BAB 5

PENUTUP

5.1. Kesimpulan

Berdasarkan penelitian dan analisis sebagaimana yang diuraikan dalam bab-bab terdahulu dapat dirumuskan kesimpulan sebagai berikut.

1. Di Indonesia, sebelum diundangkannya UU ITE, belum terdapat payung hukum dalam hal pengaturan transaksi elektronik serta tanda tangan elektronik sebagai otentifikasi informasi yang melekat pada sebuah sertifikat elektronik. Sehingga, kemungkinan akan terjadinya sengketa hukum sangatlah besar tanpa adanya landasan hukum yang digunakan dalam proses penyelesaiannya, yang pada akhirnya memaksa hakim untuk melakukan penemuan hukum agar perkara tersebut dapat diselesaikan.
2. UU ITE belum mengatur secara komprehensif mengenai transaksi elektronik khususnya mengenai otentifikasi melalui tanda tangan elektronik. UU ITE hanya mengatur mengenai pengertian umum, persyaratan tanda tangan elektronik yang memiliki kekuatan hukum dan akibat hukum, kewajiban pengamanan bagi pengguna tanda tangan elektronik, dan penggunaan sertifikat elektronik dalam tanda tangan elektronik. Tanda tangan elektronik akan diatur lebih teknis dalam suatu peraturan pemerintah yang sekarang masih dalam sebuah rancangan, yakni Rancangan Peraturan Pemerintah tentang Tanda Tangan Elektronik –perkembangan sekarang materi muatan tanda tangan elektonik, serifikat elektronik, dan penyelanggara sertifikasi elektronik diakumulasi dengan materi muatan UU ITE lainnya ke dalam

RPP tentang Penyelenggaraan Informasi dan Transaksi Elektonik- , sehingga eksistensi PP ini dapat menjadi dasar hukum bagi pelaksanaan tanda tangan elektronik secara lebih teknis dan komprehensif.

3. Selanjutnya peranan tanda tangan elektronik sebagai sarana mewujudkan s*ecure electronic transacation* (SET) di sektor perbankan memiliki peranan penting. *Electronic signature* merupakan salah satu bentuk SET yang digunakan sebagai autentifikasi dan verifikasi suatu informasi elektronik. Agar tercipta SET, maka tanda tangan elektronik tersebut harus diintegrasikan ke dalam sertifikat elektronik yang memuat tanda tangan dan identitas yang menunjukan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik. Penyelenggara sertifikasi elektronik merupakan suatu badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik.

4. SET yang umum digunakankan yakni dengan keberadaan *public key* atau *privat key* pada mesin *web* yang menggunakan skema keamanan tersebut. Komputer yang akan berkomunikasi menggunakan data terenkripsi harus memiliki kunci untuk mengenskripsi data. Meski masalah keamanan sudah ditangani dengan keberadaan *public key* atau *privat key*, masih ada masalah yang perlu diperhatikan lagi, yakni informasi atau data yang diperoleh merupakan data yang sesungguhnya yang dikeluarkan oleh pihak yang memiliki wewenang, bukan dari pihak yang berkepentingan dan menyalagunakan isi dari informasi tersebut. Sehingga dibutuhkan pihak ketiga untuk mengautentifikasi dan memverifikasi informasi yang datang.

Informasi terenskripsi yang dikirim dan diterima akan memiliki tanda tangan elektronik, dan selanjutnya penyelenggara sertifikasi elektronik tersebut melakukan verifikasi. Lembaga ini akan mengeluarkan sertifikat yang memverifikasi informasi, lalu lembaga ini akan memberikan *public key* dan *privat key*. Lembaga sertifikasi elektronik ini misalnya lembaga Verisign, Thawte, dan CaCert.org.

5. Sertifikat elektronik akan menampung tanda tangan elektronik, selain juga menunjukkan status hukum para pihak yang melakukan perbuatan hukum. Melalui sertifikat elektronik inilah jaminan keamanan terhadap suatu informasi elektronik dengan pembubuhan tanda tangan elektronik akan terjaga. Sehingga, hubungan antara sertifikat elektronik dan tanda tanga elektronik erat sekali karena terintegrasi dalam satu kesatuan organ. Sertifikat elektronik ini kemudian diproses dan dikeluarkan oleh suatu certification/certificate authority (CA).
6. CA merupakan sebuah badan hukum yang berfungsi sebagai pihak ketiga (*trusted third party*) yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik serta menyediakan layanan keamanan yang dapat dipercaya oleh pengguna dalam menjalankan pertukaran informasi secara elektonik dan memenuhi 4 (empat) aspek keamanan, yaitu aspek *confidentiality, authentification, integrity,* dan *non repudiation.* CA sebagai *trusted third party* (TTP) di sektor perbankan memiliki peran yang sama dengan CA di luar sektor perbankan. Bank sebagai *subcriber* sama kedudukan hukumnya dengan perorangan atau korporasi yang melakukan

perbuatan hukum dengan menggunakan komputer, jaringan komputer, atau media lainnya secara elektronik.

7. Dalam upaya menanggulangi resiko yang akan timbul dari penggunaan transaksi elektronik, maka Bank Indonesia sebagai bank sentral mengeluarkan peraturan terkait penggunaan teknologi informasi secara umum sebagai bentuk manajemen resiko dalam kegiatan perbankan. Peraturan terkait yakni PBI Nomor 9/15/PBI/2007 mencabut beberapa aturan lainnya di bidang teknologi informasi perbankan, yaitu: SK Dir BI No.27/164/KEP/DIR Tgl.31-3-1995 tentang Penggunaan Teknologi Informasi oleh Bank; SEBI No.27/9/UPPB Tgl.31-3-1995 tentang Penggunaan Teknologi Informasi oleh Bank; SK Dir BI No.31/175/KEP/DIR Tgl.22-12-1998 tentang Teknologi Sistem Bank dalam Menghadapi tahun 2000; SEBI No.31/14/UPPB Tgl.22-12-1998 tentang Penyempurnaan Teknologi Sistem Informasi Bank dalam Menghadapi Tahun 2000; PBI No.1/11/PBI/1999 Tgl.22-12-1999 tentang Fasilitas Khusu dalam Rangka Mengatasi Kesulitan Pendanaan Jangka Pendek bagi Bank Umum yang disebabkan Masalah Komputer Tahun 2000; dan SEBI No.6/18/DPNP Tgl.20-4-2004 tentang Penerapan Manajemen Risiko pada Aktivitas Pelayanan Jasa Bank melalui Internet (*Internet Banking*).
8. Peraturan BI ini mengatur beberapa domain turunan dari teknologi informasi yang relevan dengan perbankan, beberapa pengaturan tersebut di antaranya menejemen risiko teknologi informasi, kebijakan dan prosedur penggunaan teknologi informasi di bank, sistem pengendalian dan audit interen atas

penyelenggaraan teknologi informasi, *electronic banking*, sanksi terhadap pelanggaran pengaturan teknologi informasi di bank.

9. Dari poin-poin tersebut di atas, daya guna penerapan teknologi informasi dalam aspek transaksi elektonik di dunia perbankan yang digunakan melalui tanda tangan elektonik sebagai wujud SET, tentunya akan memiliki hambatan. Hambatan yang utama, diantaranya, hambatan Substansi UU ITE; hambatan hukum di luar UU ITE, yang meliputi: belum adanya peraturan pelaksanaan di bidang tanda tangan elektronik sebagai aturan organis UU ITE dan pertentangan dengan ketentuan peraturan perundang-undangan yang lain; hambatan teknologi; hambatan sosio-kultural (sosial budaya); serta hambatan stabilitas finansial dan keamanan.

5.2. Saran

Berdasarkan penelitian di atas, beberapa hal yang harus dilakukan guna mewujudkan *security electronic transaction* melalui tanda tangan eletronik, maka:

1. Pemerintah perlu menerbitkan peraturan pelaksanaan UU ITE mengenai tanda tangan elektronik dan sertifikat elektronik, yaitu Peraturan Pemerintah tentang Tanda Tangan Elektronik dan Peraturan Pemerintah tentang Sertifikat Elektronik (perkembangan terakhir diakumulasi dalam satu Rancangan Peraturan Pemerintah tentang Penyelenggaraan Informasi dan Transaksi Elektronik).
2. segara membentuk dan membuka seluas-luasnya kesempatan untuk mendirikan Lembaga Penyelenggara Sertifikasi Elektronik sebagai badan

hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik.

3. penyedia jasa perbankan harus menerapkan manajemen resiko yang dikeluarkan oleh Bank Indonesia dan peraturan perundang-undangan lainnya guna menghindari kemungkinan penyalagunaan teknologi informasi perbankan oleh pihak yang tidak bertanggung jawab.