PERTANGGUNG-JAWABAN KEJAHATAN YANG DILAKUKAN DALAM LAYANAN FREE WIFI MENURUT UU NO 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Oleh

Evi Retno Wulan

Abstract

In this globalization era, free wifi internet network is also widespread and available in every place, like offices, schools, cafes and other places. Indeed, development of the Internet using can provide a lot ofpositive things, like to ease of getting information, but also there are a lot of negative things that can arise from the internet using. For example cyber crimes (done in or through the Internet), such asstealing identity, phishing, cyber harrasement etc. Although late, Indonesia already has the rule that regulate the flow of information and communication through the internet with UU ITE No 11/2008, but there are still many obstacles in the application of UU ITE No 11/2008, due to the process of inquiry, investigation and proving difficult and the readiness of human resources that very less. Beside that problems, there a many articles not suitable or difficult to apply in dealing with cases of cyber crime. The problems related toissues such as jurisdiction, determining locus and tempus delicti (time of criminal action), the accountability for foreign who came from abroad is very complicated to get the evidence.

*Keywords: **cy**ber, free wifi, crime, cybercrime service*.

Pendahuluan

Maraknya layanan free wifi yang ada hampir disemua tempat umum memudahkan masyarakat untuk mendapatkan akses informasi melalui teknologi informasi yang tersedia. Teknologi informasi selain membawa manfaat dan kontribusi terhadap masyarakat tetapi disisi lain menjadi sarana dalam melakukan perbuatan melawan hukum. Perkembangan teknologi informasi mendorong adaptasi/ penyesuaian ketentuan-ketentuan konvensional menjadi lebih responsif terhadap kondisi masyarakat yang semakin dinamis karena teknologi informasi dapat berdampak pada kehidupan yang sesungguhnya. Persoalah hukum yang seringkali muncul terkait tindak pidana teknologi informasi ini adalah dapat dilakukan siapapun, dimanapun, *borderless* dan bersifat anonim.

Dengan pengguna internet sebanyak 82 juta orang di Indonesia[1]

[1]http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U8fm9aDezCI, diakses Juni 2014.
http://techno.okezone.com/read/2014/05/13/55/984151/indonesia-peringkat-8-dunia-pengguna-internet-

menjadikan negara ini rentan sebagai sasaran maupun sumber kejahatan cybercrime dengan berbagai modus seperti misalnya *counterfeit, carding, cracking, phising* dll. Sebelum adanya UU No 11 Tahun 2008 Tentang Informasi dan Teknologi Informasi aparat penegak hukum dalam menangani tindak pidana bidang teknologi informasi dengan menggunakan ketentuan-ketentuan konvensional dengan menggunakan metode penafsiran. Metode ini merupakan terobosan penegak hukum Indonesia untuk mengatasi kekosongan aturan terutama terhadap beberapa delik yang berkaitan dengan teknologi informasi seperti misalnya penggunaan Pasal 362 KUHP untuk menangani kasus *carding*/pencurian nomor kartu kredit, Pasal 331 KUHP yang digunakan untuk menangani kasus pencemaran nama baik dengan menggunakan media internet.

Namun penggunaan ketentuan-ketentuan tersebut diatas dianggap oleh banyak ahli sudah tidak relevan dalam mengakomodir serta menangani tindak pidana teknologi informasi yang semakin lama semakin sulit dan kompleks. Permasalahan tersebut seperti misalnya terkait masalah yurisdiksi, penentuan locus dan tempus delicti, pertanggungjawaban pelaku yang berasal dari luar negeri serta sistem pembuktian yang sangat rumit. Oleh karena itu penggunaan dan pemanfaatn teknologi informasi saat ini seharusnya tidak dapat lagi dilakukan dengan pendekatan sistem hukum yang masih konvensional.

Dibentuknya UU No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) diharapkan dapat menanggulangi tindak pidana teknologi informasi yang semakin meresahkan masyarakat serta menjamin kepastian dan pemanfaatan *cyberspace* supaya lebih dapat berkembang secara optimal. Untuk itu penulis tertarik untuk mengkaji efektifias penerapan serta pertanggungjawaban tindak pidana teknologi informasi melalui layanan free wifi menurut UU ITE.

Berdasarkan ketentuan tersebut di atas, maka apa saja kendala penerapan UU No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam hal kejahatan cyber yang dilakukan melalui layanan wifi ?

Pembahasan

Jurisdiksi merupakan hal yang sangat krusial dan kompleks khususnya berkenaan dengan pengungkapan kejahatan-kejahatan di dunia maya yang bersifat *borderless*. Dengan adanya kepastian jurisdiksi maka suatu negara memperoleh pengakuan dan kedaulatan penuh untuk menerapkan hukum secara penuh. Kekuasaan demikian harus dihormati pula oleh setiap negara lainnya sebagaimana kekuasaan yang dimiliki oleh negara-negara lain..

Jurisdiksi menurut hukum pidana internasional adalah kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum).

Harus diakui bahwa menerapkan jurisdiksi terhadap kejahatan-kejahatan *cybercrime* bukan merupakan pekerjaaan yang mudah, karena kejahatannya

terbesar. diakses Juni 2014

bersifat internasional sehingga banyak bersinggung dengan kedaulatan maupun sistem hukum negara lain. Sejauh mana suatu negara memberikan kewenangannya kepada pengadilan untuk mengadili dan menghukum pelaku tindak pidana.

Menurut Masaki Hamano terdapat 3 lingkup yurisdiksi di *cyberspace* yang dimiliki suatu negara berkenaan dengan penetapan dan pelaksanaan pengawasan terhadap setiap peristiwa, setiap orang dan setiap benda, antara lain:

1. JurisdiksiLegislatif (*jurisdiction to prescribe*)
2. JurisdiksiYudisial (*jurisdiction to adjudicate*)
3. JurisdiksiEksekutif (*jurisdiction to enforce*).

Dalam pembentukan undang-undang khusus mengenai *cybercrime* perlu dipikirkan bentuk jurisdiksi yang mampu menjangkau kejahatan di dunia *cyber* mengingat kejahatan ini punya karakter yang khas dan sifatnya lintas negara (*transborder*). Dengan demikian penerapan asas universal dapat digunakan disamping juga diperlukan kerjasama dengan negara-negara lain.

Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur masalah jurisdiksi yang didalamnya menggunakan asas universal. Hal ini dapat dilihat dari Pasal 2 dan penjelasannya:

- Pasal 2 UU ITE

UU ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

- Penjelasan Pasal 2 UU ITE

  Undang-Undang ini memiliki jangkauan jurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbutan hukum yang dilakukan di luar wilayah hukum Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal. Yang dimaksud dengan"merugikan kepentingan Indonesia" meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

Penulis melihat terdapat beberapa cacatan kelemahan terhadap beberapa ketentuan dalam UU No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, antara lain:

1. KualifikasiDelik

   Pada UU ini tidak mengatur kualifikasi delik "kejahatan" atau "pelanggaran" sehingga pertanggungjawaban pidana antara "kejahatan"dan "pelanggaran" dalam KUHP berbeda. UU No 12 Tahun 2011 Tentang Pembentukan Peraturan Perundangan menyatakan bahwa "*..Rumusan ketentuan pidana harus menyatakan secara tegas kualifikasi dari perbuatan yang diancam dengan pidana itu sebagai pelanggaran atau kejahatan."*

   Pengklasifikasian delik tersebut bertujuan untuk memudahkan penentuan apakah suatu perbuatan termasuk dalam kejahatan atau termasuk dalam pelanggaran.Perbuatan kejahatan maupun pelanggaran memiliki sisi pandang berbeda, dari sisi kualitatif kejahatan disebut sebagai '*rechtdelicten*" yaitu perbuatan yang meski tidak ditentukan dalam perundangan disebut sebagai perbuatan pidana karena telah dirasakan sebagai *onrecht* yaitu sebuah perbuatan yang bertentangan dengan tata hukum. Pelanggaran disebut sebagai "*wetsdelictern'* adalah perbuatan yang sifat melawan hukumnya baru dapat diketahui setelah adanya "*wet*" yang menentukan demikian. Secara kuantitatif kejahatan dan pelanggaran memiliki perbedaan mengenai berat ringannya ancaman pidana yang dikenakan. Selain disebut diatas, perbedaan lain mengenai kejahatan dan pelanggaran antara lain:

   a. Pidanapenjarahanyadiancamkanpadakejahatansaja.
   b. Jika menghadapi kejahatan maka bentuk kesalahan (kesengajaan atau kelapaan) yang diperlu kandi situ, harus di buktikan oleh jaksa, sedangkan jika menghadapi pelanggaran hal itu tidak usah. Berhubung dengan itu kejahatan dibedakan pula dalam kejahatan yang *dolus* dan *culpa*.
   a. Percobaanuntukmelakukanpelanggarantakdapatdipidana (Pasal 54 KUHP). Juga pembantuanpadapelanggarantidakdipidana (Pasal 60 KUHP).
   c. Tenggangdaluwarsa, baikuntukhakmenentukanmaupunhakpenjalananpidanabagi pelanggaranadalahlebihpendekdaripadakejahatantersebutmasing-masingadalahsatutahundanduatahun.
   d. Dalam hal pembarengan (*concursus*) pada pemidanaan berbeda buat pelanggaran dan kejahatan. Kumulasi pidana yang ringan lebih mudah dari pada pidana berat.

2. Yurisdiksi

   Salah satu keunikan tindak pidana *cyber* adalah bahwa satu tindak pidana yang dilakukan di suatu negara dapat menimbulkan akibat yang dilarang di negara lain. Ketika delik ini terjadi permasalahan yang muncul adalah mengenai yurisdiksi penegakan hukumnya terhadap tindak pidana tersebut karena setiap negara memiliki kedaulatan penuh terhadap wilayahnya.Untuk itu, penting bagi aparat hukum kita untuk melakukan kerjasama dengan berbagai negara dalam mengungkap suatu tindak pidana tertentu.

Permasalahan yurisdiksi berlakunya hukum pidana nasional terhadap suatu perbuatan berkaitan dengan asas legalitas dan prinsip-prinsip yurisdiksi sebagai dasar berlakunya hukum pidana. Berdasarkan asas legalitas suatu perbuatan dapat dituntut, diadili, dan dipidana apabila perbuatan tersebut merupakan suatu tindak pidana yang diatur dalam Undang-Undang. Penentuan suatu perbuatan sebagai tindak pidana merupakan bagian dari kekuasaan kedaulatan yang dimiliki suatu negara untuk menetapkan hukumnya (*jurisdiction to prescribe*). Namun walaupun demikian untuk melakukan kriminalisasi *cybercrime* yang memiliki dimensi transnasional atau *cross border* suatu negara harus memperhatikan aspek harmonisasi baik dengan hukum internasional maupun hukum negara-negara lain karena berkaitan dengan implementasi yurisdiksi negara yang lainnya, yaitu kekuasaan negara untuk menerapkan hukum (*jurisdiction to enforce*) dan kekuasaan negara untuk mengadili (*jurisdiction to adjudicate*). Apabila pengaturan *cybercrime* dalam hukum nasionalnya tidak memperhatikan harmonisasi dengan pengaturan dalam hukum internasional atau hukum negara-negara lain maka hal ini akan menghambat dalam penegakan hukumnya. Mengingat tidak adanya batasan yang jelas mengenai *cybercrime* dan relatif luasnya lingkup *cybercrime* sebagaimana diuraikan di atas maka sangat potensial terjadinya ketidaharmonisan dalam pengaturan *cybercrime*dalam hukum nasional masing-masing negara.

Pengaturan yurisdiksi kriminal terhadap *cybercrime* terdapat dalam Pasal 2 UU Informasi dan Transaksi Elektronik, yang pada dasarnya menyatakan bahwa UU ITE berlaku terhadap setiap orang yang melakukan tindak pidana yang berada di dalam wilayah hukum Indonesia atau berada di luar wilayah hukum Indonesia dan mempunyai akibat hukum diwilayah hukum Indonesia atau di luar wilayah hukum Indonesia dan merugikan kepentingan hukum Indonesia. Ketentuan Pasal 2 UU ITE merupakan aturan yurisdiksi yang bersifat *lex specialis* dari aturan yurisdiksi dalam Buku I KUHP. Sehingga yurisdiksi kriminal dalam UU ITE hanya berlaku terhadap tindak pidana dalam UU ITE.

Pengaturan yurisdiksi kriminal dalam Pasal 2 UU ITE relatif singkat dan padat sehingga dalam implementasinya diperlukan penafsiran-penafsiran dan perluasan terhadap prinsip-prinsip yurisdiksi dalam hukum internasional publik dan teori *locus delicti* dalam hukum pidana. Berdasarkan ketentuan Pasal 2 UU ITE prinsip yurisdiksi yang menjadi dasar berlakunya hukum pidana terhadap *cybercrime* adalah:

a. Prinsipteritorial

   Prinsip teritorial dalam Pasal 2 UU ITE terkandung dalam rumusan "yang berada di wilayah hukum Indonesia". Dalam rumusan selanjutnya juga ditegaskan prinsip teritorial objektif, yaitu dalam rumusan "di luar wikayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia". Di lain pihak dalam ketentuan ini tidak ada penegasan berlakunya prinsip teritorial subjektif, yang sangat penting dalam pemberantasan *cybercrime* yang seringkali perbuatannya dimulai disuatu wilayah negara dan

penyelesaiannya atau efeknya ada diwilayah negara lain. Namun demikian prinsip teritorial subjektif dapat digunakan dengan melakukan penafsiran.

b. Prinsipperlindungan

Prinsip perlindungan dalam Pasal 2 UU ITE terkandung dalam rumusan "di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia." Prinsip perlindungan dalam ketentuan ini lebih luas dari yurisdiksi perlindungan dalam KUHP dan prinsip perlindungan pada umumnya yaitu untuk melindungi kepentingan vital suatu negara.

Dalam Pasal 2 UU ITE prinsip-prinsip yurisdiksi lainnya seperti prinsip nasional baik prinsip nasional aktif maupun prinsip nasional pasif tidak menjadi dasar berlakunya hukum pidana terhadap *cybercrime*. Demikian pula prinsip bendera negara kapal dan prinsip pesawat negara terdaftar sebagai perluasan prinsip teritorial tidak berlaku.

Berdasarkan analisis terhadap pengaturan yurisdiksi kriminal terhadap *cybercrime* baik dalam hukum nasional, hukum internasional maupun hukum pidana negara lain, prinsip-prinsip yurisdiksi yang digunakan dalam pengaturan yurisdiksi kriminal terhadap *cybercrime* adalah prinsip-prinsip yurisdiksi yang dikenal dan diakui dalam hukum internasional publik dan hukum pidana nasional dengan beberapa perluasan sesuai dengan karakteristik cybercrime. Prinsip-prinsip yurisdiksi tersebut adalah:

a. Prinsip territorial baik territorial subjektif maupun territorial objektif yang diperluas territorial tidak hanya untuk tindak pidana yang seluruh perbuatannya dilakukan di dalam wilayah Negara tetapi juga termasuk sebagian dari perbuatan yang dilakukan atau sebagian dari akibat yang terjadi di wilayah Negara dan penerapan "*effect doctrine*" untuk perluasan prinsip territorial objektif.
b. Prinsip "bendera Negara kapal" dan prinsip "pesawat Negara terdaftar" diperluas termasuk sebagian perbuatan dilakukan dalam pesawat atau sebagian akibatnya terjadi terhadap pesawat dan perbuatan dilakukan di dalam yurisdiksi Negara lain atau di luar yurisdiksi Negara manapun.
c. Prinsipnasional, baik prinsip nasional aktif maupun prinsip nasional pasif diperluas tidak hanya untuk tindak pidana yang dilakukan di dalam yurisdiksi negara lain tetapi juga untuk "tindak pidana yang dilakukan di luar yurisdiksi territorial Negara manapun". Khusus berkaitan dengan prinsip nasional aktif di perluas termasuk "pelaku yang di kemudian hari menjadi warganegara".
d. Prinsip perlindungan di perluas termasuk "kepentingan-kepentingan vital Negara lainnya" dan tidak terbatas hanya pada kepentingan kepala Negara dan keuangan atau ekonomi Negara serta tindak pidana yang dilakukan di dalam yurisdiksi negara lain tetapi juga untuk "tindak pidana yang dilakukan

di luar yurisdiksi territorial Negara manapun".

e. Prinsip universal di mungkinkan diperluas untuk tindak pidana tertentu yang dipandang sangat membahayakan umat manusia dengan berdasarkan Konvensi Internasional.

f. Prinsip*dual criminality* berlaku terbatas hanya dalam penerapan prinsip nasional aktif dan nasional pasif serta tindak pidana yang dilakukan berada dalamyurisdiks inegara lain. Bila *cybercrime* dilakukan di luar yurisdiksi Negara manapun tidak berlakuprinsip *dual criminality*. Penerapan prinsip *dual criminality* di dasarkan prinsip keadilan dan persamaan di depanhukum, sedangkan pembatasan prinsip *dual criminality* didasarkan prinsip "*no save haven*" bagi pelaku kejahatan *cybercrime*.

Dengan demikian yurisdiksi kriminal berlakunya hukum pidana nasional terhadap *cybercrime* tidak cukup dengan menggunakan prinsip yurisdiksi teritorial dan ekstra-teritorial yang diakui dalam hukum internasional publik tetapi juga berdasarkan prinsip yurisdiksi yang berlaku terhadap tindak pidana yang dilakukan di luar yurisdiksi negara manapun. Jadi yurisdiksi kriminal berlakunya hukum pidana nasional terhadap *cybercrime* menggunakan *quasi* yurisdiksi, yaitu menggunakan yurisdiksi teritorial, yurisdiksi ekstra-teritorial terhadap *cybercrime* yang dilakukan di dalam yurisdiksi negara lain, dan yurisdiksi ekstra-teritorial terhadap *cybercrime* yang dilakukan di luar yurisdiksi negara manapun.

Saat ini Indonesia memiliki 82 juta pengguna internet, dengan 57% diantaranya memilih berbelanja secara online. Transaksi elektronik yang coba diatur dalam UU ITE ini mungkin masih akan menemui banyak kendala, seperti misalnya ternyata 99,99% transaksi elektronik masyarakat Indonesia masih berbasis email sehingga diperlukan edukasi khusus untuk para pihak tentang pentingnya melakukan transaksi aman ketika melakukan transaksi elektronik.

Kedua adalah Penggunaan tandatangan digital setiap transaksi elektronik dan penyelenggara sertifikasi (*certificate authority*) di Indonesia. Pada pasal 11 UU ITE dinyatakan tandatangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah jika memenuhi persyaratan, yaitu:

a. Data pembuatan tandatangan elektronik terkait hanya kepada Penanda Tangan;

b. Data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;

c. Segala perubahanter hadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;

d. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;

e. Terdapat cara tertentu yang di pakai untuk mengidentifikasi siapa Penandatangannya; dan;

f. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

Penjelasan Pasal 5 UU 11 2008 tentang ITE bahwa:

a. InformasiElektronikdan/atauDokumenElektronikdan/atauhasilcetaknyamerupakanalatbuktihukum yang sah.

b. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

c. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

Jika melihat pada ketentuan tersebut diatas, transaksi elektonik berpotensi masalah, karena meskipun pada dasarnya menggunakan cara transaksi elektronik sesuai dengan UU tapi ternyata peraturan teknis yang mengatur hal ini masih dalam tahap pembahasan padahal seharusnya telah selesai dibuat pada tahun 2010 lalu. Seperti misalnya kita belum memiliki penyelenggara sertifikasi / (*certificate authority*)[2] yang terdaftar di Indonesia meskipun pada prakteknya, bisnis perbankan telah menggunakan beberapa penyelenggara sertifikasi yang telah diakui diluar negeri. Contohnya beberapa CA yang dipergunakan oleh layanan e-banking perbankan kita menggunakan CA yang berasal dari US dan masih belum terdaftar di Indonesia antara lain:

1) www.permatanet.com VeriSign International Server CA
2) ibank.klikbca.com Cyber trust Sure Server Standard Validation CA
3) www.bankbii.com VeriSign International Server CA
4) ebanking.lippobank.co.id VeriSign International Server CA
5) www.permatae-business.com VeriSign International Server CA

Saat ini Indonesia telah memiliki CA yang dibuat oleh TELKOM yaitu i-trust,

[2]CA merupakan sebuah badan hukum yang berfungsi sebagai pihak ke tiga yang layak dipercaya memberikan dan mengaudit sertifikat elektronik dan menyediakan layanan keamanan yang dapat dipercaya oleh pengguna dalam menjalankan pertukaran informasi secara elektronik.CA berkedudukan sebagai pihak ke tiga yang dipercaya untuk memberikan kepastian/pengesahan terhadap identitas dari seseorang atau pelanggan. CA mengatur berbagai regulasi kepercayaan transaksi elektronik dan berwenang menerbitkan (*issuer*) sertifikat digital, mengatur penggunaan tanda tangan digital, distribusi kunci publik dan privat sekaligus sebagai lembaga yang mengeluarkan *Trustmark* (sertifikasi keandalan) yaitu melakukan audit dan mengeluarkan sertifikat keandalan atas pelaku usaha dan produk berkaitan dengan kegiatan trasnsaksi elektronik. Aspek-aspek yang menjadi layanan CA adalah *confidentiality, authentification, Integrity,* dan *non repudiation.*Informasi yang terdapat di dalam sertifikat digital pada umumnya terdiri dari Identitas CA yang menerbitkan (*issuer*), pemegang/pemilik sertifikat (*subscriber*) dan batas waktu berlaku sertifikat.
Saat ini Indonesia telah memiliki CA yang dibuat oleh TELKOM yaitu i-trust, tetapi sayangnya CA TELKOM hanya sebatas melakukan sertifikasi terbatas pada server yang dioperasikan oleh pelanggan TELKOM dan belum melakukan sertifikasi secara umum dan komersil. Meskipun nantinya Indonesia memiliki CA sendiri, masalah lain yang menanti adalah apakah CA tersebut dipercaya oleh pengguna luar negeri sebagaimana diketahui Indonesia memiliki trackrecord kasus cybercrime termasuk kasus carding yang sangat tinggi.

tetapi sayangnya CA TELKOM hanya sebatas melakukan sertifikasi terbatas pada server yang dioperasikan oleh pelanggan TELKOM dan belum melakukan sertifikasi secara umum dan komersil. Meskipun nantinya Indonesia memiliki CA sendiri, masalah lain yang menanti adalah apakah CA tersebut dipercaya oleh pengguna luar negeri sebagaimana diketahui Indonesia memiliki trackrecord kasus *cybercrime* termasuk kasus carding yang sangat tinggi.

3. KejahatanKorporasi

Kejahatan korporasi dalam terkait dengan bidang ITE juga disinggung dalam peraturan ini, ketentuan yang terkait dengan kejahatan korporasi hanya terdapat dalam beberapa pasal antara lain, pasal 1 UU ITE yang memberikan perluasan definisi orang adalah perseorangan maupun badan hukum serta pasal 52 ayat 4 yang menyatakan tindak pidana dalam pasal 27 s/d pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah 2/3. Dalam penjelasannya yang dapat dikenakan pidana yaitu mereka yang mewakili korporasi, mengambil keputusan, melakukan pengawasan dan pengendalian serta melakukan kegiatan demi keuntungan korporasi. Ketentuan yang mengatur tanggung jawab korporasi pada undang-undang ini hanya mengenal sanksi terhadap individu, tidak seperti dalam UU 32 tahun 2009 mengenai lingkungan hidup yang memberikan sanksi terhadap korporasi berupa pembekuan/pencabutan izin korporasi tersebut.

Model tanggung jawab korporasi yang dianut oleh UU ITE ini masih sederhana, kurang jelas dan menggunakan pendekatan teori lama dimana penekanannya adalah kesalahan individu dan memberikan sanksi hanya terbatas pada individu belum menyentuk korporasi. Selama ini kita mengenal beberapa pendekatan pertanggungjawaban korporasi, antara lain teori *vicarious approach* yaitu Teori ini bertolak dari doktrin "*respondeat superior*" bahwa *master is liable in certain cases for the wrongful acts of his servant, and a principal for those of his agents*. didasarkan pada employment principle bahwa majikan adalah penanggungjawab utama dari perbuatan para buruh/karyawan; jadi "*the servant's act is the master's act in law*"., *indetification approach* yaitu perusahaan dapat melakukan sejumlah delik secara langsung melalui orang-orang yang sangat berhubungan erat dengan perusahaan dan dipandang sebagai perusahaan itu sendiri. Perbuatan/kesalahan "senior officer' diidentifikasi sebagai perbuatan/kesalahan korporasi, dan *strict liability* yaitu pertanggungjawaban pidana dapat dibebankan kepada pelaku tindak pidana yang bersangkutan dengan tidak perlu dibuktikan adanya kesalahan (kesengajaan atau kelalaian) pada pelakunya.

Pendekatan baru mengenai tanggung jawab korporasi disebut sebagai *orgazational model liability* yang menekankan pada kesalahan korporasi itu sendiri, tidak lagi hanya mengatribusikan kesalahan individu kepada korporasi. Pada teori ini berfokus pada tindakan atau kelalaian korporasi itu sendiri yang terlihat pada budaya korporasi yang memungkinkan terjadinya kejahatan tersebut.

Penutup

a. Kendala penerapan UU No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam hal kejahatan cyber yang dilakukan melalui layanan wifi Rumusan dalam UU ITE tidak mengkualifikasi kandelik sebagai kejahatan maupun pelanggaran

b. Penerapan yurisdiksi sangat sulit dilakukan karena berhadapan langsung deangan kedaulatan negara lain, yang dapat dilakukan adalah menjalin kerjasama (bias dalam bentuk *mutual assistance in criminal matters, mutual legal assistance, transfer of sentenced person, transfer of criminal proceeding, joint investigation, handling over*) dengan berbagai Negara terkait tindak pidana jika perbuatan tersebut dilakukan dari wilayah negara lain maupun dari warganegara lain.

c. Terkait dengan transaksi elektronik, saat ini CA yang digunakan dalam menjalankan *e-commerce* berasal dari luar negeri yang tidak terdaftar sebagai CA yang di akui oleh pemerintah. Pemerintah perlu mendorong pihak ketiga untuk menyelenggarakan CA yang diakui sebagaimana diamanatkan oleh UU ITE.

d. Ketentuan yang mengatur kejahatan korporasi masih sangat sederhana dan kurang jelas. Selain itu, pendekatan yang digunakan dalam menjerat pelaku kejahatan korporasi masih menggunakan pendekatan turunan dari pertanggungjawaban korporasi di mana masih mengatribusikan tindakan pelaku individu terhadap korporasi. Sanksi yang diberikan dalam UU ITE ini juga masih hanya terbatas pada sanksi individu belum menyentuh pada korporasi itu sendiri.

DAFTAR PUSTAKA

UU No 11 Tahun 2008 Tentang Informasi dan Teknologi Informasi

Ayu Putriyanti, Yurisdiksi di Internet, Media Hukum/Vol.IX/No2/April-Juni/ 2009, No ISSN 1411-3759.

Barda Nawawi, Yurisdiksi Cyber, bahan kuliah cyber crime.

Saiful Hidayat Pemanfaatan Certification Authority (CA) Untuk Transaksi Elektronik_Cyber Notaria

Syamsir Alam, Peranan Undang-Undang ITE Dalam Sistem Hukum Nasional, Kultura Volume: 11 No.1 Desember 2010

Bismar Nasution, Kejahatan Korporasi dan Pertanggungjawabannya, disampaikan dalam ceramah di jajaran Kepolisian Daerah Sumatera Utara, bertempat di Tanjung Morawa Medan, pada tanggal 27 April 2006.

M, Arsyad Sanusi. *Efektifitas UU ITE dalam pengaturan perdagangan elektronik.* Jurnal Hukum Bisnis.

Philemon Ginting, 2008. *Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana*. Thesis. Magister Ilmu Hukum Undip.

Sigid Suseno. 2014. Cybercrime Dan Keberlakuan Hukum Pidana Nasional. Hukum Pidana dan Kriminologi, Kerjasama MAHUPIKI Wilayah Yogyakarta dan Fakultas Hukum UGM.