IMPLEMENTASI PERATURAN PEMERINTAH NOMOR 82 TAHUN 2012 SEBAGAI UPAYA NEGARA MENCEGAH CYBERCRIME DALAM SISTEM TRANSAKSI ELEKTRONIK

Masitoh Indriani, Adhy Riadhy Arafah, Fitri Nuril Islamy
masitoh@fh.unair.ac.id, adhy@fh.unair.ac.id, fitri_nuril@gmail.com
Fakultas Hukum Universitas Airlangga

Abstract
The development of Information Technology (IT) changes the patterns of community's behavior. The presence of the Internet as the main platform of online activities including electronic transaction is vulnerable to the presence of cyber attacks by irresponsible parties. Criminal acts in cyberspace (cybercrime) pose a major threat in the governance of online activities and other electronic transactions. One of the efforts of the Government of Republic of Indonesia to face those challenges is by authorising the Governments Regulations Number 82 Year 2012 concerning the Implementation of Electronic Transaction Systems in order to govern the electronic transaction activities. This article will discuss about how the Government of Republic of Indonesia copes the issue of the threat on electronic transactions.

Keywords: *cybercrime, electronic transactions system, goverment regulation No. 82/ 2012*

Abstrak
Perkembangan Teknologi Informasi (TI) mengubah pola perilaku masyarakat. Kehadiran Internet sebagai platform utama aktivitas *online*, termasuk transaksi elektronik, rentan terhadap adanya serangan *cyber* oleh pihak yang tidak bertanggung jawab. Tindakan kriminal di dunia maya (*cybercrime*) menimbulkan ancaman besar dalam tata kelola aktivitas *online* dan transaksi elektronik lainnya. Salah satu upaya Pemerintah Republik Indonesia untuk menghadapi tantangan-tantangan tersebut adalah dengan mengeluarkan Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik untuk mengatur kegiatan transaksi elektronik. Artikel ini akan membahas tentang bagaimana Pemerintah Republik Indonesia berupayauntuk mengahadapi ancaman dalam kegiatan transaksi elektronik.

Kata Kunci: cybercrime, electronic transactions system, PP No. 82 Tahun 2012**.**

Pendahuluan

Perkembangan Teknologi Informasi (TI) sebagai bagian dari perkembangan globalisasi membawa perubahan yang signifikan terhadap perilaku keseharian masyarakat dan pelaku bisnis di Indonesia. Internet sebagai bagian dari produk globalisasi telah menjadi bagian pola dan perilaku masyarakat dan pelaku bisnis dalam berinteraksi dengan dunia luar. Sebagai contoh, Internet menawarkan kemudahan akses dalam bertransaksi dengan komunitas masyarakat serta pelaku bisnis dari mancanegara tanpa harus mengeluarkan biaya yang tinggi dalam kegiatan bisnis maupun kegiatan komersial lainnya.

Disatu sisi, penggunaan dan pemanfaatan TI seperti yang ditawarkan oleh internet dengan sistem jaringannya, membawa perubahan pola perilaku dan melahirkan bentuk-bentuk perbuatan-perbuatan hukum baru dimana perbuatan hukum baru tersebut harus tetap berada dalam koridor aturan yang ada. Namun dalam praktek, penggunaan dan pemanfaatan TI tersebut kadangkala tidak diperuntukkan sebagaimana mestinya. Hal ini istilah *cybercrime* menjadi istilah dan isu penting ketika penggunaan dan pemanfaatan TI tidak diperuntukkan untuk sebagaimana mestinya *cybercrime* telah menjadi bagian integral dari perkembangan serta pemanfaatan internet dalam kegiatan *online* serta transaksi elektronik. Sementara itu masyarakat umum serta pelaku bisnis yang memanfaatkan TI tersebut tidak menyadari bahwa terdapat ancaman keamanan (*cybersecurity*) dalam kegiatan *online* dan transaksi elektronik mereka. Bahwa dalam hal ini, keamanan dalam melakukan kegiatan online dan transaksi elektronik adalah mutlak dibutuhkan demi membangun iklim yang kondusif dalam ranah kegiatan baik bisnis maupun non-bisnis di dunia maya.

Berdasarkan laporan Internet Security Threat Report dari Symantec, Indonesia merupakan salah satu dari beberapa negara dengan aktivitas cybercrime terbanyak sepanjang tahun 2011.[1] Dalam laporan tersebut disebutkan bahwa terjadinya peningkatan aktivitas *online* menjadi penyebab meningkatnya *cybercrime* di Indonesia.[2] Selain itu, Indonesia juga menjadi negara target dalam *cyberattack* oleh *hacker* dari berbagai negara.[3] Negara dalam hal ini Pemerintah wajib memberikan dukungan dalam pemanfaatan TI melalui infrastruktur hukum serta pengaturannya guna tercipta iklim aktivitas online serta transaksi elektronik serta mampu mencegah ancaman keamanan dalam penyelenggaraan sistem transaksi elektronik. Dalam Penyelenggaraan Sistem Transaksi Elektronik (PSTE), terdapat empat elemen Keamanan Informasi dan Transaksi Elektronik antara lain: Kerahasiaan (*Confidentiality*); Otentitas (*Authenticaty*); Integritas (*Integrity*); Nir-sangkal (*Non-Repudiation*).[4]

Dalam kaitannya dengan penanggulangan *Cybercrime* di Indonesia, keempat elemen

[1] Kompas Online, "Indonesia Masuk 10 Besar Penyumbang Cybercrime Terbanyak', http://tekno.kompas.com/read/2012/05/16/09403718/indonesia.masuk.10.besar.penyumbang.quotcyber.crimequot.terbanyak, diunduh 19 Januari 2013.

[2] *Ibid.*

[3] Kompas Online, "Tiap Hari, Indonesia Diserang Hacker 1.5 Juta kali", http://tekno.kompas.com/read/2012/03/20/14070041/tiap.hari.indonesia.diserang.hacker.15.juta.kali, diunduh 19 Januari 2013.

[4] Saiful Hidayat, "Pemanfaatan PSRE dan LSK Sebagai Trusted Third Party Dalam Rangka Meningkatkan Keamanan Transaksi Elektronik", Sosialiasasi PP No. 82 Tahun 2012 tentang PSTE.

tersebut wajib dijalankan oleh Negara. Dalam hal ini, melalui PP Nomor 82 Tahun 2012 (PP No.82/2012), negara mengatur penyelenggaraan sistem elektronik dengan pengaturan empat elemen dasar antara lain, yaitu Pengaturan tentang perangkat keras (*hardware*) dan perangkat lunak (*software*), pengaturan tentang pengawasan, pengaturan tentang tenaga ahli serta pengaturan terkait dengan sertifikasi kelayakan penyelenggaraan sistem transaksi Elektronik. Lahirnya teknologi digital telah mengakibatkan terjadinya keterpaduan ataupun konvergensi dalam perkembangan teknologi informasi, multimedia dan telekomunikasi (*Information, Media and Communication Technology*). Semula masing-masing teknologi tersebut seakan berjalan terpisah atau *linear* antara yang satu dengan yang lainnya, namun kini semua teknologi tersebut semakin menyatu.

Wujud konvergensi (perpaduan) teknologi telekomunikasi, multimedia dan informatika *(telematika)* tersebut adalah lahirnya produk-produk teknologi baru yang memadukan kemampuan sistem informasi dan sistem komunikasi yang berbasiskan sistem komputer yang selanjutnya terangkai dalam suatu jaringan (*network*) sistem informasi dan/atau sistem komunikasi secara elektronik (selanjutnya disebut, "sistem elektronik") baik dalam lingkup lokal, regional maupun global.

Kehadiran sistem informasi tersebut seakan-akan telah membuat suatu ruang baru dalam dunia ini yang populer dengan istilah *cyberspace* untuk memperlihatkan suatu bentuk halusinasi virtual.[5] Istilah *cyberspace* awalnya digulirkan oleh seorang novelis *science fiction* bernama William Gibson dalam karyanya Neuromancer (1984).[6] Gibson menguraikan seakan-akan adanya suatu ruang baru (*space*) yang lahir akibat terhubungnya medium kawat penghantar listrik (*cyber*) yang mempertemukan sistem komputer dengan sistem telekomunikasi dalam suatu penyelenggaraan sistem elektronik. Istilah tersebut bergulir terus sebagai istilah populer dari keberadaan suatu komunikasi virtual melalui jaringan komputer (*the net*), yang selanjutnya berwujud menjadi jaringan sistem komputer global (internet).[7]

Keberadaan kata '*space*' dalam istilah '*cyberspace*' secara teknis adalah berbeda sifatnya dengan kata '*space*' dalam '*aerospace*', karena makna space pada '*aerospace*' adalah ruang semesta yang tak terbatas yang diciptakan oleh sang pencipta, sementara space pada '*cyberspace*' adalah ruang komunikasi ciptaan manusia yang bersifat terbatas meskipun jumlah pengunanya akan bertambah terus dari waktu kewaktu sesuai dinamika masyarakat.[8]

Seiring dengan dinamika tersebut, masing-masing bidang hukum yang terkait dengan konvergensi telematika, yakni hukum telekomunikasi, hukum multimedia dan hukum informatika (Komputer) yang semula dikaji secara terpisah/linear, dalam perkembangannya kini juga kian menyatu menjadi hukum terhadap informasi, multimedia dan komunikasi itu

---

[5] Brian D. Loader et.al, *The Governance of Cyberspace*, London: Routledge, 1997.

[6] *Ibid.*

[7] *Ibid.*

[8] Carlo A. Gerungan, Tanggung Jawab Penyelenggara Sistem Informasi Jika Terjadi Kegagalan Sistem', Jurnal Vol.Xxi/No.4/April-Juni /2013 Edisi Khusus 42.

sendiri.[9]

Jelas terlihat bahwa konvergensi hukum telematika (hukum telekomunikasi, hukum media dan hukum informatika) sesungguhnya merupakan benturan paradigma hukum sebelumnya yang selanjutnya melahirkan suatu paradigma hukum yang baru. Benturan paradigma hukum tersebut juga membuat ketidakjelasan tentang siapa yang harus bertanggungjawab dan bagaimana pertanggungjawabannya jika terhadap penyelenggaraan sistem elektronik terjadi suatu kerusakan atau tidak bekerja sebagaimana mestinya sehingga mengakibatkan kerugian kepada pihak lain. Hal tersebut tidak dapat dengan mudah ditentukan karena begitu rumit atau kompleksnya hubungan para pihak yang mempunyai kontribusi terhadap penyelenggaraan sistem tersebut kepada publik.

Internet sebagai *platform* utama kegiatan *online* dari masyarakat, mempunyai sifat yang *borderless*, dimana tidak mengenal batas-batas teritori sebuah negara. Dengan kondisi seperti ini, ancaman terhadap keamanan kegiatan *online* masyarakat menjadi isu yang harus segera di tangani dengan cepat mengingat perkembangan TI terjadi tidak hanya dalam hitungan hari melainkan lebih cepat dari itu.

Istilah *Cybercrime* adalah istilah yang disepakati untuk menggambarkan kejahatan yang dilakukan dalam dunia maya.[10] *Cybercrime* adalah kejahatan transformasi dari kejahatan yang dilakukan dalam dunia nyata ke dalam *cyberspace*.[11] Sedangkan *Cyberspace* sendiri adalah istilah yang digunakan untuk menggambarkan tempat atau lokasi dalam melakukan perbuatan kriminal baru, dalam hal imi melakukan kegiatan melawan hukum serta dalam bentuk kejahatan yang baru pula.[12]

Pada masa awalnya, istilah *Cybercrime* hanya didefinisikan sebagai kejahatan komputer dan masih belum ada keseragaman serta penggunaan istilah.[13] Penggunaan sitilah yang ada antara lain '*computer misuse'*, '*computer abuse'*, '*computer fraud'*,'*computer-related crime'*, '*computer-assited crime'* serta '*computer crime'*.[14] *The British Law Commission* mendefinisikan '*computer crime'* sebagai manipulasi komputer dengan berbagai cara yang dilakukan dengan itikad buruk untuk memperoleh keuntungan materi dan keuntungan lainnya yang dimaksudkan untuk menimbulkan kerugian kepada pihak lain. [15]Selanjutnya, Mandell membagi '*computer crime*' menjadi dua kegiatan utama yaitu: Penggunaan komputer untuk melaksanakan perbuatan penipuanm pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan dan pelayanan. Ancaman terhadap komputer itu

[9] *Ibid.*

[10] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge Polity Press, 2007.

[11] Susan W. Brenner, *Cybercrime: Criminal Threats From Cyberspace*, Greenwood Publishing Groups, 2010.

[12] *Ibid.*

[13] Budhi Suhariyanto, Tindak Pidana Teknologi Informasi (*Cybercrime*), Raja Grafindo Persada, Cet.1, 2012.

[14] *Ibid*, h. 9.

[15] Puslitbang Hukum dan Peradilan, Mahkamah Agung RI, Naskah Akademis Kejahatan Internet (*Cyber-crimes*), 2004

sendiri seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.[16] Sehingga pada dasarnya, *cybercrime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi, sistem informasinya sendiri serta komunikasi yang merupakan sarana untuek penyampaian atau pertukaran informasi kepada pihak lain (*transmitter/originator or reciptient*).[17]

Di dalam *Convention on Cybercrime* disebutkan bahwa penanggulangan *Cybercrime* harus memperhatikan 3 (tiga) aspek utama antara lain kerahasiaan (*confidentiality*), integritas (*integrity*) serta kesiapan dan ketersediaan sistem jaringan komputer.[18] Maka dari itu, diperlukan sebuah sistem perangkat yang dapat diandalkan serta sesuai dengan standar internasional yang dapat diterapkan dalam ranah nasional. Selanjutnya, untuk menangani *cyberspcae*, dibutuhkan aturan yang tidak hanya mencakup permasalahan teknis perbuatan penegakan hukum saja, melainkan bagaimana pengaturan tersebut adalah teknis semata dalam persepektif perkembangan dunia TI.[19]

Di dalam literatur disebutkan bahwa *Cybercrime* mempunyai karakteristik sebagai berikut: 1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang siber (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya; 2. Perbuatan tersebut dilakukan dengan menggunakan peralatan yang terhubung dengan internet; 3. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil yang cenderung lebih besar dari kejahatan kejahatan konvensional; 4. Pelakunya adalah orang yang menguasai Teknologi Informasi beserta aplikasinya; 5. Perbuatan tersebut sering dilakukan secara transnasional, melintasi batas negara.[20]

Menurut para ahli dan sarjana dalam pengklasifikasian bentuk kejahatan siber, terdapat beberapa hal yang dapat disimpulkan dari bentuk *Cybercrime* antara lain: 1)Kejahatan yang menyangkut data atau informasi komputer; 2) Kejahatan yang menyangkut program komputer (*software*); 3) Pemakaian fasilitas komputer tanpa wewenang untuk kepentingan yang tidak sesuai dengan tujuan pengelolaanya; 4) Tindakan-tindakan yang mengganggu operasi komputer; 5) Tindakan merusak komputer peralatan komputer atau peralatan lain yang berhubungan dengan komputer atau sarana penunjangnya.[21]

Secara umum dapat dijelaskan bahwa *cybercrime* merupakan bentuk kejahatan yang erat kaitannya dengan penggunaan atau pemanfaatan teknologi informasi yang berbasis kepada komputer, jaringan komunikasi berupa internet, serta beberapa aplikasi terapannya. Selanjutnya, dalam beberapa praktik kejahatan komputer yang terjadi, dapat diklasifikasikan beberapa bentuknya, antara lain:[22] *1) Unauthorised access to Computer System and Services*;

---

[16] *Ibid.*, h. 10.

[17] *Ibid.*

[18] Preambule of Convention on Cybercrime 2001

[19] David S. Wall, "Policing Cybercrimes: Situating the Public Police in Networks Security Within Cyberspace", Police Practice and Research: An International Journal, Vol. 8, No. 2, pp. 183-205, May 2007, Revised February 2011.

[20] Budhi Suhariyanto, *Op.Cit.*, h. 15.

[21] *Ibid*, h. 14.

[22] *Ibid.*

yaitu kejahatan yang dilakukan dengan cara memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya; 2) *Illegal Contents*; yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis dan dapat dianggap sebagai pelanggaran hukum atau mengganggu ketertiban umum; 3) *Data Forgery*; yaitu kejahatan dengan memalsukan data pada dokumen-dokumen melalui internet; 4) *Cyber Espionage*; yaitu kejahatan dengan memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran; 5) *Cyber Sabotage and Extortion*; yaitu kejahatan yang dilakukan dengan membuat perusakan, gangguan serta penghancuran terhadap suatu data, program internet atau sistem jaringan yang terhubung dengan internet; 6) *Offense Against Intellectual Property*; yaitu kejahatan terjadap Hak Kekayaan Intelektual (HKI) yang dimiliki oleh pihak lain di internet. 7) *Infringements of Privacy*; yaitu kejahatan yang ditujukan terhadap informasi pribadi dan rahasia seseorang. Maka yang dimaksud dengan Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan atau memanfaatkan komputer, jaringan komputer dan atau/media elektronik lainnya.[23] Selanjutnya, transaksi yang dimaksud tidak hanya meliputi bidang *e-commerce* saja, melainkan semua aspek perbuatan hukum dalam ranah konvensional namun yang dijalankan di dalam *cyberspace*.

Penyelenggaraan Sistem Elektronik di Indonesia

Penyelenggaraan Sistem Elektronik diatur dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektonik (UU No. 11/2008). UU No. 11/2008 menjadi tonggak lahirnya payung hukum baru dalam pengaturan masalah pemanfaatan Informasi dan Transaksi Elektronik. UU No. 11/2008 tersebut mengatur aspek-aspek penting dalam pemanfaatan informasi dan transaksi elektronik. Disamping itu, UU tersebut mengatur juga masalah-masalah yang kemungkinan timbul dari pemanfaatan teknologi infomasi seperti; hak cipta, transaksi elektronik, sengketa, yusridisksi dan lain-lain.

Penyelenggaraan Sistem Informasi di diatur dalam Pasal 15 UU No. 11/2008, adapun ketentuan Penyelenggaran Sistem Informasi tersebut adalah: a) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. b) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya. c) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Selanjutnya dalam Pasal 16 UU No. 11/2008 disebutkan bahwa sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

[23] Ketentuan Umum PP No. 82/2012.

1) dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan; 1) dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut; 2) dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut; 3) dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan 4) memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk. Selanjutnya, Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah dalam hal ini adalah Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik (PP No. 82/2012).

Lingkup transaksi Elektronik menurut Pasal 40 (2) PP No. 82/2012 dapat dilakukan dalam lingkup publik dan privat. Sedangkan pada ayat (4) menekankan bahwa Transaksi Elektronik dalam lingkup publik atau privat yang menggunakan Sistem Elektronik untuk pelayanan publik, dilaksanakan sesuai dengan ketentuan dalam PP No.82/2012, yakni harus dengan menggunakan Sertifikat Keandalan dan/atau Sertifikat Elektronik. Penyelenggara Transaksi Elektronik di wilayah Indonesia bbaik dari lingkup publik maupun prifat wajib memperhatikan aspek keamanan, keandalan, dan efisiensi; melakukan penyimpanan dan transaksi di dalam negeri; memanfaatkan gerbang nasional, jika dalam penyelenggaraannya melibatkan lebih dari satu Penyelenggara Sistem Elektronik; dan memanfaatkan Sistem Elektronik dalam negeri. Jika gerbang nasional dan jaringan Sistem Elektronik dalam negeri belum dapat dilaksanakan, penyelenggaraan Transaksi Elektronik dapat menggunakan sarana lain atau fasilitas dari luar negeri setelah memperoleh persetujuan dari Instansi Pengawas dan Pengatur Sektor terkait.

Transaksi elektronik dapat dilakukan berdasarkan kontrak elektronik atau bentuk kontraktual lainnya sebagai bentuk kesepakatan yang dilakukan oleh para pihak yang dibuat dalam bahasa Indonesia dan sesuai dengan ketentuan mengenai klausula baku seperti yang diatur dalam peraturan perundang-undangan. Kontrak elektronik tersebut dianggap sah apabila terdapat kesepakatan para pihak; dilakukan oleh subjek hukum yang cakap atau yang berwenang mewakili sesuai dengan ketentuan peraturan perundang-undangan; terdapat hal tertentu; dan objek transaksi yang tidak bertentangan dengan peraturan perundang-undangan, kesusilaan, dan ketertiban umum.

Penyelenggaraan Sistem Transaksi Elektronik (PSTE)

Di dalam PP No. 82/2012 disebutkan bahwa yang dapat menyelenggarakan Sistem Transaksi Elektronik adalah Orang, Penyelenggara Negara, Badan Usaha dan masyarakat yang menyediakan, mengelola dan/atau mengoperasikan Sistem Elektronik baik untuk keperluan

dirinya maupun keperluan pihak lain.[24] Transaksi Elektronik yang dimaksud harus memenuhi syarat subjektif serta syarat objektif seperti halnya transaksi yang di lakukan di kegiatan konvensional. Pasal 1320 BW menyebutkan syarat subjektif adalah: 1) Kesepakatan, dalam hal ini adanya sistem elektronik yang disepakati; 2)Kecakapan, yaitu dewasa atau tidak dibawah pengampunan. Sedangkan syarat objektif adalah: 1) Hal tertentu, yaitu adanya informasi yang valid; 2)Sebab yang halal, yaitu sesuai dengan UU, Kesusilaan serta Ketertiban Umum.

Syarat subyektif dan obyektif ini didalam PP No. 82/2012 diatur di dalam Pasal 20 yaitu Transaksi dianggap terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.[25] Bahwa selanjutnya persetujuan atas penawaran harus dilakukan dengan pernyataan penerimaan secara elektronik.[26] Selain itu, transaksi elektronik dapat dilakukan melalui Kuasa atau Agen Elektronik.[27] Sedangkan yang dimaksud dengan Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan Informasi Elektronik.[28]

Secara teknis, penyelenggaraan Sistem Elektronik di dalam PP No. 82/2012 ini dapat dibedakan menjadi 4 kategori kegiatan besar yaitu pendaftaran, pengamanan, pengawasan serta sertifikasi kelaikan sistem transaksi. Kegiatan pertama adalah pendaftaran. Kegiatan Pendaftaran dalam PSTE ini berkaitan erat dengan perangkat keras (*hardware*). Pendaftaran bagi Penyelenggara Sistem Elektronik (PSE) bersifat wajib bagi Pelayanan Publik, sedangkan untuk Non Publik bersifat sukarela. Sedangkan tata cara pendaftaran akan diatur dalam Peraturan Menteri dimana sampai sekarang masih belum terbit aturan yang dimaksud. Khusus mengenai Perangkat keras yang dimaksud harus memenuhi standar antara lain:Memenuhi aspek interekonektivitas dan kompatibilitas; Memperoleh sertifikasi kelaikan dari Menteri; Mempunyai layanan dukungan teknis, pemeliharaan maupun purnajual; Memiliki referensi pendukung bahwa perangkat keras tersebut berfungsi sesuai dengan spesifikasinya; Memiliki jaminan ketersediaan suku cadangnya, yaitu sedikitnya 3 tahun memiliki jaminan kejelasan mengenai kondisi kebaruan; Memiliki jamiman bebas dari cacat produk.

Kegiatan berikutya setelah pendaftaran adalah pengamanan. Kegiatan pengamanan dalam hal ini adalah berkaitan dengan tenaga ahli. Beberapa poin penting terkait dengan tenaga ahli ini adalah bahwa: Harus memiliki kompetensi TI; PSE yang strategis harus dipegang Tenaga Ahli WNI; Jabatan tenaga ahlli yang strategis tersebut pengaturannya harus disesuaikan dengan Peraturan Menteri. Selanjutnya adalah kegiatan pengawasan yakni yang terkait dengan perangkat lunak (*software*). Adapun beberapa hal penting dalam kegiatan pengawasan ini adalah: Perangkat lunak untuk PSE pelayanan publik wajib terdaftar di Kominfo; Wajib menyerahkan kode sumber (*Source Code*) kepada instansi pemerintah, dalam hal ini adalah

[24] Bab Ketentuan Umum PP No. 82/2012.
[25] Pasal 20 (1) PP No. 82/2012.
[26] Pasal 20 (2) PP No. 82/2012.
[27] Pasal 21 (1) PP No. 82/2012.
[28] Lihat no. 15

khusus untuk perangkat lunak yang dibuat untuk instansi; Apabila terdapat kepentingan umum yang menghendaki, maka dapat dilakukan pemeriksaan terhadap kode sumber perangkat lunak tersebut; Bahwa ketentuan tersebut diatas diatur khusus dalam Peraturan Menteri.

Kegiatan yang keempat adalah Sertifikasi Kelaikan Sistem Transaksi. Fokus dalam kegiatan ini adalah tentang tata kelola internet (*Internet Governance*). Bahwa PSE mempunyai kewajiban antara lain: Menjamin tersedianya *service level agreement*; Menjamin tersedianya Perjanjian Keamanan Informasi (PKI); Menjamin keamanan informasi dan sarana komunikasi internal; Menjamin keterpaduan seluruh komponen; Menerapkan manajemen resiko; Memiliki kewajiban tata kelola, prosedur kerja pengoperasian serta mekanisme audit.

Khusus terkait dengan tata kelola data pribadi, PSE mempunyai kewajiban: Menjaga rahasia, keutuhan dan ketersediaan data pribadi yang dikelolanya; Menjamin perolehan, penggunaan, dan pemanfaatan data pribadi berdasarkan persetujuan orang yang bersangkutan, kecuali ditentukan lain oleh peraturan perundangan; Menjamin penggunaan atau pengungkapan data dilakukan berdasarkan persetujuan dari pemilik data pribadi tersebut dan sesuai dengan tujuan yang disampaikan kepada pemilik data pribadi pada saat perolehan data.

Dalam PP No. 82/2012, didalam Pasal 12 menyebutkan : Penyelenggara Sistem Elektronik wajib menjamin: a) tersedianya perjanjian tingkat layanan; b) tersedianya perjanjian keamanan informasi terhadap jasa layanan TI yang digunakan; dan c) keamanan informasi dan sarana komunikasi internal yang diselenggarakan. Selanjutnya dalam Pasal 13, 14 dan 15 disebutkan: a) Penyelenggara sistem elektronik wajib menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan. b) Penyelenggara sistem elektronik wajib memiliki kebijakan tata kelola, prosedur kerja pengoperasian, dan mekanisme audit yang dilakukan berkala terhadap sistem elektronik. c) Penyelenggara sistem elektronik wajib menjaga rahasia, keutuhan, dan ketersediaan data pribadi yang dikelolanya; menjamin bahwa perolehan, penggunaan, dan pemanfaatan data pribadi berdasarkan persetujuan pemilik data pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan menjamin penggunaan atau pengungkapan data dilakukan berdasarkan persetujuan dari pemilik data pribadi tersebut dan sesuai dengan tujuan yang disampaikan kepada pemilik data pribadi pada saat perolehan data.

Menyangkut tanggung jawab penyelenggaraan sistem informasi, dalam Pasal 28 disebutkan penyelenggara sistem elektronik bertanggung jawab terhadap pengamanan dan perlindungan sarana dan prasarana sistem elektronik. Jika terjadi kegagalan terhadap suatu sistem informasi yang mengakibatkan sistem menjadi tidak berjalan sebagaimana mestinya, maka tentunya akan terjadi suatu ’kerugian’ baik materil maupun imateril yang mungkin tidak hanya diderita oleh pihak penyelenggara secara langsung melainkan juga oleh pihak lain (pihak ketiga) sebagai pengguna atas keberadaan sistem tersebut. Sebagai konsekuensinya akan timbul suatu tanggung jawab hukum atas gugatan ganti rugi akibat kerusakan sistem tersebut.

Keamanan Informasi Dalam Transaksi Elektronik

Keamanan Informasi dalam transaksi elektronik adalah mutlak dibutuhkan. Keamanan menjadi hal yang penting karena sifat penyebaran internet yang sangat cepat. Dengan kata lain, internet dan teknologi menjadi sarang komunikasi serta pertukaran informasi beserta data yang mana dapat memberikan keuntungan serta kerugian bagi penggunanya dimana menciptakan potensi pelanggaran di dunia maya.

Isu keamanan dalam ranah dunia maya bukanlah isu yang baru. Keamanan dalam mengakses informasi, bertukar informasi serta transaksi elektronik menjadi bagian yang tidak terpisahkan dari satu rangkaian kegiatan. Isu keamanan dalam internet yang menjadi perhatian saat ini dapat digolongkan menjadi 3 (tiga) kriteria besar: a) Jenis Tindakan; b) Jenis Pelaku Kejahatan; c) Jenis Target.[29] Klasifikasi berdasarkan jenis tindakan ini antara lain pencegahan data, intervensi data (*data intervention*), akses ilegal (*illegal access*), *spyware*, korupsi data (*data corruption*), sabotase, DOS (*denial of service*) serta pencurian identitas (*identity theft*). Klasifikasi berikutnya yakni jenis pelaku kejahatan didasarkan pada subjek yang bertanggung jawab terhadap isu keamanan informasi serta data di internet. Pelaku kejahatan dapat berupa *hacker, cyber-criminal, cyber-warrior*, serta *cyber-terrorist*. Sedangkan klasifikasi berdasarkan jenis target didasarkan pada objek atau target serangan yang potensial seperti dari individu, perusahaan swasta, institusi pemerintah hingga instusi militer. Berdasarkan kriteria tersebut diatas, khusus mengenai keamanan dalam bertransaksi di Indonesia diperlukan perhatian lebih terutama menyangkut permasalahan subjek atau si pelaku dan jenis target yang mengalami perkembangan dan tidak dapat diprediksi potensi perubahannya.

Pihak-Pihak Dalam Penyelenggaraan Transaksi Elektronik

Dalam Pasal 3 ayat (1) PP No. 82/2012 disebutkan bahwa Penyelenggaran Transaksi Elektronik dilaksanakan oleh Penyelenggara Transaksi Elektronik. Dalam hal ini yang dimaksud dengan penyelenggaran transaksi elektronik dapat dilakukan oleh 1) pelayanan publik dan 2) non pelayanan publik.[30] Secara umum, terdapat kewajiban yang harus dipenuhi oleh PSE yaitu antara lain: Menyediakan rekam jejak audit untuk seluruh PSE; Melakukan pengamanan terhadap komponen PSE; Memiliki dan menjalankan prosedur pengamanan SE utk menghindari gangguan, kegagalan serta kerugian; Menyediakan sistem pengamanan mencakup prosedur dan sistem pencegahan serta penanggulangan terhadap ancaman (*cyberthreat*); Apabila terjadi kegagalan atau gangguan SE yang berdampak serius, maka PSE wajib mengamankan data dan segera melapor ke APH atau instansi pengawas serta pengatur sektor terkait pada kesempatan pertama.

Adapun penyelenggaran transaksi elektronik yang dilakukan oleh 1) Pelayanan Publik dan 2) Non Pelayanan Publik dapat dijabarkan bahwa pelayanan publik yang dimaksud dalam hal

[29] Jovan Kurbalija, "Sebuah Pengantar Tentang Tata Kelola Internet", Jakarta : CV Goentoer Printing, 2011, h. 73.

[30] Pasal 3 ayat (2) PP No. 82/2012.

ini mempunyai kewajiban: Menerapkan tata kelola yang baik dan akuntabel; Memiliki rencana keberlangsungan kegiatan untuk menanggulangi gangguan; Menempatakan Pusat Data dan Pusat Pemulihan Bencana di wilayah Indonesia untuk kepentingan Penegakan hukum, perlindungan dan penegakan kedaulatan negara terhadap data warga negaranya; Instansi pengawas-pengatur sektor terkait dapat mengatur pusat data dan pusat pemulihan bencana serta tata kelola PSE di sektornya dengan tetap berkoordinasi dengan menteri. Kemudian, pelayanan non publik yang dimaksud dalam hal ini mempunyai kewajiban: Wajib menerapkan tata kelola yang baik dan akuntabel; Wajib memiliki rencana keberlangsungan kegiatan untuk menanggulangi gangguan; Wajib menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia untuk kepentingan penegaka hukum, perlindungan dan penegakan kedaulatan negara terhadap data warga negaranya; instansi pengawas-pengatur sektor terkait dapat mengatur lebih lanjut mengenai pusat data dan pusat pemulihan bencana serta tata kelola PSE di sektornya dengan tetap berkoordinasi dengan Menteri.

Upaya Negara Dalam Penanggulangan *Cybercrime* Dalam Penyelenggaraan Sistem Transaksi Elektronik

Upaya yang dilakukan lainnya dapat dilihat dari program *E-Authentication for Public Services* dengan pemanfaatan *National Key Infrastructure*.[31] *E-Authetication* merupakan proses pengamanan pengguna atau pemanfaat sistem transaksi elektronik pada sebuah Sistem Informasi.[32] Kegiatan pengamanan ini melibatkan proses teknis pada sebuah sistem informasi yang diterjemahkan melalui program komputer. Terdapat 2 (dua) model pengamanan dalam kegiatan ini yaitu: *Direct Authentication;* pada model ini, terdapat keterlibatan antara *users*, dalam hal ini adalah penyelenggara sistem transaksi elektronik dengan *Service Provider* dengan memanfaatkan "*username and password*" sebagai alat validasi untuk masuk atau sebagai akses dari elemen kerahasiaan (*credentials*). *Trust Third Party Authentication;* pada model ini, tidak ada hubungan secara langsung antara users dengan Service Provider melainkan memanfaatkan atau melibatkan pihak ketiga (*Third Party*) untuk melaksanakan proses validasi.[33] Untuk memperjelas kedua model tersebut diatas, dapat dilihat dalam berbagai aktivitas *e-commerce* yang mensyaratkan adanya pelibatan *Third Party* dalam proses validasi pembayaran *e-payment* seperti yang seringkali terlihat di halaman muka sebuah situs seperti yang terlihat dalam gambar dibawah ini:

Gambar 2. *Third Party*

[31] Pratama D. Persadha, "E-Authentication for Public Services Using National Public Key Infrastructure", LEMSANEG, paperworks, Januari 2013.

[32] *Ibid.*

[33] *Ibid.*

Bentuk pengamanan yang lain adalah pemanfaatan *Public Key Infratructure (PKI)*. PKI merupakan gabungan antara *software*, *encryption technologies* serta *Service Provider* yang diterjemahkan melalui *Digital Certificates*, *Public Key Cryptography* serta adanya pelibatan otoritas sertifikasi dalam sebuah sistem *enterprise-wide network security architecture*.[34] Didalam sistem ini, komunikasi yang dilakukan antara PSTE dengan *users*, akan dienkrpsi sedemikan rupa dengan menggunakan *digital signature technique* dimana didalamnya terdapat elemen-elemen khusus yang menjadi basis pengamanan fungsi distribusi dalam bertransaksi elektronik. Pengamanan dengan sistem yang unik ini mempunyai potensi untuk tidak memberikan kesempatan kepada para pelaku *Cybercrime* dalam sebuah sistem jaringan informasi.

Selanjutnya, upaya pencegahan dan pengamanan yang dilakukan adalah PKI adalah berupa *Certificate/Digital Certificat.* Berdasarkan data dari NIST Publication 800-63 Version 1.0.2, PKI Certificate merupakan satu dari 5 (lima) model E-Authentication.[35] Pengamanan yang dimaksud didalam sistem ini mentitikberatkan kepada penggunaan *Public Key*, *Private Key,* erta fungsi alogaritma. PKI *Certificate* ini dapat diimplementasikan pada pelayanan publik berupa *Internet Banking, E-Commerce, E-Procurement* serta aplikasi-aplikasi yang berbasis *E-Government* lainnya.

Upaya terakhir dalam pengamanan PSTE adalah dengan Program *Secure Sockets Layer (HTTPS)*. Program ini merupakan program yang paling umum digunakan sebagai pengamanan di dalam ranah *cyberspace*. Program *Sockets Layers* digunakan untuk mengenkripsi informasi yang dikirim melalui jaringan internet kepada penerima informasi. Program ini dapat terlihat pada sebuah *tab address* sebuah *browser* yaitu "https://". Fungsi dari *Socket Layers* ini adalah melindungi *users* dari upaya pengalihan ke situs lain yang tidak diinginkan. Selain itu, program ini juga telah dilengkapi dengan PKI *Certificate* yang seperti yang telah dijelaskan dibagian sebelumnya.

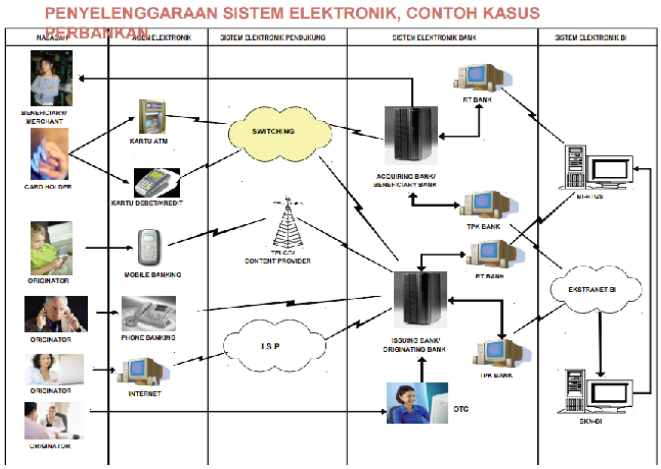
Hal tersebut sesungguhnya telah diatur sedemikian rupa didalam PP PSTE yaitu pada ada tataran implementasi sistem keamanan dalam penyelenggaraan sistem transaksi elektronik dilaksanakan dengan Pemanfaatan dan Penyelenggaraan Sertifikat Elektronik. Pemanfaatan yang dimaksud dalam hal ini adalah diselenggarakan oleh pelaku usaha, yaitu pelaku usaha yang menyelenggarakan transaksi elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan. Lembaga sertifikasi keandalan terdiri atas: lembaga sertifikasi keandalan, Indonesia, lembaga sertifikasi keandalan asing. Selanjutnya lembaga sertifikasi keandalan Indonesia harus berdomisili di Indonesia. Sedangkan lembaga sertifikasi keandalan harus terdaftar dalam daftar lembaga sertifikasi keandalan yang diterbitkan. Khusus mengenai siapa saja yang berhak atas Sertifikat Keandalan ini, diperlukan pelibatan profesional yang sesuai dengan bidangnya. Misalkan, Konsultan TI, Audior TI serta Konsultan Hukum Bidang TI. Selain itu juga diperlukan peran dari profesional lainnya seperti Akuntan, Penilai, Notaris, hingga profesi lainnya yang akan ditentukan oleh menteri dikemudian hari.

[34] *Ibid.*

[35] NIST Special Publication 800-63 Version 1.0.2: Electronic Authentication Guidelines, 2006.

Selain pemanfaatan dan penyelenggaraan sertifikat elektronik dilaksanakan juga Pemanfaatan Sertifikat Keandalan berupa Tanda Tangan Digital. Dalam hal ini tanda tangan elektronik berfungsi sebagai alat autentikasi dan verifikasi atas identitas penanda tangan dan keutuhan dan keautentikan informasi elektronik. Tanda tangan elektronik dalam transaki elektronik berfungsi sebagai persetujuan penanda tangan atas IE/DE yang ditanda tangai dengan tanda tangan elektronik tersebut. Apabila terjadi penyalahgunaan tanda tangan elektronik oleh pihak lain, beban pembuktian pada penyelenggara sistem elektronik.

Sebagai ilustrasi pengamanan *Cybercrime*, dibawah ini ditampilkan contoh PSTE dalam bidang perbankan yang melibatkan begitu banyak sistem.



Gambar 2. penyelenggaraan system elektronik, contoh kasus perbankan
Sumber : Djoko Agung Harijadi, Ditjen Aplikasi Informatik, KOMINFO, Februari 2013

Dari ilustrasi gambar tersbebut diatas, dapat dijelaskan alur pengamanan terhadap tindakan *Cybercrime* adalah terdapat proses Dekripsi pada Sistem Elektronik Pendukung. Setelah itu proses Dekripsi dalam Sistem Elektronik Bank dan Sistem Elektronik BI. Pada masing-masing Sistem Elektronik, terdapat *Public Key* serta *Private Key* yang dijamin keamanannya dengan proses validasi baik itu berdasarkan *Direct Autenthication* maupun yang melibatkan *Third Party*.

Strict Liability

Eksistensi suatu sistem informasi berbasiskan komputer akan merujuk kepada tiga hal penting, yakni (i) keberadaan komponen-komponen yang digunakannya, (ii) keberlangsungan aktivitas-aktivitas fungsi yang telah ditentukan, dan (iii) sifat keterpaduan dari semua hal tersebut. Untuk melihat adanya kerusakan pada suatu sistem informasi tentunya juga akan melihat kepada tiga hal tersebut, yakni: a) Tidak bekerjanya komponen-komponen (*hardware, software*, data, *procedure* dan *brainware*) dalam sistem sebagaimana yang diharapkan; b) Tidak berfungsinya semua aktivitas fungsional (input, proses, *output*, *storage*, *communicate*) dalam sistem sebagaimana yang telah ditentukan; c) Tidak terjaganya sifat keterpaduan (integrasi) dalam sistem. Sehubungan dengan itu, kegagalan tersebut pada dasarnya disebabkan oleh tiga hal yang menyebabkan *malfunction*, yakni: tidak bekerjanya perangkat keras (*hardware*

malfunction) sebagaimana mestinya; atau tidak bekerjanya kode-kode instruksi dalam perangkat lunak sebagaimana yang ditentukan, mencakup (i) kesalahan pemrograman yang berdampak langsung kepada proses fisik (*software produces incorrect information which feeds directly into a physical process*), atau (ii) kesalahan program yang menghasilkan informasi yang tidak sebagaimana yang diharapkan (*software produces incorrect information which is relied on by human mind*). Untuk menentukan tanggung jawab tersebut, maka tanggung jawab dapat ditentukan berdasarkan (i) kontrak/perjanjian para pihak, atau (ii) tanggung jawab berdasarkan ketentuan dalam undang-undang yang disebut juga sebagai perbuatan melawan hukum (PMH).

Tanggung jawab berdasarkan kontrak akan melihat kepada keberadaan klausul-klausul dalam kontrak, seperti kontrak penjualan atau pemasokan perangkat, kontrak penyediaan jasa, atau kontrak lisensi penggunaan *software*. Sementara PMH, akan melihat kepada (a) tanggung jawab produk akibat cacat produk (*defective product*), (b) tanggung jawab atas kelalaian yang berakibat kerusakan barang atau lukanya badan, atau kelalaian yang berakibat kerugian finansial (*financial loss*), mencakup kerugian konsekwensial akibat *software* yg tidak dapat digunakan atau kerugian akibat keterpercayaan terhadap informasi yang diproduksi oleh suatu software yang tidak benar. Kelalaian tersebut dapat terjadi karena (i) kelalaian atas perancangan/ desain sistem (*negligencein designing the system*), (ii) kelalaian dalam pengoperasian sistem (*negligence in operating the system*), (iii) kelalaian dalam penentuan hasil keluaran dari sistem (*negligencein relying on the output of the system*), atau (iv) kesalahandalam penggunaan sistem (*failure to use a computer system*).

Umumnya kontrak tentang pengembangan sistem elektronik ataupun sistem komputer (*system supply contract*) jika dilakukan dari awal, akan mencakup secara keseluruhan komponen-komponen yang dibutuhkandalam sistem tersebut, yakni umumnya akan berbentuk *turn-key contract*, yang mencakup: (i) Pengadaan perangkat keras komputer (baik jual beli ataupun sewa menyewa); (ii) Pengadaan perangkat lunak komputer, baik sistem operasi maupun sistem aplikasinya, (iii) pengadaan perangkat tambahan (*peripherals*), seperti antara lain *cabling* dan *power supply*, dan (iv) pengadaan jasa pelayanan yang dibutuhkan (contoh: *consultancy, installation, support and maintenance*).

Dalam prakteknya, jika sistem elektronik tersebut telah ada sebelumnya dan yang dilakukan berikutnya hanyalah proses pengembangan lebih lanjut, maka kontrak tersebut tidak lagi merupakan pengadaaan secara keseluruhan melainkan cukup parsial saja dengan kombinasi dari setiap komponen-komponen yang dibutuhkan tersebut. Menurut Chris Reed disebutkan bahwa:

> *Any well drawn contract will have provisions relating to three board categories of expectation: a) Contract mechanics: for example who delivers what, and when?; b) Commercial highlights: for example, what is the price, who owns IPR's, what warranties are given in respect of the system? c) Problem management: what happens if the project goes wrong, and what remedies are available*?[36]

[36] Chris Reed et. al, Computer Law, (4th ed.), London: Blackstone Press Ltd. 2000, h. 87-88.

Setidaknya ada empat pertanyaan yang dapat menjadi tolok ukur untuk menentukan bilamana suatu tanggung jawab tersebut adalah bersifat kontraktual ataukah perbuatan melawan hukum. 1) Apakah penggugat mempunyai hubungan kontraktual (*privity of contract*) dengan tergugat?; 2) Apakah penggugat hanya menderita kerugian ekonomis (material) saja ataukah juga menderita kerugian fisik?; 3) Apakah klausul pembatasan atau pembebasan tanggung jawab telah sesuai atau konsisten dengan kebijakan publik atau keadilan (*fairness*)?; 4) Apakah pemulihan hak berdasarkan kontrak sudah sepadan dengan kerugian?

Penerapan *strict liability* di ranah TI, ternyata memperlihatkan dua hal, yakni (i) terhadap tanggung jawab produk perangkat keras karena dapat dikategorikan sebagai barang (*goods*) dapat dilakukan penerapan prinsip strict liability (*strict product liability*) dengan mudah, sedangkan (ii) terhadap tanggung jawab atas data, perangkat lunak (*softwar*e) atau tanggung jawab terhadap jasa yang digunakan, tampaknya sulit untuk menerapkan *strict liabil*ity meskipun kebutuhan ataupun desakan untuk menerapkan *strict* daripada penerapan *negligence*.

Dari uraian tersebut diatas, tergambar jelas bahwa negara telah mengupayakan mengatur tentang Sistem PSTE dengan mengedepankan semangat tanggung jawab yang melekat kepada para PSTE dengan membebankan penerapan *strict liability* daripada penerapan *negligence*.

Kesimpulan

Penyelenggaraan Sistem Transaksi Elektronik di Indonesia tidak hanya berfokus terhadap perijinan semata, namun juga menitikberatkan kepada hal-hal pengaturan yang bersifat teknis yang bersentuhan langsung dengan TI; Dalam hal berkaitan dengan penanggulangan dan pemberantasan *Cybercrime*, pemerintah telah cukup komprehensif mengatur penyelenggaran dan pemanfaatan sistem transaksi elektronik dengan menitikberatkan 4 komponen dalam PSTE yaitu: Pendaftaran berupa Pengaturan tentang Perangkat Keras (*hardware*); Pengamanan berupa pengaturan tentang perangkat lunak (*software*); Pengawasan yang menitikberatkan kepada pemanfaatan tenaga ahli dalam PSTE; Sertifikasi kelaikan sistem transaksi yang menyangkut tentang teknis pengaturan sistem transaksi.

Lembaga sandi negara mempunyai peran yang sangat vital dalam pengamanan PSTE di Indonesia. Hal ini dapat terlihat dari berbagai program yang telah dijalankan antara melalui program *National E-Authentication*. Sedangkan penerapan *Strict Liability* dalam bidang TI perlu diimplementasikan secara komprehensif guna mendukung kelancaran sebuah sistem informasi khususnya adalah penyelenggaraan sistem transaksi elektronik.

Daftar Bacaan

Buku

Brenner, Susan W. *Cybercrime: Criminal Threats from Cyberspace*, Greenwood Publishing Groups, 2010.

Fafinski, Stefan, *Computer Misuse: Response, Regulation and the Law*, Cullompton, 2009.

Kurbalija, Jovan, *Sebuah Pengantar Tentang Tata Kelola Internet*, Jakarta: Goentoer Printing, 2011.

Marzuki, Peter Mahmud *Penelitian Hukum*, Jakarta, Kencana Prenada Media Group, 2008.

Mertokusumo, Sudikno *Penemuan Hukum: Sebuah Pengantar,* Cetakan Kelima, Yogyakarta: Liberty, 2007.

Loader, Brian D. *et.al*, *The Governance of Cyberspace*, London, Routledge, 1997.

Suhariyanto, Budhi, *Tindak Pidana Teknologi Informasi (Cybercrime), Urgensi Pengaturan dan Celah Hukumnya,* Raja Grafindo Persada, Cetakan Pertama, 2012

Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge Polity, 2007.

Makalah

Gerungan, Carlo A. *Tanggung Jawab Penyelenggara Sistem Informasi Jika Terjadi Kegagalan Sistem*, Jurnal *Vol.Xxi/No.4/April-Juni /2013 Edisi Khusus* 42

Wall, David S. "*Policing Cybercrimes: Situating the Public Police in Networks Security Within Cyberspace"*, Police Practice and Research: An International Journal, Vol. 8, No. 2, p. 183-205, May 2007, Revised February 2011

Laman

http://tekno.kompas.com/read/2012/05/16/09403718/indonesia.masuk.10.besar.penyumbang.quotcyber.crimequot.terbanyak, diakses tanggal 12 Mei 2012.

http://tekno.kompas.com/read/2012/03/20/14070041/tiap.hari.indonesia.diserang.hacker.15.juta.kali, diakses tanggal 12 Mei 2012.