PERBANDINGAN HUKUM PENGATURAN YURISDIKSI TINDAK PIDANA SIBER DI INDONESIA DAN DI AFRIKA SELATAN[1]

Oleh: Herlyanty Yuliana Anggraeny Bawole[2]

A. PENDAHULUAN

Berbagai penemuan di bidang teknologi, informasi, dan komunikasi saat ini memungkinkan orang menggunakan internet melalui komputer pribadi atau media elektronik lainnya, dimana kemajuan- kemajuan yang dicapai manusia tersebut telah banyak memberikan kemudahan-kemudahan dan manfaat bagi manusia dalam upayanya untuk meningkatkan kesejahteraan umat manusia. Teknologi informasi dan komunikasi saat ini dimanfaatkan oleh pribadi, korporasi, pemerintah dan kelompok-kelompok masyarakat untuk berbagai aktifitas manusia, seperti pendidikan, kesehatan, bisnis, pemerintahan, komunikasi, hiburan, dan lain- lain.

Namun demikian kemajuan- kemajuan di bidang teknologi, informasi, dan komunikasi tersebut juga di ikuti dengan dampak negatif yang mengancam dam membahayakan pembangunan sosial dan ekonomi umat manusia di dunia. Misalnya ancaman serangan terhadap sarana prasarana teknologi informasi dan komunikasi yang terkoneksi secara global, yang dapat membahayakan tidak hanya materi tetapi juga nyawa manusia. Teknologi digunakan untuk menciptakan atau menjadi sarana untuk melakukan tindak pidana. Dampak negatif dari kemajuan teknologi informasi dan komunikasi adalah munculnya tindak pidana baru di bidang teknologi informasi dan komunikasi, baik berupa tindak pidana terhadap data atau sistim komputer maupun tindak pidana yang dilakukan dengan menggunakan media teknologi informasi dan komunikasi alat. Semua tindak pidana yang dilakukan di *cyberspace* tersebut termasuk tindak pidana siber.[3]

Cyberspace merupakan tempat kita berada ketika kita mengarungi dunia informasi global interaktif yang bernama internet. Istilah ini pertama kali digunakan oleh William Gibson dalam novel fiksi ilmiahnya yang berjudul *Neuromancer*.[4] Cyberspace menampilkan realitas, tetapi bukan realitas yang nyata sebagaimana bisa kita lihat, melainkan realitas virtual (*virtual reality*), dunia maya, dunia yang tanpa batas. Inilah sebenarnya yang dimaksud dengan *borderless world*, karena memang dalam *cyberspace* tidak mengenal batas negara, hilangnya batas dimensi ruang, waktu, dan tempat, sehingga penghuni-penghuninya bisa berhubungan dengan siapa saja dan dimana saja.

Kemajuan –kemajuan yang dicapai manusia dalam kehidupan selalu di ikuti dengan tindak pidana baru yang menyertai kemajuan-kemajuan tersebut. Tindak pidana di bidang teknologi, informasi, dan komunikasi dilakukan dengan menyalahgunakannya untuk tujuan mengambil keuntungan financial atau keuntungan lainnya sehingga dalam pemanfaatan teknologi, informasi, dan komunikasi harus disertai dengan upaya untuk mengantisipasi, mencegah, dan memberantas tindak pidana siber tersebut. Pencapaian hasil pembangunan akan terhambat jika langkah-langkah tersebut tidak dilaksanakan secara konstruktif.

Tindak pidana siber di dunia, awal mula berkembang pada tahun 1988 yang pada saat itu lebih dikenal dengan istilah *Cyber Attack*. Pada waktu itu ada seorang mahasiswa yang berhasil menciptakan

---

[1] Artikel

[2] Dosen Pada Fakultas Hukum Universitas Sam Ratulangi Manado

2Majid., Yar., *Cybercrime and Society*, SAGE Publication, London, 2006, hal. 7.

[3] Mahzar, Ahmadi., Spritualitas Cyberspace, *Bagaimana teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*, Mizan, Bandung, 1999, hal. 9.

sebuah *worm* atau virus yang menyerang program komputer dan mematikan sekitar 10% dari seluruh jumlah komputer di dunia yang terhubung ke internet. Pada tahun 1994 seorang bocah sekolah music yang berusia 16 tahun bernama Richard Pryce, atau yang lebih dikenal sebagai "*the hacker*" alias "*Datastream Cowboy*", ditahan lantaran masuk secara illegal ke dalam ratusan sistem komputer rahasia termasuk pusat data dari *Griffits Air Force*, NASA, dan *Korean Atomic Research Institute* atau Badan Penelitian Atom Korea. Dalam interogasinya dengan FBI, ia mengaku belajar *hacking* dan *cracking* dari seseorang yang dikenalnya lewat internet dan menjadikannya seorang mentor yang memiliki julukan "Kuji". Hebatnya hingga saat ini sang mentor tidak pernah ia ketahui dimana tempatnya.

Berdasarkan data dari Internet World Stats tanggal 30 Juni 2010 jumlah penduduk Indonesia yang menggunakan internet meningkat mencapai 30 juta orang dari total penduduk Indonesia 242.968.342 orang atau dengan tingkat penetrasi 12,3 %. Kerugian-kerugian yang ditimbulkan oleh tindak pidana siber di Indonesia telah menimbulkan reaksi negatif dari negara-negara lain dalam transaksi bisnis secara *online*. Korban tindak pidana siber yang dilakukan oleh pelaku dari Indonesia tersebar di berbagai benua mulai dari Asia, Australia, Eropa sampai Afrika dan mencapai kerugian lebih dari 11,6 Milyar.[5] Melihat dari fakta yang terjadi pelaku dari Indonesia sudah tersebar di berbagai negara maka akan dilihat perbandingan hukum yurisdiksi antara Indonesia dengan negara lain dalam hal ini sebagai salah satu negara yang akan dibahas yakni Afrika Selatan.

[5] Febrian, Jack., *Kejahatan Yang Dilakukan Dalam Transaksi Secara Elektronik (melalui internet) dengan menggunakan Kartu Kredit orang lain secara illegal*, Informatika, Bandung, 2011, hal. 82.

B. PERUMUSAN MASALAH

Berdasarkan latar belakang masalah ini maka yang menjadi permasalahan adalah bagaimana perbandingan hukum pengaturan yurisdiksi tindak pidana siber di Afrika Selatan dan di Indonesia?

C. METODE PENELITIAN

Dalam menyusun tulisan ini penulis menggunakan metode penelitian kepustakaan (*Library Research*) yakni suatu metode yang digunakan dengan jalan mempelajari buku literatur, perundang-undangan, dan bahan-bahan tertulis lainnya yang berhubungan dengan materi pembahasan yang penulis gunakan untuk menyusun tulisan ini.

D. TINJAUAN PUSTAKA

Tindak pidana siber adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan yang utama. Tindak pidana siber ini merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet.

Tindak pidana siber juga dapat diartikan sebagai suatu perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet. Dalam perkembangannya kejahatan ini sering juga disebut kejahatan kerah biru atau kejahatan kerah putih.

Untuk mempermudah penanganan kejahatan ini, maka tindak pidana siber ini diklasifikasikan dalam beberapa kelompok, yakni:

- *Cyberpiracy* adalah penggunaan teknologi komputer untuk mencetak ulang *software* atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
- *Cybertrespass* adalah penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau individu.

- *Cybervandalism* adalah penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik dan menghancurkan data di komputer.

Jenis-jenis tindak pidana siber ada bermacam-macam bentuk yakni:

a. Berdasarkan jenis aktivitasnya
   - *Unauthorized Access to Computer and Service*
     Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.
   - *Illegal Contents*
     Kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Seperti pemuatan suatu berita yang tidak benar atau bohong yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi, pemuatan informasi rahasia negara, agitasi, dan propaganda untuk menentang pemerintahan yang sah.
   - *Data Forgery*
     Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi salah ketik yang pada akhirnya akan menguntungkan pelaku.
   - *Cyber Espionage*
     Kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem *computerized*.
   - *Cyber Sabotage and Extortion*
     Kejahatan dengan membuat gangguan perusakan atau penghancuran terhadap suatu data program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data program komputer atau sistem jaringan komputer yang telah disabotase tersebut dengan bayaran tertentu. Kejahatan ini sering disebut *cyberterrorism*.
   - *Offense Against Intellectual Property*
     Kejahatan yang ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Contohnya adalah peniruan pada tampilan *web page* suatu situs milik orang lain secara illegal, penyiaran

suatu informasi di internet yang ternyata ini merupakan rahasia dagang orang lain.

- *Infrigements of Privacy*
  Kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi secara *computerized* yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materiil maupun immaterial.
- *Cracking*
  Kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian tindakan anarkis begitu merekam mendapatkan akses. Biasanya terjadi salah penafsiran antara *hacker* dan *cracker*. Hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dirahasiakan tetapi ada pula yang bersifat dapat dipublikasikan.
- *Carding*
  Kejahatan yang menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan *credit card* orang lain sehingga dapat merugikan orang tersebut baik materiil maupun immaterial.

b. Berdasarkan motif
   - Tindak pidana siber yang menyerang individu
     Kejahatan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasaan pribadi. Contoh: Pornografi, *cyberstalking*, dll.
   - Tindak pidana siber yang menyerang hak cipta (hak milik)
     Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi atau umum demi materi maupun non materi.
   - Tindak pidana siber yang menyerang pemerintah
     Kejahatan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak, ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan atau menghancurkan suatu negara.

Setelah membahas tentang tindak pidana siber maka akan dijelaskan pula tentang yurisdiksi itu sendiri. Yurisdiksi atau jurisdiksi berasal dari bahasa Latin dari kata *iuris* dan *dicere*. *Iuris* artinya hukum sedangkan *dicere* artinya berbicara. Jadi, yurisdiksi adalah wilayah atau daerah tempat berlakunya sebuah undang-undang yang berdasarkan hukum.

Pada awalnya yurisdiksi merupakan konsekuensi logis dari kedaulatan negara atas wilayahnya. Yurisdiksi negara atas individu, benda dan lain-lain dalam batas wilayahnya (teritorial daratan, laut, dan udara) pada akhirnya dapat berkembang atau meluas melalui batas-batas negara (perluasan atas individu dan benda-benda yang terletak di negara lain). Hal ini merupakan salah satu dampak atau akibat dari semakin terbukanya hubungan internasional dan perdagangan internasional yang ada. Di sinilah perlu ada kesepakatan bersama.

Adanya proses yang berlangsung atau berkembang melalui kesepakatan bersama tersebut, hukum internasional menyusun aturan yang mengikat. Sebagaimana sering terlihat, kedaulatan yang dimiliki suatu negara, kadang-kadang menimbulkan konflik antar negara yang ada. Hal ini banyak terkait dengan adanya kewenangan

atau yurisdiksi yang dimiliki oleh satu negara terhadap individu, benda, dan lain-lain, misalnya seorang warga negara dari suatu negara melakukan kejahatan di banyak negara, dapat berkembang menjadi masalah pula di negara lain, persoalan tersebut masuk dalam lingkup yurisdiksi.

E. PEMBAHASAN

Pengaturan yurisdiksi kriminal berlakunya hukum pidana nasional terhadap tindak pidana siber berdasarkan prinsip-prinsip yurisdiksi berkaitan dengan batas-batas pelaksanaan yurisdiksi suatu negara dan berlakunya yurisdiksi negara dan berlakunya yurisdiksi negara lain. Dalam hukum pidana Indonesia pengaturan yurisdiksi kriminal berlakunya hukum pidana nasional terdapat dalam Kitab Undang-undang Hukum Pidana (KUHP) Buku I Pasal 2 sampai Pasal 9. Buku I KUHP yang mengatur pengertian dan asas-asas hukum pidana merupakan aturan umum (*general rules*) yang berlaku terhadap tindak pidana di dalam KUHP (Buku II dan Buku III) dan tindak pidana dalam perundang-undangan di luar KUHP, kecuali perundang-undangan di luar KUHP tersebut menentukan lain.

Pengaturan yurisdiksi kriminal terhadap tindak pidana siber terdapat dalam Pasal 2 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang pada dasarnya menyatakan bahwa:

> "Undang-undang ini 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 di wilayah hukum Indonesia atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia".

Ketentuan Pasal 2 ini merupakan aturan yurisdiksi yang bersifat khusus atau *lex specialis* dari aturan yurisdiksi dalam Buku I KUHP sehingga yurisdiksi kriminal dalam undang-undang ini hanya berlaku dalam tindak pidana terhadap undang-undang ini.

Dalam pemberantasan tindak pidana siber ketentuan baru mengenai yurisdiksi kriminal sangat penting karena keterbatasan yurisdiksi kriminal berlakunya hukum pidana dalam Buku I KUHP sehingga tidak dapat menjangkau perkembangan tindak pidana siber tertentu. Prinsip nasional aktif dengan tidak mensyaratkan prinsip *dual criminality* yang bersifat terbatas untuk tindak pidana dan dengan syarat prinsip *dual criminality* dapat menjadi celah untuk modus operandi tindak pidana siber dengan memanfaatkan belum adanya harmonisasi atau pengaturan tindak pidana siber di suatu negara.[6]

Penggunaan prinsip nasional dalam perkembangan tindak pidana siber bukan hanya untuk melindungi kepentingan-kepentingan khusus Indonesia seperti keamanan negara, kepala negara, dan wakil kepala negara yang kemungkinan besar tidak diatur dalam hukum pidana negara lain tetapi untuk jenis tindak pidana lainnya. Demikian pula prinsip perlindungan yang masih bersifat terbatas, karena kepentingan-kepentingan negara Indonesia sudah mengalami perkembangan tidak hanya yang berkaitan dengan masalah makar, kejahatan mata uang, dan surat utang.

Pengaturan yurisdiksi kriminal dalam Pasal 2 Undang-undang Informasi dan Transaksi Elektronik relatif singkat dan padat sehingga dalam implementasinya diperlukan penafsiran-penafsiran dan pengempangan terhadap prinsip-prinsip yurisdiksi dalam hukum internasional publik dan teori *locus delicti* dalam hukum pidana. Berdasarkan Pasal 2 ini prinsip yurisdiksi yang menjadi dasar berlakunya hukum pidana terhadap tindak pidana siber adalah:

[6] Suseno, Sigid., *YURISDIKSI TINDAK PIDANA SIBER*, Refika Aditama, Bandung, 2012, hal. 278.

1. Prinsip Teritorial
   Prinsip ini terkandung dalam rumusan Pasal 2 "yang berada di wilayah hukum Indonesia". Dalam rumusan selanjutnya juga ditegaskan prinsip territorial objektif, yaitu dalam rumusan "di luar wilayah hukum Indonesia". Di lain pihak dalam ketentuan ini tidak ada penegasan berlakunya prinsip territorial subjektif, yang sangat penting dalam pemberantasan tindak pidana siber yang seringkali perbuatannya dimulai di suatu wilayah negara dan penyelesaiannya atau efeknya ada di wilayah negara lain. Namun demikian prinsip teritorial subjekytf dapat digunakan dengan melakukan penafsiran.
2. Prinsip Perlindungan
   Prinsip ini terkandung dalam rumusan "di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia". Prinsip perlindungan dalam KUHP dan prinsip perlindungan pada umumnya yaitu untuk melindungi kepentingan vital suatu negara.

   Prinsip-prinsip yurisdiksi lainnya seperti prinsip nasional baik prinsip nasional aktif maupun nasional pasif tidak menjadi dasar berlakunya hukum pidana terhadap tindak pidana siber. Demikian pula prinsip bendera negara kapal dan prinsip pesawat negara terdaftar sebagai perluasan prinsip territorial tidak berlaku.

   Berkaitan dengan pengaturan yurisdiksi berlakunya hukum pidana menurut temapat maka Barda Nawawi Arief berpendapat bahwa pada dasarnya sudah diatur secara umum dalam KUHP yang didasarkan pada asas teritorial, asas nasional aktif, asas perlindungan, dan asas universal, sehingga Undang-undang di luar KUHP tidak perlu dibuat aturan tersendiri, kecuali akan mengatur hal khusus yang belum diatur KUHP. [7]

   Pengaturan yurisdiksi kriminal berlakunya hukum pidana dalam KUHP bersifat terbatas dan tidak dapat menjangkau berbagai perkembangan tindak pidana siber, sehingga tidak cukup apabila hanya menggunakan ketentuan dalam KUHP atau menegaskan prinsip-prinsip yurisdiksi dalam KUHP ke dalam undang-undang khusus. Demikian pula pengaturan yurisdiksi kriminal terhadap tindak pidana siber sehingga dimungkinkan untuk memperluas pengaturannya dengan menggunakan prinsip nasional pasif, prinsip perlindungan atau bahkan prinsip universal untuk tindak pidana siber.

   Upaya pengaturan yurisdiksi kriminal berlakunya hukum pidana terhadap tindak pidana siber adalah dengan mengaturnya dalam KUHP Nasional, namun tampaknya keinginan tersebut untuk situasi saat ini masih jauh dari harapan sementara kebutuhan pengaturan yurisdiksi kriminal terhadap tindak pidana siber sangat penting dan mendesak dilakukan sebagai implikasi yurisdiksi negara tindak pidana siber. Alternatif lain yang dapat dilakukan adalah dengan mengamandemen ketentuan pasal 2 sampai Pasal 9.

   Pengaturan yurisdiksi kriminal berlakunya hukum pidana dalam Rancangan KUHP sesungguhnya sudah mengakomodasi perkembangan penerapan prinsip yurisdiksi kriminal terhadap tindak pidana siber. Prinsip-prinsip yurisdiksi yang digunakan dalam Rancangan KUHP antara lain:
   1. Prinsip territorial
   2. Prinsip nasional aktif
   3. Prinsip nasional pasif

[7] Arief, Barda, Nawawi., *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Raja Grafindo Persada, Jakarta, 2006, hal. 49.

4. Prinsip perlindungan
5. Prinsip universal.

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

1. Prinsip teritorial baik prinsip 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 sebagaian dari akibat yang terjadi di wilayah negara dan penerapan doktrin efek untuk perluasan prinsip territorial objektif.
2. 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.
3. Prinsip nasional, 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 negara aktif diperluas termasuk "pelaku yang di kemudian hari menjadi warga negara".
4. Prinsip perlindungan diperluas 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".
5. Prinsip universal dimungkinkan diperluas untuk tindak pidana tertentu yang dipandang sangat membahayakan umat manusia dengan berdasarkan konvensi Internasional.
6. Prinsip *dual criminality* berlaku terbatas hanya dalam penerapan prinsip nasional aktif dan nasional pasif serta tindak pidana yang dilakukan berada dalam yurisdiksi negara lain. Bila tindak pidana siber dilakukan di luar yurisdiksi negara manapun tidak berlaku prinsip *dual criminality*. Penerapan prinsip *dual criminality* didasarkan prinsip keadilan dan persamaan di depan hukum, sedangkan pembatasan prinsip *dual criminality* didasarkan prinsip " *no save haven* " bagi pelaku tindak pidana siber.

Berdasarkan uraian di atas dan dengan memperhatikan karakteristik tindak pidana siber maka yurisdiksi kriminal berlakunya hukum pidana nasional terhadap tindak pidana siber tidak cukup dengan menggunakan prinsip yurisdiksi territorial dan ekstra-territorial yang diakui dalam hukum internasional publik tetapi juga harus berdasarkan prinsip yurisdiksi yang berlaku terhadap tindak pidana yang dilakukan di luar yurisdiksi manapun. Jadi yurisdiksi kriminal berlakunya hukum pidana nasional terhadap tindak pidana siber harus menggunakakn prinsip quasi yurisdiksi,

yaitu menggunakan yurisdiksi teritorial, yurisdiksi ekstra teritorial terhadap tindak pidana siber yang dilakukan di dalam yurisdiksi negara lain, dan yurisdiksi ekstra teritorial terhadap tindak pidana siber yang dilakukan di luar yurisdiksi negara manapun.

Pengaturan yurisdiksi kriminal terhadap tindak pidana siber di Afrika Selatan terdapat dalam Act no.25 of 2002 tentang *Electronic Communication and Transaction Act*, 2002. Dalam undang- undang ini diatur mengenai yurisdiksi yudisial dari pengadilan Afrika Selatan untuk mengadili tindak pidana yang dilakukan di luar wilayah Afrika Selatan. Pengaturan yurisdiksi yudisial dalam undang-undang ini didasarkan pada Konvensi Dewan Eropa 2001 tentang tindak pidana siber.

Afrika Selatan merupakan salah satu negara bukan anggota *Council of Europe* yang menjadi peserta dan penanda tangan konvensi tentang tindak pidana siber. Dalam ketentuan umum hukum pidana Afrika Selatan tidak mempunyai yurisdiksi terhadap tindak pidana yang dilakukan di luar wilayah Afrika Selatan.

Yurisdiksi kriminal berlakunya hukum pidana Afrika Selatan berdasarkan teritorial dan ekstra teritorial. Perumusan dalam pasal 90:

a. Tindak pidana dilakukan di wilayah Afrika Selatan
b. Tindak pidana termasuk tindakan persiapan dan sebagian dari tindak pidana dilakukan di dalam wilayah Afrika Selatan.

Hal ini didasarkan pada perkembangan yurisdiksi kriminal terhadap tindak pidana siber yang mempertimbangkan karakteristik tindak pidana siber yang seluruhnya dapat dilakukan dalam satu wilayah negara atau sebagian dari tindak pidana dilakukan di dalam satu wilayah negara dan sebagian tindak pidana terjadi di wilayah negara lain. Prinsip yurisdiksi dalam perumusan tersebut dapat didasarkan pada prinsip teritorial subjektif. Sedangkan perumusan selanjutnya dalam huruf b yaitu *"where any result of the offence has had an effect in the Republic"* merupakan penerapan prinsip teritorial objektif, yaitu efek atau akibatnya terjadi di dalam wilayah Afrika Selatan.

Yurisdiksi ekstra-teritorial sebagai perluasan penerapan yurisdiksi teritorial didasarkan pada prinsip nasional aktif sebagaimana perumusan dalam huruf c *(the offence was committed by a South African citizen*). Berdasarkan prinsip nasional setiap warga negara wajib mentaati hukum nasionalnya bahkan ketika berada di luar wilayah negaranya. Dalam perumusan huruf c, kewajiban untuk mentaati hukum nasional Afrika Selatan diperluas termasuk seseorang bukan warga negara Afrika Selatan yang sudah menjadi *permanent residence* di Afrika Selatan atau seseorang yang melakukan kegiatan bisnis di Afrika Selatan. Seseorang yang sudah memperoleh keuntungan dari Afrika Selatan dan memperoleh perlindungan hukum dari Afrika Selatan juga mempunyai kewajiban untuk menaati hukum nasional Afrika Selatan termasuk ketika berada di luar wilayah Afrika Selatan.

Penerapan prinsip nasional dalam *Electronic Communication and Transaction Act*, 2002 lebih luas dibandingkan dengan Konvensi Dewan Eropa 2001. Dalam Konvensi Dewan Eropa 2001 prinsip nasional dapat diterapkan dengan syarat : tindak pidana siber tersebut juga harus merupakan tindak pidana berdasarkan hukum negara tempat tindak pidana dilakukan atau tindak pidana dilakukan di tempat di luar yurisdiksi teritorial negara manapun. Pengadilan Afrika

Selatan mempunyai yurisdiksi terhadap warga negaranya yang melakukan tindak pidana siber di luar negeri semata-mata dengan berdasarkan kaitan antara Afrika Selatan dengan pelaku tindak pidana.

Prinsip yurisdiksi lain yang menjadi dasar penerapan yurisdiksi ekstra teritorial terhadap tindak pidana siber adalah prinsip bendera negara kapal dan prinsip pesawat negara terdaftar. Berdasarkan prinsip tersebut hukum Afrika Selatan mempunyai yurisdiksi terhadap tindak pidana siber yang dilakukan di dalam kapal yang berbendera Afrika Selatan atau pesawat yang didaftarkan berdasarkan hukum Afrika Selatan. Prinsip ini juga diperluas termasuk tindak pidana yang dilakukan di dalam kapal atau pesawat yang sedang dalam perjalanan atau penerbangan dari atau ke Afrika Selatan ketika tindak pidana dilakukan.

Pengaturan yurisdiksi kriminal dalam E*lectronic Communication and Transaction, Act,* 2002 Afrika Selatan lebih konfrehensif dibandingkan Konvensi Dewan Eropa 2001 yaitu dengan memperluas prinsip- prinsip yang ada dalam Konvensi Dewan Eropa 2001. Konvensi Dewan Eropa tentang tindak pidana siber telah mengatur hukum pidana substantive tentang percobaan/*attempt*, *aiding*, dan *abetting*.

Tujuan pengaturan yurisdiksi dalam Pasal 22 Konvensi Dewan Eropa 2001 adalah agar negara pihak dalam Konvensi menetapkan berlakunya yurisdiksi terhadap tindak pidana siber dalam hukum nasionalnya.pengaturan yurisdiksi ini juga dimaksudkan untuk menghadapi terjadinya dua atau lebih negara pihak yang menuntut yurisdiksi terhadap tindak pidana siber untuk menentukan *locus delicti* dan hukum mana yang harus digunakan, termasuk masalah *nebis in idem* dalam hal terdapat *multiple jurisdiction*. Termasuk juga bagaimana menyelesaikan terjadinya konflik yurisdiksi positif dan menghindari terjadinya konflik yurisdiksi negatif.[8]

Berdasarkan rumusan ketentuan Pasal 22 tersebut, tampak bahwa prinsip-prinsip yurisdiksi yang digunakan dalam Konvensi Dewan Eropa 2001 sebagai dasar berlakunya yurisdiksi kriminal terhadap tindak pidana siber yang mencakup prinsip territorial dan ekstra prinsip nasional.

- Prinsip Teritorial

Konvensi Dewan Eropa 2001 menempatkan prinsip teritorial sebagai dasar utama dalam menetapkan berlakunya yurisdiksi kriminal terhadap tindak pidana siber sebagaimana dirumuskan dalam Pasal 22 ayat 1 huruf a, yakni:

"Setiap negara pihak wajib untuk menjatuhkan pidana terhadap tindak pidana siber yang ditetapkan dalam Konvensi dan dilakukan dalam wilayah teritorialnya".

Negara pihak menyatakan dengan tegas yurisdiksi teritorialnya jika pelaku melakukan serangan terhadap sistem komputer dan korbannya berada dalam wilayah teritorialnya atau jika sistem komputer diserang di wilayah teritorialnya dan pelakunya berada di luar wilayah teritorialnya.

Sepanjang tindak pidana dilakukan di eilayah nasionalnya, dengan sendirinya dalam lingkup hukum nasionalnya, kekuasaan penegak hukum dapat menuntut dan mengadili terhadap tindak pidana tersebut. Lokasi fisik dapat diidentifikasi sebagai tempat ketika seseorang menggunakan perangkat sistem elektronik dengan maksud untuk memasuki, memulai

[8] Britz, Marjie., *Computer Forensic and Cyber Crimes, An Introduction*, Prectice Hall, New Jersey, 2009, hal. 27.

atau memelihara komunikasi elektronik. Pada lokasi tersebut untuk pengguna berlaku hukum nasionalnya berdasarkan prinsip teritorial. Instrumen elektronik dapat berupa sistem komputer , termasuk peralatan teknis untuk menembus sistem pengamanan dari sistem komputer dengan tujuan untuk mengakses sistem komputer tersebut. Lokasi fisik pelaku tindak pidana termasuk juga sistem yang menjadi target tindak pidana berada atau penggunaan instrumen elektronik berada dalam kendalinya.

Dalam kasus *computer related offence* misalnya, unsur-unsur "menyebarluaskan". "menawarkan", "membuat dapat diaksesnya", informasi yang bersifat kriminal menunjuk pada tindakan-tindakan dari lokasi fisik dimana pelaku tindak pidana berada.[9]akibat dari jenis tindak pidana seperti ini mungkin saja terjadi di wilayah negara lain dan oleh karena itu perbuatannya dianggap dilakukan di negara yang terakhir.

Pengaturan yurisdiksi iniberskaitan dengan sifat *ubiquitous* dari tindak pidana siber yang akan menimbulkan *multiple jurisdiction* atau konflik yurisdiksi. Hal ini karena kesulitan menentukan secara tegas lokasi:

a. Dimana pelaku tindak pidana melakukan perbuatan;
b. Dimana perangkat sistem elektronik digunakan; dan
c. Dimana kerugian akibat dari tindak pidana terjadi.

Secara teoritis hal ini akan menuimbulkan sejumlah konflik yurisdiksi di antara negara-negara.

Ketentuan ini tidak termasuk satelit karena satelit berfungsi untuk saluran transmisi, mengirim, dan menerima arus informasi dari dan ke satelit yang dikendalikan oleh stasiun bumi yang berada di wilayah negara tertentu.

- Prinsip Nasional

  Pasal 22 ayat (1) huruf d menjelaskan 2 (dua) kewajiban yang harus dilakukan negara pihak, yaitu:

  a. Negara pihak wajib menetapkan yurisdiksi terhadap tindak pidana siber dalam Konvensi yang dilakukan oleh warga negara di dalam wilayah negaranya dan perbuatan tersebut merupakan tindak pidana menurut hukum negara tersebut. Rasio dari prinsip nasional adalah setiap warga negara wajib untuk mentaati hukum dimanapun dia berada. Pembatasan prinsip nasional adalah dengan adanya persyaratan terpenuhinya *dual criminality*, yaitu bahwa perbuatan tersebut harus merupakan tindak pidana berdasarkan hukum negara tersebut.
  b. Negara pihak wajib menetapkan yurisdiksi terhadap tindak pidana yang dilakukan oleh warga negara pada suatu tempat di luar yurisdiksi teritorial setiap negara.

Ketentuan mengenai yurisdiksi dalam Konvensi Dewan Eropa 2001 tidak meniadakan yurisdiksi kriminal yang dapat diterapkan negara pihak dalam hukum nasionalnya tetapi negara pihak dimungkinkan untuk menetapkan yurisdiksi kriminal sesuai dengan sistem hukum nasionalnya.

F. PENUTUP

Dasar pengaturan yurisdiksi kriminal terdapat dalam Kitab Undang-undang Hukum Pidana (KUHP) Buku I Pasal 2 sampai Pasal 9 dan Pasal 2 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menganut prinsip territorial, prinsip bendera negara kapal dan prinsip pesawat negara terdaftar, prinsip nasional, prinsip perlindungan, prinsip universal, dan prinsip *dual criminality*. Sedangkan Pengaturan

[9] *ibid*, hal. 28

yurisdiksi kriminal terhadap tindak pidana siber di Afrika Selatan terdapat dalam Act no.25 of 2002 tentang *Electronic Communication and Transaction Act*, 2002 yang menganut prinsip dalam Konvensi Dewan Eropa 2001 yakni prinsip territorial subyektif, prinsip territorial obyektif, prinsip ekstra terirotial, prinsip nasional, prinsip bendera negara kapal, dan prinsip pesawat negara terdaftar.

Pengaturan yurisdiksi kriminal dalam Pasal 2 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik relatif singkat dan padat sehingga dalam implementasinya diperlukan penafsiran-penafsiran dan pengempangan terhadap prinsip-prinsip yurisdiksi dalam hukum internasional publik dan teori *locus delicti* dalam hukum pidana. Oleh karena itu, perlu adanya perluasan prinsip untuk meminimalisir dan menanggulangi berbagai tindak pidana siber yang semakin marak terjadi di Indonesia, seperti halnya Afrika Selatan yang memperluas prinsip dalam Konvensi Dewan Eropa 2001 untuk menentukan hukum negara mana yang harus digunakan jika melibatkan dua negara dalam tindak pidana siber dan perlu adanya upaya konsultasi antara dua negara tersebut agar tidak terjadi duplikasi permintaan yurisdiksi.

DAFTAR PUSTAKA

Arief, Barda, Nawawi., *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Raja Grafindo Persada, Jakarta, 2006.

Britz, Marjie., *Computer Forensic and Cyber Crimes, An Introduction*, Prectice Hall, New Jersey, 2009.

Febrian, Jack., *Kejahatan Yang Dilakukan Dalam Transaksi Secara Elektronik (melalui internet)* dengan *menggunakan Kartu Kredit orang lain secara illegal*, Informatika, Bandung, 2011.

Mahzar, Ahmadi., Spritualitas Cyberspace, *Bagaimana teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*, Mizan, Bandung, 1999.

Majid., Yar., *Cybercrime and Society*, SAGE Publication, London, 2006.

Suseno, Sigid., *YURISDIKSI TINDAK PIDANA SIBER*, Refika Aditama, Bandung, 2012