabah menyetujui semua komunikasi dan instruksi dari Nasabah yang diterima oleh BCA merupakan alat bukti yang sah meskipun tidak dibuat dokumen tertulis ataupun dikeluarkan dokumen yang ditandatangani<sup>57</sup>”.

## **2.1.2. Pembuktian tanda tangan elektronik**

### **2.1.2.1. Asas praduga kehandalan (*presomption de fiabilité*)**

Sebuah tanda tangan elektronik yang menggunakan prosedur yang handal<sup>58</sup> layak untuk menikmati asas *presomption de fiabilité* yang kelak akan diatur dalam RUU ITE beserta Peraturan Pemerintah tentang tanda tangan elektronik. Peraturan perundang-undangan Perancis tentang tanda tangan elektronik melekatkan asas ini bila tanda tangan elektronik *securisée* (terkualifikasi) tersebut menggunakan teknik kriptologi sesuai dengan kondisi-kondisi yang ditetapkan oleh dekrit dan menggunakan sertifikat elektronik terkualifikasi yang diterbitkan oleh penyelenggara sertifikasi tanda tangan elektronik terakreditasi pemerintah.

Menurut hemat Penulis, tanda tangan elektronik yang kelak akan diatur di Peraturan Pemerintah sesuai dengan wewenang yang akan diberikan Pasal 13 ayat (2) RUU ITE harus memberikan perbedaan antara tanda tangan elektronik *simple* (sederhana) dan tanda tangan elektronik *securisée* (diamankan/terkualifikasi). Jenis terakhirlah yang berhak untuk menikmati *presomption de fiabilité*. Kecuali dibuktikan lain, keuntungan dari asas ini adalah jaminan praduga kehandalan identitas dari pengguna dan integritasnya dengan akta yang dilekatinya. Ketidakkampuan pengguna untuk menikmati asas ini, menciptakan kesulitan kepada mereka dalam membuktikan kehandalan prosedur yang digunakannya. Dari sudut kekuatan hukum dan akibat hukum, jelaslah tipe *securisée* yang akan mendapatkan nilai pembuktian lebih unggul daripada tanda tangan elektronik sederhana.

### **2.1.2.2. Konflik pembuktian tanda tangan elektronik**

Seandainya RUU ITE beserta perangkat pelaksanaannya sudah menjadi hukum positif maka kesulitan Hakim dalam melakukan verifikasi terhadap kehandalan sebuah tanda tangan mungkin akan tereduksi, tetapi realitas mengatakan lain. Jadi untuk saat ini, bagaimana seorang Hakim mampu memverifikasi dan memberikan nilai hukum terhadap kehandalan sebuah tanda tangan elektronik yang digunakan para pihak yang bersengketa ?

Selain seorang Hakim harus melengkapi dirinya dengan pengetahuan berkaitan dengan akta elektronik, tanda tangan elektronik dan cara kerja transaksi elektronik, dia juga

<sup>57</sup> Syarat dan Ketentuan Internet Banking (IB) BCA, [http://www.klikbca.com/website/indo/consumer\\_banking/ib\\_termandcondition.html](http://www.klikbca.com/website/indo/consumer_banking/ib_termandcondition.html)

<sup>58</sup> Menggunakan teknik kriptologi dan sertifikat elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik terakreditasi oleh pemerintah.

dapat meminta pertolongan seorang ahli<sup>59</sup> yang memiliki keahlian khusus di bidang teknologi informasi yang dapat dipertanggungjawabkan secara akademis mengenai pengetahuannya tersebut<sup>60</sup>. Pada hakekatnya “alat” ini merupakan sarana bagi Hakim untuk mencari kebenaran yang hakiki agar dapat menjatuhkan keputusan yang adil<sup>61</sup>. Namun, harus diperhatikan bahwa seorang Hakim tidak terikat untuk mengikuti keterangan tersebut bila berlawanan dengan keyakinannya.

Hukum pembuktian dalam hukum perdata berdasarkan Pasal 1865 KUHPerdata dan Pasal 163 HIR memuat asas “*actori incumbit probatio*”, artinya siapa yang mendalilkan sesuatu dia harus membuktikannya. Sepintas lalu, asas ini sangat mudah diaplikasikan di mana beban pembuktian “selalu” berada pada penggugat. Sesungguhnya dalam praktek, Hakim sering kali kesulitan dalam menjalankan perintah Pasal ini sebab pada dasarnya tidaklah seorang pihak saja yang diwajibkan memberikan bukti, melainkan harus ditinjau dari kasus per kasus, sesungguhnya keadaan yang nyata, menurut Retnowulan Sutantio, “pembuktian itu hendaknya diwajibkan kepada pihak yang sedikit diberatkan<sup>62</sup>”.

Selanjutnya menurut Profesor R. Subekti, S.H. dalam bukunya “Hukum Pembuktian” mengatakan bahwa, “beban pembuktian harus dilakukan dengan adil dan tidak berat sebelah, karena suatu pembagian beban pembuktian yang berat sebelah berarti *a priori* menjerumuskan pihak yang mendapat beban terlalu berat kedalam jurang kekalahan<sup>63</sup>”. Berkaitan dengan beban pembuktian terhadap tanda tangan elektronik, hendaknya dibebankan kepada pihak yang mempunyai alat-alat yang memadai untuk membuktikan bahwa tanda tangan elektronik tersebut dibuat dengan prosedur yang handal dan dapat dipertanggungjawabkan.

## **2.2. Tanggung jawab Penyelenggara Sertifikasi Tanda Tangan Elektronik**

Seperti telah diutarakan pada tulisan-tulisan sebelumnya bahwa penyelenggara sertifikasi tanda tangan elektronik (selanjutnya disingkat PSE) merupakan salah satu pemain kunci dalam sistem tanda tangan elektronik. Dialah yang menerbitkan sertifikat elektronik yang ditujukan untuk mengidentifikasi secara sempurna subyek hukum yang menandatangani secara elektronis sebuah akta elektronik. Selain itu, PSE juga menawarkan jasa pembuatan tanda tangan elektronik dengan penggunaan sebuah prosedur yang handal untuk menjamin

---

<sup>59</sup> Pasal 154 HIR.

<sup>60</sup> Pasal 47 ayat (2) butir h RUU ITE.

<sup>61</sup> R. SOESILO, *RIB/HIR dengan penjelasan*, Politeia, Bogor, 1995, h. 113.

<sup>62</sup> Retnowulan SUTANTIO dan Iskandar OERIPKARTAWINATA, *Hukum acara perdata dalam teori dan praktek*, cetakan ke-8, Penerbit C.V. Mandar Maju, Bandung, 1997, h. 60.

<sup>63</sup> Pembagian beban pembuktian yang tidak adil dapat dianggap sebagai suatu pelanggaran hukum atau undang-undang yang menjadikan alasan bagi Mahkamah Agung untuk membatalkan putusan Hakim di pengadilan rendahan yang bersangkutan. Malikul Adil dalam bukunya yang berjudul “Pembaharuan Hukum Perdata Kita” mengatakan bahwa “Hakim yang insyaf akan arti kedudukannya tidak akan lupa bahwa dalam membagi-bagi beban pembuktian, ia harus bertindak jujur dan sportip, tidak akan membebaskan kepada suatu pihak untuk membuktikan hal yang tidak dapat dibuktikan”. R. SOESILO, *op.cit.*, h. 120-121.

hubungan hukum antara Penandatanganan dengan akta elektronik dan integritas dari akta elektronik tersebut.

Sebelum membahas tanggung jawab PSE maka akan diuraikan terlebih dahulu secara singkat tanggung jawab dari Pengguna tanda tangan elektronik, baik yang diatur oleh RUU ITE<sup>64</sup> maupun yang menjadi kebiasaan dalam transaksi elektronik, yaitu : (1) Pengguna harus memberikan pengamanan yang selayaknya atas tanda tangan elektronik yang digunakannya, pelanggaran dari ketentuan ini akan mengakibatkan tanda tangan elektronik tersebut tidak dapat digunakan sebagai alat bukti; (2) Pengguna harus waspada terhadap penggunaan tidak sah dari data pembuatan tanda tangan oleh orang lain (kewajiban kewaspadaan); (3) Pengguna tanpa menunda-nunda, harus memberitahukan kepada PSE bila tanda tangan elektroniknya dicurigai telah dibobol oleh pihak yang tidak berkepentingan, sehingga PSE akan memblokir sertifikat elektronik terkait dan mempublikasikan ke *Certification Revocation List*<sup>65</sup>; dan (4) Pengguna dilarang menggunakan kunci privat untuk mengambil tindakan-tindakan yang bertentangan dengan undang-undang, kesusilaan dan ketertiban umum.

Tanggung jawab PSE baik dengan Pengguna jasanya (Penandatanganan) maupun terhadap pihak ketiga dapat dituntut berdasarkan ketentuan-ketentuan yang terdapat dalam buku ke-3 KUHPdata, yaitu tuntutan ganti rugi atas dasar *wanprestatie/cidera janji* (2.2.1.) dan tuntutan ganti rugi atas dasar *onrechtmatige daad*<sup>66</sup>(2.2.2.)

### **2.2.1. PSE dan tanggung jawab kontraktual terhadap pemegang sertifikat elektronik**

#### **2.2.1.1. Landasan dari tanggung jawab kontraktual**

PSE mengeluarkan sertifikat elektronik yang bertujuan untuk mengidentifikasi subyek hukum/Penandatanganan elektronis dan mengotentifikasi tanda tangan elektronik tersebut. Sesungguhnya, proses pemberian sertifikasi tersebut diawali dengan kesepakatan (*overeensteming*) antara pengguna dan PSE yang tertuang dalam suatu perjanjian (*overeenkomst*). Adapun asas-asas utama dari hukum perikatan<sup>67</sup> yang termuat dalam buku ke-3 KUHPdata, yaitu : (1) asas kebebasan berkontrak (*liberté contractuelle*), (2) asas konsensual (*consensualisme*), (3) asas *obligatoire*<sup>68</sup> dan (4) asas *pacta sunt servanda*<sup>69</sup>.

<sup>64</sup> Pasal 14 ayat (1) RUU ITE beserta penjelasannya.

<sup>65</sup> Suatu pusat *data base* di mana PSE mengumumkan sertifikat-sertifikat elektronik baik yang masih berlaku maupun yang tidak berlaku, sehingga para pengguna dapat memeriksa apakah sertifikat elektronik mitranya masih berlaku atau sudah tidak berlaku.

<sup>66</sup> Perbuatan melanggar hukum.

<sup>67</sup> Perikatan itu dapat timbul karena perjanjian dan juga karena undang-undang sehingga kata “perikatan” (*verbintenis*) mempunyai arti yang lebih luas dari kata “perjanjian” (*overeenkomst*).

<sup>68</sup> Suatu prinsip yang mengajarkan bahwa jika suatu kontrak telah dibuat, maka para pihak telah terikat, tetapi keterikatannya itu hanya sebatas timbulnya hak dan kewajiban semata-mata, dan haknya belum beralih sebelum dilakukan penyerahan. Munir FUADY, *Hukum kontrak (dari sudut pandang hukum bisnis)*, cetakan ke-2, P.T. Citra Aditya Bakti, Bandung, 2003, h. 50.

<sup>69</sup> Perjanjian itu berlaku sebagai undang-undang dan mengikat bagi para pihak yang memperjanjikan.

Kewajiban-kewajiban yang umumnya<sup>70</sup> harus dipenuhi oleh PSE sebagaimana yang dituangkan dalam perjanjian antara PSE dan pengguna jasa, sebagai berikut :

- (a) PSE harus memastikan keterkaitan suatu tanda tangan elektronik dengan Penandatanganan;
- (b) Menggunakan sistem yang aman dan handal dalam proses pensertifikasian;
- (c) Memastikan sertifikat elektronik dari Pengguna jasa yang telah disahkan. Demi keuntungan dari para Pengguna jasa, sertifikat tersebut dimuat kedalam *Certificate Revocation List*;
- (d) Memastikan pencabutan atau pembekuan sementara sertifikat elektronik, atas persetujuan dari Pemiliknya;
- (e) Memastikan secara presisi waktu diterbitkannya dan dicabutnya sebuah sertifikat elektronik;
- (f) Memperkerjakan para pegawai yang mempunyai pengetahuan, pengalaman dan kualifikasi teknis yang tepat dalam proses pensertifikasian;
- (g) Menggunakan sistem-sistem dan produk-produk yang menjamin keamanan teknik dari sertifikat elektronik dan kriptologi;
- (h) Mengambil semua tindakan yang perlu untuk mencegah pemalsuan sertifikat elektronik;
- (i) Bila PSE sebagai pembuat tanda tangan elektronik dari pengguna jasanya, PSE wajib untuk menjaga kerahasiaan dari data-data yang timbul dari proses pembuatan tersebut dan PSE harus menolak baik untuk menyimpan maupun memproduksi ulang data-data ini;
- (j) Semua informasi-informasi yang terkait dengan sertifikat elektronik harus disimpan secara aman dan terjamin keintegritasannya guna menjadi alat bukti di muka pengadilan;
- (k) Menggunakan sistem pengarsipan sertifikat-sertifikat elektronik yang handal dan yang menjamin :
  - i. Pemasukan dan modifikasi terhadap data-data hanya dilakukan oleh pihak-pihak yang diberikan otorisasi oleh PSE;
  - ii. Akses publik terhadap sertifikat elektronik hanya diijinkan bila Pemegang sertifikat memberikan persetujuannya;
  - iii. Segala perubahan terhadap sistem dapat diketahui;
- (l) Memverifikasi identitas dari subyek hukum di mana sertifikat elektronik diterbitkan untuknya dengan meminta dokumen-dokumen resminya;

---

<sup>70</sup> Kewajiban-kewajiban ini sebagaimana diatur dalam Pasal 6-II tentang “sertifikat elektronik terkualifikasi” *Décret du 30 mars 2001*. RUU ITE sendiri akan mengatur lebih lanjut kewajiban-kewajiban minimal yang harus dipenuhi oleh PSE dan selanjutnya akan diatur lebih mendalam pada Peraturan Pemerintah tentang PSE.

- (m) Ketika sertifikat elektronik tersebut akan diterbitkan, PSE harus memastikan bahwa informasi-informasi yang terkait dengan sertifikat tersebut sudah tepat dan tanda tangan elektronik dari Penandatanganan telah sesuai dengan data-data dari tanda tangan elektronik yang terdapat dalam sertifikat.

Dikatakan *wanprestatie*<sup>71</sup> terhadap kewajiban-kewajibannya, bila PSE melakukan salah satu dari berikut : (1) PSE sama sekali tidak berprestasi, (2) PSE salah berprestasi, dan (3) PSE terlambat berprestasi. Akibat hukumnya berdasarkan Pasal 1246 KUHPerdara, Pemegang sertifikat elektronik yang diterbitkan PSE berhak untuk menuntut penggantian kerugian yang berupa biaya-biaya, kerugian dan bunga<sup>72</sup>. Namun, penggantian kerugian ini baru mulai diwajibkan, apabila PSE telah dinyatakan lalai memenuhi perjanjiannya, tetap melalaikannya, atau sesuatu yang harus diberikan atau dibuatnya, hanya dapat diberikan yang harus diberikan atau dibuatnya, hanya dapat diberikan atau dibuat dalam tenggang waktu yang telah dilampaukannya<sup>73</sup>.

#### **2.2.1.2. Beban Pembuktian**

Beban pembuktian dalam hukum perdata secara umum adalah siapa yang mendalilkan sesuatu dia harus membuktikannya (*actori incumbit probatio*). Sehingga secara sepintas dikatakan bahwa beban pembuktian dibebankan kepada pihak penggugat. Bila pemegang sertifikat sebagai penggugat dan PSE sebagai tergugat maka pemegang sertifikatlah yang dibebankan untuk membuktikan dalil-dalilnya. Namun, apakah harus demikian ?

Sesungguhnya beban pembuktian harus dibagi secara merata, artinya seorang Hakim tidak boleh membebankan beban pembuktian ke pihak untuk membuktikan hal yang tidak dapat dia buktikan. Bila beban pembuktian tetap dijatuhkan kepada pengguna jasa maka sama seperti penumpang kereta api sebagai penggugat harus membuktikan adanya *technical error* ataupun *human error* yang mengakibatkan kecelakaan kereta api tersebut<sup>74</sup>, apakah tidak

<sup>71</sup> *Wanprestatie* dapat timbul karena adanya (1) kesengajaan atau kelalaian dan (2) keadaan memaksa (*overmacht*). Menurut R. Setiawan yang dimaksud dengan keadaan memaksa adalah, "Suatu keadaan yang terjadi setelah dibuatnya persetujuan, yang menghalangi debitur untuk memenuhi prestasinya, di mana debitur tidak dapat dipersalahkan dan tidak harus menanggung resiko serta tidak dapat menduga pada waktu persetujuan dibuat. Kesemuanya itu sebelum debitur lalai untuk memenuhi prestasinya pada saat timbulnya keadaan tersebut". R. SETIAWAN, *Pokok-pokok hukum perikatan*, cetakan ke-4, Binacipta, Bandung, 1987, h. 27 sebagaimana yang dikutip oleh P.N.H. Simanjuntak, *Pokok-pokok hukum perdata Indonesia*, Djembatan, Jakarta, 1999, h. 344.

<sup>72</sup> Menurut ketentuan Pasal 1246 KUHPerdara, ganti kerugian itu terdiri dari tiga unsur, yaitu : biaya, rugi dan bunga. Namun tidak semua kerugian dapat dimintakan penggantianannya. Undang-undang menentukan bahwa kerugian yang harus dibayar oleh debitur kepada kreditur sebagai akibat dari wanprestasi adalah sebagai berikut : (1) kerugian yang dapat diduga ketika perjanjian dibuat (Pasal 1247 KUHPerdara) dan (2) Kerugian sebagai akibat langsung dari wanprestasi (Pasal 1248 KUHPerdara). P.N.H. SIMANJUNTAK, *ibid.*, h. 340-343. Baca lebih lanjut tentang "Bab V : Prestasi dan Wanprestasi" dan "Bab VI : Akibat wanprestasi", J. SATRIO, *Hukum perikatan : perikatan pada umumnya*, cetakan ke-3, Penerbit P.T. Alumni, Bandung, 1999.

<sup>73</sup> Pasal 1243 KUHPerdara.

<sup>74</sup> Undang-undang Nomor 13 Tahun 1992 tentang Perkeretaapian menganut prinsip pertanggungjawaban berdasarkan kesalahan (Pasal 28 ayat (1)). Julius SINGARA, *Skripsi : Tanggung*

sama saja Hakim menggiring penggugat ini kedalam kekalahan ? Dari sudut kemampuan teknis dan peralatan teknis, apakah para penggugat tersebut *capable* membuktikan dalil-dalil mereka ?

Sehingga menurut Penulis, tanggung jawab yang melekat pada PSE seharusnya adalah “tanggung jawab karena praduga” (*responsabilité pour faute présumée*), bukan tanggung jawab karena kesalahan (*responsabilité pour faute prouvée*). Prinsip tanggung jawab karena praduga telah diterapkan oleh Perancis dalam sebuah undang-undang, yaitu *la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* (undang-undang untuk kepercayaan dalam perdagangan elektronik, selanjutnya disebut la LEN) menentukan bahwa, “Setiap subyek hukum penyelenggara sertifikat elektronik atau penyedia jasa-jasa lainnya yang terkait dengan penyelenggaraan tanda tangan elektronik dianggap bertanggungjawab atas kerugian yang disebabkan kepada orang lain yang mempercayai sertifikat elektronik yang diterbitkan olehnya (PSE)<sup>75</sup>”.

Dengan prinsip tersebut di atas, beban pembuktian jatuh pada PSE untuk membuktikan ketiadaan unsur kelalaian (*absence de faute*) mereka dalam memenuhi perjanjiannya. Kiranya RUU ITE beserta Peraturan Pemerintah tentang penyelenggaraan sertifikasi elektronik memuat prinsip ini demi meringankan kesulitan para pengguna jasa PSE khususnya dalam hal pembuktian dengan alat bukti elektronik.

### **2.2.2. PSE dan tanggung jawab deliktual terhadap pihak ketiga**

Perjanjian yang disepakati antara PSE dan pengguna jasanya (Penandatanganan) dapat mengakibatkan kerugian kepada pihak ketiga<sup>76</sup>, tetapi karena ketiadaan hubungan kontraktual antara PSE dan pihak ketiga maka pihak ketiga hanya dapat menuntut ganti rugi kepada PSE atas dasar *onrechtsmatige daad* (perbuatan melanggar hukum) yang tidak lain adalah suatu perikatan yang dilahirkan karena undang-undang (Pasal 1353 KUHPerdara).

*Onrechtsmatige daad* diatur dalam Pasal 1365 KUHPerdara, “Tiap perbuatan melanggar hukum, yang membawa kerugian kepada seorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut”. Selanjutnya dalam Pasal 1366 KUHPerdara, menentukan bahwa, “Setiap orang bertanggungjawab tidak saja untuk kerugian yang disebabkan perbuatannya, tetapi juga untuk kerugian yang disebabkan kelalaian atau kurang hati-hatinya” dan Pasal 1367 ayat (1) menegaskan bahwa “Seorang tidak saja bertanggung jawab untuk kerugian yang disebabkan perbuatannya sendiri, tetapi juga untuk kerugian yang disebabkan perbuatan orang-orang yang menjadi tanggungannya atau disebabkan oleh barang-barang yang berada di bawah pengawasannya”.

---

*jawab P.T. Kereta Api Indonesia terhadap kecelakaan kereta api di Cirebon*, Universitas Surabaya, Surabaya, 2002, h. 16.

<sup>75</sup> La LEN, Pasal 33 yang merupakan transposisi dari Pasal 6 ayat (2) dari *Directive communautaire 1999/93/CE du 13 décembre 1999*.

<sup>76</sup> Merupakan pihak yang bertransaksi melalui elektronik dengan Penandatanganan/pengguna jasa sertifikasi tanda tangan elektronik dari PSE (pihak yang mempunyai hubungan kontraktual dengan PSE).

Ketentuan ganti rugi yang harus dibayar karena adanya perbuatan melanggar hukum tidak diatur dalam KUHPerdata, melainkan yang diatur hanyalah ganti rugi akibat *wanprestatie*. Namun, yurisprudensi Mahkamah Agung menegaskan bahwa, “Kerugian yang timbul karena *onrechtmatige daad* ketentuannya sama dengan kerugian yang timbul karena *wanprestatie* dalam perjanjian, ketentuan tersebut diberlakukan secara analogis<sup>77</sup>”.

Berkaitan dengan beban pembuktian, kembali lagi seperti pembahasan-pembahasan sebelumnya bahwa pada umumnya beban pembuktian jatuh kepada penggugat untuk membuktikan unsur-unsur perbuatan melanggar hukum yang dilakukan oleh tergugat. Unsur-unsur ini terdiri dari<sup>78</sup> : (1) perbuatan itu harus melawan hukum, (2) perbuatan itu harus menimbulkan kerugian, (3) perbuatan itu harus dilakukan dengan kesalahan dan (4) perbuatan itu harus ada hubungan kausal.

Namun dalam hal beban pembuktian, menurut Penulis, sistem beban pembuktian yang digunakan terhadap PSE seharusnya adalah prinsip “praduga kesalahan” (*presomption de faute*). Dengan demikian, kesulitan pihak ketiga dalam hal membuktikan unsur-unsur tersebut terutama dengan menggunakan alat bukti elektronik dapat diringankan karena PSE-lah yang mempunyai kemampuan teknis dan peralatan teknik untuk membuktikan kehandalan dan keamanan prosedur yang mereka gunakan.

### **Kesimpulan**

Pada akhir dari tulisan ini, Penulis menyimpulkan bahwa penggunaan teknik kriptologi dan sertifikat elektronik merupakan salah satu cara yang aman untuk melindungi keotentikan, keintegrasian dan kerahasiaan suatu akta elektronik terutama dalam transaksi elektronik. Namun alangkah baiknya, bila ada suatu peraturan perundang-undangan yang mengatur secara khusus pemanfaatan teknik kriptologi yang menjamin kerahasiaan suatu pesan demi menghindari penyalahgunaannya<sup>79</sup>, di mana peraturan perundang-undangan ini mewajibkan untuk melaporkan kepada Badan Pengawas dan/atau Lembaga Sandi Negara terhadap segala bentuk enkripsi atau penyandian atau teknik kriptologi yang digunakan oleh PSE ataupun penyedia jasa lainnya bahkan termasuk Pemakai pribadi.

Akta elektronik dan tanda tangan elektronik dapat diakui mempunyai kekuatan hukum dan akibat hukum yang sama dengan akta dan tanda tangan manuskrip dengan kondisi bahwa subyek hukum terkait akta elektronik dan tanda tangan elektronik ini harus dapat diidentifikasi dengan sangat meyakinkan, serta akta elektronik dan tanda tangan elektronik ini dibuat dan disimpan dalam kondisi yang menjamin keintegritasannya.

---

<sup>77</sup> Abdulkadir MUHAMMAD, *Hukum perikatan*, cetakan ke-4, Citra Aditya Bakti, Jakarta, 1992, h. 146.

<sup>78</sup> P.N.H. SIMANJUNTAK, *op.cit.*, h. 353-354.

<sup>79</sup> Saat ini jaringan teroris internasional menggunakan pesan-pesan rahasia yang terenkripsi dengan teknik kriptologi untuk saling berkomunikasi, akibat dari penggunaan teknik ini, badan-badan intelijen Negara akan mengalami kesulitan untuk melacak atau mencegah serangan-serangan terencana dari jaringan teroris internasional, misalnya serangan 11 September 2000 terhadap World Trade Center Amerika, di mana sebelum serangan tersebut para pelakunya saling berkomunikasi dengan pesan-pesan terenkripsi.

Hakim tidak boleh menolak untuk memeriksa, mengadili dan memutuskan suatu perkara hanya karena akta elektronik dan tanda tangan elektronik belum diatur oleh peraturan perundang-undangan (*ius curia novit*). Namun, Hakim wajib untuk menginterpretasi sesuatu yang tidak terang agar menjadi terang dengan mendasarkan interpretasi tersebut terhadap hal-hal yang dapat diterima dengan akal atau terhadap nilai-nilai hukum yang hidup dalam masyarakat (*semper in obscuris inspicere debet quod versimilis est aut quod plerumque fieri solet*).

Berkaitan dengan tanggung jawab yang melekat pada PSE maka RUU ITE ataupun Peraturan Pemerintah tentang PSE kelak hendaknya menggunakan sistem tanggung jawab atas kesalahan (*responsabilité pour faute présumée*), dengan demikian akan mengurangi kesulitan penggugat, yang pada umumnya adalah orang awam, dalam membuktikan dalil-dalilnya dengan menggunakan alat bukti elektronik, misalnya tanda tangan elektronik.

### **Daftar Pustaka**

#### **Buku hukum dibidang hukum informatika**

WISNUBROTO, Aloysius, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer*, Yogyakarta : Penerbitan Universitas Atma Jaya Yogyakarta, 1999, 331 halaman.

SJAHPUTRA, Iman *Problematika Hukum Internet Indonesia*, Jakarta: P.T. Prenhallindo, 2002, 199 halaman.

VIVANT, Michel dan Christian LE STANC, *Lamy Droit de l'Informatique et des Réseaux : Informatique, Multimedia, Réseaux, Internet*, Paris : LAMY, 2003, 2073 halaman.

#### **Buku hukum umum**

FUADY, Munir, *Hukum Kontrak : dari Sudut Pandang Hukum Bisnis*, Bandung : Citra Aditya Bakti, 2003, 278 halaman.

KANSIL, C.S.T., dan Christine S.T. KANSIL, *Modul Hukum Perdata Termasuk Asas-asas Hukum Perdata*, Jakarta : Pradnya Paramita, 2000, 305 halaman.

SATRIO, J., *Hukum Perikatan : Perikatan pada Umumnya*, Bandung : Penerbit Alumni, 1999, 376 halaman.

SIMANJUNTAK, P.N.H., *Pokok-pokok Hukum Perdata Indonesia*, Jakarta : Penerbit Djambatan, 1999, 391 halaman.

SUTANTIO, Retnowulan dan Iskandar OERIPKARTAWINATA, *Hukum Acara Perdata dalam Teori dan Praktek*, Bandung : C.V. Mandar Maju, 1997, 456 halaman.

#### **Skripsi, Thesis dan Penelitian**

DIMITRIOU, Philippe, *L'application du Droit de la Cryptologie en Matière de Sécurité des Réseaux Informatiques*, thesis dari D.E.A. Défense Nationale option Sécurité européenne et internationale, Université de Lille 2, September 2002, 124 halaman.

ESNAULT, Julien, *La Signature Electronique*, thesis dari D.E.S.S. Droit du Multimédia et de l'Informatique, Université de Paris II Pantheon-Assas, Tahun akademik 2002-2003, 54 halaman.

Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan Jakarta dan Lembaga Kajian Hukum Teknologi-Fakultas Hukum Universitas Indonesia (LKHT-UI), *Naskah akademik Rancangan Undang-Undang tentang Tanda Tangan Elektronik dan Transaksi Elektronik*, Laporan penelitian tahap pertama versi 1.04, Jakarta, 2001.

Global Internet Policy Initiative-Indonesia : Mas Wigrantoro Roes SETIYADI dan Mirna Dian Avanti SIREGAR dan Indonesia Media Law And Policy Center, *Naskah akademik, Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi*, Jakarta, November 2003, 56 halaman.

SINGARA, Julius I.D., *Tanggung jawab P.T. Kereta Api Indonesia terhadap Korban Kecelakaan Kereta Api di Cirebon*, skripsi dari Fakultas Hukum, Universitas Surabaya, 2002, 47 halaman.

-----, *La cryptologie et la Preuve Electronique de la France à l'Indonésie*, thesis dari D.E.A. Informatique et Droit, Université Montpellier I, Tahun akademik 2003-2004, 95 halaman.

WIBOWO, Arianto Mukti, Edmon MAKARIM, Hendra YURISTIawan, Muhammad AULIA, Leny HELENA, Leo FARAYTODY, dan Patricia GABY K., *Kerangka Hukum Digital Signature dalam Electronic Commerce*, Jakarta : Grup Riset Digital Security and Electronic Commerce, Fakultas Ilmu Komputer Universitas Indonesia, Juni 1999, 45 halaman.

#### Artikel khusus

##### Artikel berbahasa Perancis

CAPRIOLI, ERIC A., *Traçabilité e Droit de la Preuve Electronique*, Droit et Patrimoine, Mei 2001, No. 93, h. 68, 8 halaman.

-----, *Le Juge et la Preuve Electronique*, <http://www.caprioli-avocats.com/>, 10 Januari 2000.

MAMOUN Firaz, Rano Louis XAVIER, Olivier REISCH, Rafaël RIVIERE, Julius SINGARA, Anna TRINH, *La Signature Electronique*, 2004, 10 halaman.

Pretty Good Privacy, *An Introduction to Cryptographie*, 2004, 84 halaman.

##### Artikel berbahasa Indonesia

KHAIRANDY, Ridwan, *Pengakuan dan Keabsahan Digital Signature dalam Perspektif Hukum Pembuktian*, Jurnal Hukum Bisnis, Jakarta : Yayasan Pengembangan Hukum Bisnis, Maret 2002, No. 18, h. 31, 9 halaman.

RAMLI, Ahmad M., *Perlindungan Hukum Terhadap Konsumen dalam Transaksi E-Commerce*, Jurnal Hukum Bisnis, Jakarta : Yayasan Pengembangan Hukum Bisnis, Maret 2002, No. 18, h. 14, 4 halaman.

SJAHDEINI, Sutan Remy, *Sistem Pengamanan E-Commerce*, Jurnal Hukum Bisnis, Jakarta: Yayasan Pengembangan Hukum Bisnis, Maret 2002, No. 18, h. 5, 9 halaman.

**1Lampiran I :**

Pesan ini telah ditandatangani dengan tanda tangan elektronik dari pengirim pesan. Hasil verifikasi dari piranti-lunak PGP menentukan bahwa tanda tangan elektronik ini sah "*Good Signature*". Dengan demikian, penerima pesan mempunyai keyakinan akan keotentikan, dan keintegritasan dari pesan tersebut.

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Julius Indra Dwipayono Singara adalah angkatan 1998 di Fakultas Hukum-Universitas Surabaya

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.1 - not licensed for commercial use: [www.pgp.com](http://www.pgp.com)

iQA/AwUBQY998fFSHuSSJRVrEQLpDQCgymN12xEq50eykD2NEZapVP2ukzQAoKt/  
Pa0DvDp8GcZ2wvTPJXC5rG+a

=MGfz

-----END PGP SIGNATURE-----

**HASIL VERIFIKASI :**

\*\*\* PGP SIGNATURE VERIFICATION \*\*\*

\*\*\* Status: Good Signature

\*\*\* Signer: Julius Singara <[julius\\_singara@yahoo.com](mailto:julius_singara@yahoo.com)> (0x9225156B)

\*\*\* Signed: 08/11/2004 15:08:49

\*\*\* Verified: 08/11/2004 15:09:24

\*\*\* BEGIN PGP VERIFIED MESSAGE \*\*\*

Julius Indra Dwipayono Singara adalah angkatan 1998 di Fakultas Hukum-Universitas Surabaya

\*\*\* END PGP VERIFIED MESSAGE \*\*\*

## Lampiran II

bila "angkatan 1998" dihilangkan/diganti menjadi "angkatan 1970" maka hasil verifikasi dari piranti-lunak PGP menentukan bahwa tanda tangan elektronik ini **tidak sah "Bad Signature"**. Dengan demikian, penerima pesan tidak akan mempunyai keyakinan akan keotentikan, dan keintegritasan dari pesan ini.

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Julius Indra Dwipayono Singara adalah angkatan 1970 di Fakultas Hukum-Universitas Surabaya

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.1 - not licensed for commercial use: [www.pgp.com](http://www.pgp.com)

iQA/AwUBQY998fFSHuSSJRvREQLpDQCgymN12xEq50eykD2NEZapVP2ukzQAoKt/  
Pa0DvDp8GcZ2wvTPJXC5rG+a  
=MGfz

-----END PGP SIGNATURE-----

### **HASIL VERIFIKASI :**

\*\*\* PGP SIGNATURE VERIFICATION \*\*\*

\*\*\* Status: Bad Signature

\*\*\* Alert: Signature did not verify. Message has been altered.

\*\*\* Signer: Julius Singara <[julius\\_singara@yahoo.com](mailto:julius_singara@yahoo.com)> (0x9225156B)

\*\*\* Signed: 08/11/2004 15:08:49

\*\*\* Verified: 08/11/2004 15:11:10

\*\*\* BEGIN PGP VERIFIED MESSAGE \*\*\*

Julius Indra Dwipayono Singara adalah angkatan 1970 di Fakultas Hukum-Universitas Surabaya

\*\*\* END PGP VERIFIED MESSAGE \*\*\*