TINJAUAN YURIDIS TANDA TANGAN DIGITAL PADA AKTA ELEKTRONIK

Mochammad Kusjairi
Fakultas Hukum Universitas Yos Soedarso
e-mail: moch_kusjairi@yahoo.co.id

ABSTRAK

Tanda tangan digital merupakan suatu cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut Tanda tangan digital menggunakan algoritma-algoritma serta teknik-teknik komputer khusus dalam penerapannya. Hal ini diciptakan untuk menjaga otentikasi dari suatu kontrak secara elektronik.

Kata kunci: *tanda tangan digital, digital signature, information authentication, cryptography.*

PENDAHULUAN

Pengertian Tandatangan elektronik menurut UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik adalah : tanda tangan yang terdiri atas Informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

Konvergensi 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 *(borderless)*. La 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 kemudah-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.

Di Indonesia, perkembangan teknologi informasi semakin pesat dan penggunanyapun semakin banyak, tetapi perkembangan ini tidak diimbangi dengan perkembangan produk hukum sehingga timbullah berbagai macam sengketa hukum antara para penggunanya baik di tingkat nasional maupun di internasional. Padahal, kehandalan dan keamanan teknologi informasi hams

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. Dalam perdagangan elektronik tidak terlepas dari masalah dalam pelaksanaannya, permasalahan yang sering timbul antara lain mengenai keabsahan kontrak dalam e commerce (online contract/e contract) serta pembuktian kontrak tersebut apabila terjadi sengketa.[1]

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.

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 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 dan mampu mengidentifikasi si Penandatangan dari akta elektronik ini.

PEMBAHASAN

Pasal 11 UU 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 UU 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 dengan kata lain kriptologi merupakan kombinasi dari

---

1 Dikdik M Arief Mansur, Elisatris Gultom, Aspek Hukum Teknologi Informasi (Cyber law), Refika Aditama, Bandung, 2005, him 172.

2. M. VIVANT, C. LE STANC, *Lamy Droit tie I'lnformotique et des Rtseaux,* 186me ed., e1d. 2003. ed. Lamy, Paris, 2003, N' 3112, h. 1784

3. Pretty Good Privacy, *An introduction to cryptographie,* Juni 2004, h. 71.

kriptografl[2] *(cryptographie)* dan kriptanalis[3] *(cryptanalyse).*

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 penggesaran abjad-abjad. Kunci rahasia untuk mendekripsi pesan rahasia ini adalah jumlah karakter yang digeser.

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. Berkat algoritma ini, Phil Zimmerman mampu membuat sebuah piranti lunak yang diberi nama *Pretty Good Privacy* (selanjutnya disebut PGP). Karena piranti lunak ini didistribusikan secara bebas dan gratis maka penyebaran piranti lunak ini sangat cepat di kalangan pengguna pribadi.

Proses ini melibatkan dua buah kunci, yang disebut kunci privat dan kunci publik. Kunci privat digunakan untuk mengenkripsi pesan rahasia sedangkan kunci 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, sehingga sangat dimungkinkan untuk mendistribusikan seluas-luasnya kunci publik. Namun sebaliknya, kunci privat harus disimpan dan dijaga kerahasiaannya. Teknik kriptologi asimetris ini merupakan dasar dari pembuatan tanda tangan elektronik.

Proses tanda tangan elektronik

Untuk menandatangani secara elektronis sebuah pesan, dengan bantuan piranti lunak, pengirim akan membuat pertama-tama sebuah *message digest* dari pesan yang asli dengan menggunakan *fonction de hachage (hash* dalam bahasa inggris). *Message digest* dari setiap pesan asli adalah unik layaknya "sidik jari", sehingga

---

2

3

perubahan sekecil-kecilnya pada sebuah *message digest* akan mengakibatkan perubahan "sidik jarinya" pula. Keuntungannya, baik sang Pengirim maupun Penerima dapat mengetahui keintegritasan pesan tersebut.

Selanjutnya *message digest* tersebut akan ditanda tangani dengan menggunakan kunci privat pengirim, dengan kata lain tanda tangan elektronik adalah *message digest* yang dienkripsi oleh kunci privat Pengirim. Kemudian pesan asli dan tanda tangan elektronik dikirim bersama-sama ketujuan yang diinginkan. Berkat kunci publik dari Pengirim yang dikomunikasikan terlebih dahulu ke penerima pesan, Penerima dapat mendekripsi tanda tangan elektronik tersebut.

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

(a) Data pembuatan tanda tangan terkait hanya kepada Penandatangan saja;

(b) Data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penandatangan;

(c) […]

(e) Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangannya;

(f) Terdapat cara tertentu untuk menunjukkan bahwa Penandatangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.

Ketentuan-ketentuan Pasal 13 merupakan syarat-syarat minimal yang harus dipenuhi sebuah tanda tangan elektronik sebelum menikmati "asas praduga kehandalan" *(presomption defiabiliti)* 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.

Kesempurnaan prosedur identifikasi Penandatangan 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 Penandatangan dari sebuah akta elektronik dan hubungan antara kunci publik dan subyek hukum membutuhkan bantuan dari pihak ketiga yaitu, Penyelenggara Sertifikasi Tanda Tangan

Elektronik dengan bantuan sebuah sertifikat elektronik.

Sertifikat elektronik

Sertifikat elektronik menduduki peran layaknya "paspor elektronik", ia tidak dapat dipisahkan dari praktek tanda tangan elektronik, ia membawa kekuatan hokum yang kuat karena dapat meyakinkan identitas Penandatangan. Sertiflkat 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.

Sertifikat elektronik, hendaknya memperhatikan empat aspek keamanan yaitu:

1. Informasi yang dipertukarkan hanya bisa dibaca oleh penerima yang berhak dan tidak dapat dipahami oleh pihak yang tidak berhak (privacy/confidentialy).
2. Identitas pihak yang terkait dapat diketahui atau dijamin otentisitasnya (Authentification)
3. Informasi yang dikirim dan diterima tidak berubah (integrity], dan
4. Pihak yang terkait tidak dapat menyangkal telah melakukan transaksi (Non Repudiation).

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, 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 Penandatangan, yang pada akhirnya akan memberikan kekuatan hukum, berdasarkan asas *presomption defiabilite,* kepada tanda tangan elektronik.

Peraturan perundang-undangan di Perancis, Malaysia, Singapura maupun UU ITE mensyaratkan adanya pihak ketiga yang layak dipercaya untuk

menerbitkan sertifikat elektronik, pihak ini yang dikenal dengan nama "penyelenggara sertifikasi tanda tangan elektronik" **Penyelenggara Sertifikasi Tanda Tangan Elektronik**

Penyelenggara sertifikasi elektronis, menurut UU ITE, adalah subyek hukum yang berfiingsi sebagai pihak ketiga yang layak dipercaya, yang menyelenggarakan tanda tangan elektronik untuk Penandatangan dan memastikan identitas dan status subyek hukum Penandatangan tersebut.

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, sehingga Organisasi-organisasi internasional semakin memikirkan pengakuan hukum terhadap akta elektronik dan tanda tangan elektronik. Akhirnya, dorongan datang dari Komisi Perserikatan Bangsa-Bangsa untuk hukum dagang internasional (selanjutnya disebut UNC1TRAL) 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 transaksi elektronik lainnya. 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 decembre 1999* tentang "tanda tangan elektronik", Perancis dengan *Loi du 13 mars 2001* tentang "pengadaptasian hukum pembuktian dalam *Code civil francais* 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. Di Indonesia diatur dalam Pasal 1 butirl2 UUITE mengenai tanda tangan elektronik

Berdasarkan Pasal 4 ayat (1) UU ITE, informasi elektronik 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. Bahkan secara tegas, Pasal 6 UU 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), 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".

Saat ini akta elektronik dianggap sama dengan akta konvensional, begitu pula dengan tanda tangan elektronik dianggap sama dengan tanda tangan manuskrip. 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.

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

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 hubungan hukum antara Penandatangan 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 UU ITE maupun yang menjadi kebiasaan dalam transaksi elektronik, yaitu : (1) Pengguna harus memberikan pengamanan yang selayaknya atas tanda tangan elektronik yang digunakannnya, 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,* dan (4) Pengguna dilarang menggunakan kunci privat untuk mengambil tindakan-tindakan yang bertentangan dengan undang-undang, kesusilaan dan ketertiban umum.

PSE mengeluarkan sertifikat elektronik yang bertujuan untuk mengidentifikasi subyek hukum/Penandatangan 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 yang termuat dalam buku ke-3 KUHPerdata, yaitu : (1) asas kebebasan berkontrak *(liberte contractuelle),* (2) asas konsensual *{consensualisme),* (3) asas *obligatoire* dan (4) asas *pacta sunt servanda.*

Penyelenggaran CA di Indonesia harus memenuhi persyaratan sebagai berikut:

1. Berbentuk badan hukum Indonesia dan beroperasi di Indonesia, serta memiliki izin operasi CA dari Menteri Komunikasi dan Informatika berdasarkan pertimbangan dari BP-CA.
2. Memiliki peran cross border, berarti hukum nasional mengatur keberadaan CA yang ada sebagai subyek hukum di Indonesia dan hukum nasional mengakui eksistensi keberadaan CA internasional yang eksis sesuai hukum tempat domisili CA tersebut
3. Sebagai subyek hukum, *CA* sebagai pihak ketiga terpercaya yang memberikan kepastian/pengesahan identitas pelanggan dan pengesahan pasangan kunci publik dan kuci pribadi.
4. Layanan CA terbuka dan dapat diakses oleh seluruh aplikan (pemohon) yang membutuhkan CA.
5. Independen dan tidak memihak.
6. Memiliki fungsi manajemen dalam sistem operasinya sesuai kriteria SNI yang dipersyaratkan dan memenuhi persyaratan / kesesuaian standar manajemen (ISO/IEC 27001:2005, Information Technology – Security Technique Information Security Management System Requirement, yaitu :
   - *Policy Authority* yang bertanggung jawab menetapkan kebijakan tertulis (Certificate Policy - CP] dan Certification Practise Statement (CPS), serta melakukan *management review* untuk mengevaluasi dan melakukan perbaikan terhadap pelaksanaan CPS;
   - *Registration Authority* yang bertanggung jawab memverifikasi data identitas pemegang sertifikat dan memvalidasi kebenarannya;

- o *Certificate Issuer* bertanggung jawab menerbitkan kunci kriptografi atau memvalidasi kunci kriptografi apabila kunci tersebut diterbitkan oleh pihak lain, serta melaksanakan pembuatan, pembubuhan tandatangan CA dan publikasi serta pemeliharaan SD;
- o *Repository Service* yang bertanggung jawab mempublikasikan CP, CPS, SD dan *revocation status bulletin,* baik melalui repository yang dimiliki oleh CA maupun oleh pihak lain;
- o *Revocation Management* yang bertanggung jawab mengawasi penyalahgunaan SD, menyelidiki kebenaran pengaduan yang diterima, menentukan langkah-langkah yang harus dilakukan sehubungan dengan pembekuan atau pembatalan SD, serta menyusun *revocation status bulletin.*

7. Status personal badan hukum CA tunduk sepenuhnya kepada hukum Indonesia.

8. Personal CA harus orang yang kompeten, memenuhi kualifikasi dan terlatih, bersertifikasi/lisensi untuk kriteria teknis tertentu, menguasai teknis SN1 terkait, komunikatif lisan dan tertolis, bebas dari konflik kepentingan. [4]

Kewajiban-kewajiban yang umumnya 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 Penandatangan;

(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;

(a) Memastikan secara presisi waktu diterbitkannya dan dicabutnya sebuah

---

[4] Pedoman Penyelenggaraan CA, Badan Pengawas CA, Jakarta, 2011, him 2.
Bandung, 2005, him 172.

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 system 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;

(1) Memverifikasi identitas dari subyek hukum di mana sertifikat elektronik diterbitkan untuknya dengan meminta dokumen-dokumen resminya;

(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 Penandatangan telah sesuai dengan data-data dari tanda tangan elektronik yang terdapat dalam sertifikat.

PSEdapat dikatakan *wanprestatie* 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 KUHPerdata, Pemegang sertifikat elektronik yang diterbitkan PSE berhak untuk menuntut penggantian kerugian yang berupa biaya-biaya, kerugian dan bunga. Namun, penggantian kerugian ini baru mulai diwajibkan, apabila PSE telah dinyatakan lalai memenuhi perjanjiannya, tetap melaiaikannya, 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.

Beban pembuktian dalam hukum perdata secara umum adalah siapa yang mendalilkan sesuatu dia harus membuktikannya *(actori incombit 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.

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 *humain error* yang mengakibatkan kecelakaan kereta api tersebut, apakah tidak 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 tanggung jawab yang melekat pada PSE seharusnya adalah "tanggung jawab karena praduga" *{responsabilite pour faute presumee),* bukan tanggung jawab karena kesalahan *{responsabilite pour faute prouvee).* 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 conflance dans I'economie num4rique* (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 disebabkannya kepada orang lain yang mempercayai sertifikat

elektronik yang diterbitkan olehnya (PSE)".

Dengan prinsip tersebut di atas, beban pembuktian jatuh pada PSE untuk membuktikan ketiadaan unsur kelalaian *{absence de faute)* mereka dalam memenuhi perjanjiannya. Kiranya UU 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

Perjanjian yang disepakati antara PSE dan pengguna jasanya (Penandatangan) dapat mengakibatkan kerugian kepada pihak ketiga, 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 KUHPerdata).

Onrechtsmatige daad diatur dalam Pasal 1365 KUHPerdata, "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 KUHPerdata, 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".

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 *onrechtsmatige daad* ketentuannya sama dengan kerugian yang timbul karena *wanprestatie* dalam perjanjian, ketentuan tersebut diberlakukan secara analogis".

Berkaitan dengan beban pembuktian, kembali lagi seperti pembahasan-pembahasansebelumnya bahwa pada umumnya beban pembuktian jatuh kepada

penggugat untuk membuktikan unsur-unsur perbuatan melanggar hukum yang dilakukan oleh tergugat. Unsur- unsur ini terdiri dari : (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

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, 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.

DAFTAR PUSTAKA

Badan Pengawas CA, Pedoman Pelaksanaan dan Pengawasan CA di Indonesia, Jakarta, 2011

Pretty Good Privacy, *An introduction to cryptographie,* Juni 2004

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

WIB0W0, Arianto Mukti, Edmon MAKAR1M, Hendra YURIST1AWAN, 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.

Kitab Undang-Undang Hukum Perdata

Undang-Undang 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.