BAB III

UPAYA DAN KEBIJAKAN PEMERINTAH MEMERANGI

CYBER CRIME DI INDONESIA

Kebijakan dalam perundang-undangan mutlak diperlukan oleh para penegak hukum dan pemerintah untuk menaggulangi dan menindak pelaku kejahatan, sama halnya dengan tindak kejahatan mayantara (*cyber crime),* tentunya jenis hukum perundang-undangan haruslah sesuai dengan jenis kejahatan dan cara untuk mengungkap kasus kejahtan dunia maya. Maka dari itu sejak tahun 2008 pemerintah republik Indonesia sudah berkoitmen untuk memerangi kejahatan dunia maya.

Pemberlakuan dan pengesahan Undang-Undang Informasi Dan Transaksi Elektronik Tahun 2008 Atau UU ITE 2008 merupakan salah satu babak baru bagi pemerintah republik Indonesia untuk melawan kejahatan berbasis teknologi komunikasi dan informasi. Dengan aturan ini maka akan membuka jalan bagi penegak hukum untuk bertindak dan mengadili pelaku kejahatan teknologi informasi. Semakin pesatnya penggunaan teknologi maka semakin rawan untuk tingkat kejahatanya yang dilakukan oleh orang-orang yang tidak bertanggung jawab untuk melakukan aksinya baik penipuan, pencurian dan pencemaran nama baik melalui internet.

Pada bab ini akan dijelaskan bagimana dan apa sajakah upaya yang dilakukan oleh pemerintah indonesia dalam menindak kejahatan-kejahatan berbasis teknologi informasi dan komunikasi baik yang dilakukan di dalam negeri maupun oleh sindikat internasional yang beroperasi wilayah kedaulatan Negara Kesatuan Republik Indonesia.

A. Kebijakan Memerangi *Cyber Crime*

Kebijakan diartikan sebagai rangkaian konsep dan asas yang menjadi garis besar dan dasar rencana dalam pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak tentang pemerintahan , organisasi dam sebagainya. Pernyataan cita-cita, tujuan, Prinsip dan garis pedoman untuk manakjemen dalam usaha mencapai sasaran. Carl J Federick

sebagaimana dikutip Leo Agustino (2008:7) mendefenisikan kebijakan sebagai tindakan dan kegiatan yang disuslkan seseorang , kelompk atau pemerintahan dalam suatu lingkungan ternetntu dimana terdapat hambatan-hambatan, kesulitan dan kesmpatan-kesempatan terhadap pelaksanaan usulan kebijaksanaan tersebut dalam rengaka mencapai tujuan tertentu. Lingkup dari studi kebijakan publik sangat luas karena mencakup berbagai bidang dan sektor seperti ekonomi, politik, sosial, budaya, hukum dan sebagainya. Disamping itu dilihat dari hirarkinya kebijakan publik dapat bersifat nasional, tegional maupun lokal seperti undang-undang, peraturan pemerintah, peraturan presiden, peraturan menteri, peraturan daerah/provinsi, keputusan gubernur, peraturan daerah kabupaten/kota, dan keputusan bupati/walikota.

Secara *Terminology* kebijakan publik (*public policy*) itu ternyata banyak sekali, tergantung dari sudut mana kita mengartikanya Easton memberikan definisi kebijakan publik sebagai the *authorative allocation of values for whole society* atau sebagai pengalokasian nilai-nilai secara paksa kepada seluruh anggota masyarakat. Laswell dan Kaplan juga mengartikan kebijakan publik sebagai *a projected program of goal, value, and practice* atau sesuatu program pencapaian tujuan, nilai-nilai dalam praktek-praktek yang terarah. Pada sub bab ini akan dijelaskan pendekatan-pendekatan hokum apa saja yang telah dilakukan oleh pemerintah indonesia dalam menaggulangi kejahatan *cybercrime* Dalam rangka menaggulangi kejahatan diperlukan strategi yang mantap dari Negara dan masyarakat, dan harus dilakukan dengan cara bersama-sama secara simultan. Allan R.Coffey berpendapat sebagai berikut. strategi pencegahan kejahatan kenakalan dapat dilakukan melalui dua fokus utama yaitu

a) Usaha mencegah pelanggaran yang pertama
b) Mencegah penggulangan pelanggaran dan kejahatan.

Usaha pertama dilakukan dengan cara pencegahan sebelum melakukan penindakan dengan cara menggunakan sistem peradilan pidana. Sedangkan usaha yang kedua dilakukan dengan cara penetrasi melalui penetapan sistem peradilan pidana. Usaha penegakan hukum yang sukses perlu ditopang oleh masyarakat, baik pencegahan kejahatan preventif maupun

penindakan secara represif. Selanjutnya Allan R.Coffey [1] menguraikan bahwa dalam perencanaan startegi penaggulangan kejahatan ada 4 (empat) pendekatan umum yang dapat digunakan, yaitu.

A. Pengembangan program modifikasi pelaku
B. Pengembangan pelayanan jasa kelembagaan untuk pelanggar
C. Penciptaan jasa baru untuk kedua-duanya, yaitu pelanggar dan orang yang berpotensi melakukan pelanggaran
D. Pengembangan program untuk menetralkan pengaruh yang menggerakan anak-anak, seperti halnya orang dewasa agar tidak bergeser pada pelanggaran hukum.

Dalam rangka menerapkan kebijakan kriminal perlu dikombinasikan dengan berbagai aktivitas pencegahan dan pembenahan infarstuktur agar semua langkah terkordinasi secara menyeluruh dalam suatu pengorganisasian aktivitas yang sistematis. Pendapat ini dikemukakan oleh Karl O.Christiansen. Selain kebijakan preventif dan represif diatas, penulis juga mengutip dari sumber- sumber lain untuk menangani kejahatan konvensional maupun *cyber* teori yang dikutip adalah sebagai berikut. Penanggulangan kejahatan juga dapat dilaksanakan dengan cara melakukan kebijakan kriminalisasi karena didalam kebijakan tersebut terkandung aspek ancaman pidana yang dapat mempengaruhi pikiran atau bahkan dapat menyebabkan rasa takut kepada orang-orang yang berpotensi melakukan kejahatan. Hal ini dapat mempunyai dampak psikologis bagi masyarakat, terutama bagi orang-orang yang berpotensial melakukan kejahatan sehingga mereka tidak jadi melakukan kejahatan.

Sudarto berpendapat, bahwa pengertian kriminalisasi adalah proses penetapan suatu perbuatan orang sebagai suatu perbuatan pidana. Proses ini diakhiri dengan terbentuknya undang-undang yang mengatur bahwa perbuatan tersebut dapat dipidana.[2] Melihat teori kriminalisasi yang telah dikemukakan oleh sudarto penulis setuju jika untuk mencegah perbuatan kejahatan maka perlu diberlakukannya kriminalisasi dengan adanya aturan yang menyertakan sanksi-sanksi mulai dari yang ringan hingga yang paling berat berupa kurungan penjara seumur hidup maupun hukuman mati jika memang pelaku atau tersangka

[1] Allan R.Coffey
[2] Sudarto, *kapita selekta pidana*, bandung 1993

telah terbukti melakukan pelanggaran hukum dan kejahatan. Namun bagaimana jika kasus kejahatan berupa kejahatan dunia maya *(cyber*), dari data yang didapatkan oleh penulis melihat dari meningkatnya serangan dunia maya (*cyber*) dari tahun ke tahun di indonesia semakin lama-semakin meningkat, seiring dengan banyaknya pengguna internet di indonesia, lebih ironisnya lagi tingkat kejahatan semakin meningkat justru ketika pemerintah indonesia sudah memberlakukan UU ITE No 11 (Undang-Undang Informasi Dan Transaksi Elektronik) 2008. Fakta tersebut mengindikasikan masih banyak celah yang masih bisa dimanfaatkan oleh pelaku kejahatan dunia maya.

A. 1 Pendekatan Hukum Untuk Keamanan Dunia *Cyber* (Maya)

Pendekatan hukum bertujuan untuk menentukan langkah-langkah apa saja yang dilakukan dan diperlukan oleh para penegak hukum untuk menindak suatu perbuatan yang melawan hukum. Dalam dunia *cyber* terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace.* Yaitu yang pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya dan ketiga adalah pendekatan hukum. utuk mengatasi gangguan keamanan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi, atau diakses secara illegal dan tanpa hak. dalam kaitanya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu

1. ***Subjective Territoriality***

   Yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan dinegara lain
2. ***Objective Territoriality***

   Yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memebrikan dampak yang sangat merugikan bagi Negara yang bersangkutan
3. ***Nationality***

   Yang menentukan bahwa Negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku
4. ***Passive Nationality***

   Yang menekankan jurisdiksi berdasarkan kewarganegaraan korban

5. ***Protective Principle***

   Yang menyatakan berlakunya hukum didasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan diluar wilayahnya yang umumnya digunakan apabila korban adalah Negara atau pemerintah

6. **Asas *Universality***

   Selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus *cyber*. Asas ini disebut sebagai "*universal interest jurisdiction*". Pada mulanya asas ini menetukan bahwa setiap Negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini diperluas sehingga mencakup pula pada kejahatan kemanusiaan (*crimes against humanity*) misalnya genosida, pembajakan udara dan lain-lain. meskipun dimasa mendatang asas jurisdiksi universal ini mungkin dikembangkan untuk internet *piracy*, seperti *computer cracking, carding hacking, and viruses*. Namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan pada perkembangan hukum internasional [3]

A. 2 Kerangka Hukum Telematika

Membahas kerangka hukum dalam konteks dalam sistem telematika merupakan suatu tantangan baru dalam dunia hukum itu sendiri. Ketersediaan dan keterbatasan aturan-aturan hukum yang ada selama ini, "*memaksa*" aparat penegak hukum dan penagmbil kebijakan untuk menemukan penemuan hukum di bidang ini sehingga pututsan-putusan yang berkaitan dengan masalah-masalah telematika dapat memenuhi aspek keadilan, kemanfaatan dan kepastian hukum.

Hukum yang kemudian yang didefenisikan berdasar pada sudut pandang setiap orang sebenarnya memiliki ruang lingkup yang sangat luas sehingga ia dapat diartikan sebagai apa saja sesuai dengan paradigma hukum oleh masyarakat itu sendiri. Dalam hal ini, hukum dapat diartikan sebagai suatu disiplin, ilmu pengetahun, kaidah, dan tata hukum. Kedudukan hukum dalam ranah telematika, jika ditelaah lebih jauh juga memiliki implikasi

[3] Pendekatan Hokum Untuk Keamanan Dunia Cyber Serta Urgensi Cyberlaw Bagi Indonesia Hal 16 Danan Mursito Fakultas Ilmu Computer Universitas Indonesia 2005

bagi perubahan yang terjadi di masyarakat. Perkembangan teknologi informatika (telematika) telah melahirkan bias-bias lingkungan sekitarnya termasuk didalamnya masyarakat. Perubahan sosial yang timbul sebagai implikasi berkembangnya ranah telematika haruslah menempatkan hukum sebagai sandaran kerangka untuk mendukung usaha-usaha perubahan yang terjadi dalam masyarakat. Mochtar Kusumaatmadja mengatakan bahwa perubahan ketertiban dalam keteraturan merupakan tujuan kembar dari masyarakat yang sedang berubah (membangun) oleh karena itu, jika perubahan hendak dilakukan dengan tertib dan teratur, maka hukum adalah sarana yang tidak dapat diabaikan[4]. Perubahan karakter sosial dam budaya dalam masyarakat sebagai akibat perkembangan telematika tentunya merupakan fakta yang tidak dapat dihindarkan.

Perubahan karakter tersebut mengantarkan masyarakat pada pola "pengingkaran hakikat kemanusiaan manusia" sebagai mahluk tuhan yang berakal. Dampaknya dapat diprediksi bahwa masyarakat semakin tak terekendali hingga menyentuh titik kriminalisasi dari apa yang diperoleh dari perkembangan telematika tersebut. Oleh karena itu, hukum yang diharapkan lahir, apapun bentuknya haruslah memiliki kekuatan mengikat bagi para pihak di dalamnya (*legally bound*) yang tentunya dilengkapi dengan mekanisme sanksi sebagai alat pemaksa.

Menururt Grolier hukum dapat didefenisikan secara luas sebagai suatu standar sistem dan aturan yang ada di dalam masyarakat. Standar tersebut akan menjadi acuan bagi setiap individu yang akan melahirkan hak dan kewajiban. Sementara aturan-aturan akan menjadi pertimbangan dalam memperoleh, menciptakan, memodifikasi dan menegakkan hak dan kewajiban yang dilakukan oleh setiap individu. Tentunya, hukum sebagai suatu kesatuan sistem yang diakui oleh masayarakat haruslah berada dalam lingkup kewenangan Negara atau pemerintah yang menetukan mana yang boleh dan mana yang tidak. Pendapat Grolier tidak sepenuhnya benar dalam mendiskripsikan hukum khususnya dalam melihat peran pemerintah dalam mengatur apa yang boleh dan apa yang tidak oleh warga negaranya khususnya dalam bidang telematika, mengantarkan pada suatu perdebatan tersendiri. ada yang berpandangan bahwa pemerintah perlu dilibatkan, tetapi di sisi lain ada yang berpendapat sebaliknya. Pandangan lain tentunya menghendaki agar pemerintah sama

[4] Mochtar Kusumaatmadja

sekali tidak terlibat dalam urusan hukum, khususnya *cyber space*. paham ini dikonstruksi dari paham *deleglalization*, yang menjadi sebuah tren baru dalam pemikiran hukum pandangan ini berpandanan bahwa privatisasi kehidupan manusia harus dikembalikan oleh Negara yang di awali dengan konsep *the welfare state modern* itu, sedikit demi sedikit harus semakin di batasi. Keterlibatan hukum formal dalam aspek tertentu kehidupan manusia malah sering menimbulkan keruwetan dan ketidakadilan. Hukum semakin terbatas kemampuanya untuk memberikan solusi dalam berbagai *conflict of interest* warga masyarakatnya. Fakta menunjukan bahwa penggabungan telekomunikasi dan informatika telah melahirkan suatu fenomena yang telah mengubah konfigurasi model komunikasi konvensional[5].

Dalam dimensi ke tiga yang berimplikasi pada keterbatsan aturan-aturan hukum yang ada mengejar perubahan yang begitu cepat, oleh karena itu peran pemerintah sangatlah startegis dalam merusmuskan aturan yang menjadikan aturan main yang wajib di taati oleh setiap "*actor"* telematika. Sebelum lebih jauh menguraikan kerangka hukum yang tepat dalam bidang telematika. maka menarik untuk mengkaji dan menganalisis urgensi aturan-aturan hukum yang khusus yang mengatur masalah telematika.

Menyoal urgensi aturan-aturan ini diharapkan dapat menjawab keterbatasan aturan-aturan hukum klasik yang merupakan produk colonial dan nasional misalnya Kitab Undang-Undang Hukum Pidana (KUHP). Filosofi perlunya adanya aturan dan atau norma dalah untuk memebrikan tuntunan pada manusia dalam bertingkah dan berperilaku aturan atau norma diharapkan dapat menajdi rambu-rambu yang seharusnya ditaati dalam suatu komunitas. Keterbatsasan ketersediaan aturan hukum di bidang telematika secdara faktual menjadikan aturan atau norma di bidang ini penting untuk diadakan. Haruslah di akui pula bahwa beberapa Negara didunia dewasa ini belumlah memiliki aturan secara khusus dibidang telematika. Indonesia sendiri telah memiliki undang-undang teknologi informasi yang dikenal dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) yang diundangkan pada tanggal 21 april 2008.Signifikansi perkembangan teknologi komputer dengan telematika mengharuskan filosofi adanya aturan atau norma sebagai suatu yang tidak dapat diabaikan lagi. Dalam beberapa kasus

[5] Dikdik, M Arief Manshur

teleamtika. Warna dan tuntutan jaksa dan putusan hakim menjadi sesuatu yang, "meneglikan" (*ridiculous*). Akan tetapi hal ini tidaklah mengherankan di tengah keterpurukan sumber daya manusia dan keterbatsan aturan hukum telematika. Dalam kasus-kasus telematika yang terdahulu sebelum lahirnya UU ITE yang berkaitan dengan persoalan pidana, misalnya, aturan hukum yang digunakan selain undang-undang nomor 36 tahun 1999 tentang telekomunikasi adalah Kitab Undang-Undang Hukum Pidana (KUHP). padahal sangatlah disadari bahwa KUHP merupakan produk peninggalan zaman kolonial yang telah tertinggal secara materi (*substances*). Hal tersebut senada dengan apa yang dikemukakan oleh R. Kusuma Iwa Sumantri yang menagtakan bahwa KUHP yang berlaku sekarang ini berasal dari zaman penjajahan dimana terdapat ansir-ansir yang sama sekali tidak sesuai dengan keadaan sekarang.[6]

Berangkat dari deskripsi singkat tentang tertatihnya hukum mengejar kemajuan zaman, maka Chris Red merumuskan suatu kerangka telematika yang disebutnya sebagai hukum komputer.hukum ini dianggap sebagai cabang dari hukum yang berhubungan dengan teknologi informasi. Yang merupakan suatu perangkat aturan yang memiliki kelengkapan dalam menangani isu-isu yang dimunculkan dan dihasilkan oleh komputer. Hukum ini juga disebut sebagai uapaya dan usaha dari pembuat undang-undang dan penegak hukum dalam bergerak bersama menangani masalah teknologi yang kadang-kadang terlihat janggal.[7] Hal ini dapat dilihat dari beberapa kasus yang berkaitan dengan penyalahgunaan komputer seperti *carding, hacking*, dan lain sebagainya. Meskipun kebutuhan akan kerangka hukum di bidang telematika pada awalnya merupakan sesuatu yang harus dibuat, ternyata hal tersebut tidak sepenuuhnya di respon oleh para ahli hukum.

beberapa ahli hukum menganggap bahwa tidak diperlukanya suatu hukum khusus untuk memenuhi bidang baru ini, khususnya dibidang informatika, hal senada juga dikemukakan oleh beberapa pengacara (*lawyer*) yang mengatakan bahwa penting untuk membeicarakan isu-isu hukum yang relevan dengan komputer. Tetapi tidak terlalu jauh dari apa yang saat ini umumnya dikaitkan dengn label hukum komputer atau hukum teknologi informasi.[8] Terlepas dari kontroversi pro-kontra pentingnya suatu aturan khusus dibidang

[6] R. Iwa Sumantri 1985
[7] David Bainbridge 1996
[8] Asafa Endeshaw

telematika, sangatlah disadari bahwa bidang baru ini terus berkembang dengan tingkat kompleksitas yang sangat tinggi. Tentunya memerlukan suatu payung hukum yang mengatur seluruh permasalahan di bidang telematika. Oleh karena itu, kerangka pembentukan hukumnya harus dilihat dari berbagai aspek *rule of law the internet*, yurisdiksi dan konflik hukum.

Pengakuan hukum terhadap dokumen serta tanda tangan elektronik (*electronic signature*), perlindungan dan privasi konsumen, *cyber crime*, penagturan konten dan cara-cara penyelesain sengketa domain[9]. Oleh karena itu, keberadaan hukum telematika sebagai suatu pendekatan hukum interdisipliner yang dikaji berdasarkan perkembangan dan konvergensi telematika yang sebenarnya tidak hanya hidup dalam tataran wacana saja. Melainkan keberadaanya selaras dengan perbidangan hukum yang sesuai dengan dinamika masyarakat itu sendiri karena memepunyai tempat dalam sistem tata hukum[10]. Pendekatan hukum interdisipliner yang digunakan misalnya. Dapat dilihat dari beberapa aspek yang berkorelasi pada lahirnya kerangka hukum di bidang telematika seperti hukum telekomunikasi hukum perlindungan data dan hak pribadi, hukum media, hukum perikatan, hak kekayaan intelektual, hukum perlindungan konsumen, hukum pidana dan hukum internasional.

A. 3 Hukum Pidana

Kecanggihan teknologi komputer disadari telah memberikan kemudahan, terutama membantu pekerjaan manusia. Selain itu, perkembangan teknologi komputer menyebabkan munculnya kejahatan-kejahatan baru, yaitu dengan memanfaatkan komputer sebagai modus operandinya. Penyalahgunaan komputer dalam perkembanganya menimbulkan persoalan yang sangat rumit, terutama dalam kaitanya dengan proses pembuktian pidana. Penggunaan komputer sebagai media untuk melakukan kejahatan memiliki tingkat kesulitan tersendiri dalam pembuktianya. Hal ini dikarenakan komputer sebagai media memiliki karakteristik tersendiri atau berbeda dengan kejahatan konvensional yang dilakukan tanpa komputer. Kondisi objektif di atas memaksa Indonesia berupaya untuk mengoptimalkan KUHP, meskipun dalam subtansi pasal-pasal KUHP dapat saja di upayakan untuk mengakomodasi

[9] Dikdik M Arief Manshur dan Alitaris Gultom
[10] Edmon Makarim

modus kejahatan komputer, namun pertanyaan yang sering kali muncul kemudian adalah relevansi pasal-pasal tersebut dengan jenis kejahatan yang berkembang sekarang khususnya kejahatan komputer itu sendiri.

A. 4 Hukum *E-Commerce*

Dunia perdagangan atau bisnis yang berkembang sangat pesat menawarkan sebuah model atau system perdagangan yang inovatif dan kreatif mengikuti kemajuan teknologi yang tinggi di bidang media komunikasi dan informasi. Model itu tentunya juga dipahami sebagai konstruksi terhadap model perjanjian "klasik" yang selama ini dikenal. Meskipun berbeda secara bentuk, akan tetapi secara subtansi tetaplah sama dengan sentuhan modifikasi. Hukum Indonesia yang mengatur perjannian secara umumditemukan dalam kitab undang-undang hukum perdata pada buku III bab kedua tentang perakitan-perakitan yang dilahirkan dari kontrak atau perjanjian.

Pasal 1313 KUH Perdata menyebutkan bahwa perjanjian adalah, suatu perbuatan dengan nama satu orang atau kelompok atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih."dalam konteks yang sederhana mungkin perjanjian dalam bisnis yang berbasis komputer tidaklah masalah, akan tetapi dalam konteks yang lebih rumit, menjelma menjadi suatu masalah tersendiri khuusnya lingkup KUH Perdata. Apakah KUHP Perdata masih relevan atau tidak. Pada dasarnya, lingkup KUHP perdata yang selama ini dipahami menyajkan transaksi atau kontrak dalam bentuk tertulis (paper based). Hal ini disebabkan pemahaman konvensional yang menyebutkan bahwa transaksi yang dilakukan haruslah dalam bentuk "*hitam di atas putih*" yang harus disertai tanda tangan dan materai. Sementara transaksi dengan basis teknologi informasi lebih bersifat *electronic based*. Sistem ini dipahami sebagai perikatan ataupun hubungan hukum yang dilakukan secara elektronik dengan memadukan jaringan (*networking*) dari sistem yang berbasis komputer dengan sistem komunikasi yang berdasarkan jaringan dan jasa telekomunikasi yang selanjutnya difasilitasi oleh keberadaan jaringan komputer global internet (*network of network*)[11]. Oleh karena itu syarat sahnya perjanjian bertumpu pada apakah sistem elektronik dapat dipercaya atau berjalan sebagaimana mestinya.Kontrak atau transaksi pada hakikatnya terjadi ketika sebuah penawaran dari *offeror* diterima oleh *offere* dengan

[11] Edmon Makarim

kondisi-kondisi hukum yang jelas dengan tujuan untuk menciptakan hubungan hukum. Kondisi-kondisi hukum yang dimaksud tentu saja dengan adanya syarat-syarat hukum seperti adanya kesepakatan, kecakapan, objek tertentu serta adanya sebab yang tidak dilarang. Dalam perdagangan elektronik *(e-commerce*), bentuk kontraknya tertuang juga dalam kondisi-kondisi hukum sebagaimana di atas yang berlaku mutatis-mutandis. Akan tetapi, dalam kontraknya (*contents*) penggunaan peranti atau instrument menjadi sesuatu yang harus dipertimbangkan. Hal ini dikarenakan perbedaan bentuk penawaran dalam kontrak konvensional dalam bentuk konkret dan nyata, sementara kontrak dalam perdagangan elektronik dibuat dalam bentuk elektronik atau digital. Sehingga kesepakatan yang tercipta adalah melalui *online* penawaran dalam transaksi *e-commerce* juga dilakukan secara transparan, jelas, sering kali tanpa batas waktu, tanpa batas *audience* dan tanpa batas wilayah.

A .5 Hukum Perlindungan Konsumen

Konsumen bukanlah merupakan hal yang baru dalam literature kepustkaan pada hakikatnya setiap individu dalam aktivitas keseharinya adalah konsumen. Hanya dalam kedudukan sebagai konsumen seseorang tidaklah menyadari akan hak dan kewajiban yang melekat pada dirinya sebagai konsumen yang saat bersamaan adalah sesungguhnya haruslah dilindungi. Di indonesia perlindungan konsumen diatur berdasarkan Undang-Undang No 8 Tahun 1999 tentang perlindungan konsumen. Aturan khusus ini terasa membawa angin perubahan yang sangat diharapakan akan menjadi argumentasi hukum ketika perosalan-persoalan konsumen tampak di permukaan UU ini sebenarnya juga memberikan suatu posisi tawar bagi konsumen sekaligus menciptakan aturan main yang *fair* bagi semua pihak. Konsumen dalam pasal 1angka 2 UUPK disebutkan sebagai orang pemakai barang atau jasa yang tersedia dalam msayarakat, baik bagi kepentingan diri sendiri, keluarga, orang lain, maupun mahluk hidup.

Hal ini berarti konsumen adalah pemakai terakhir dan bukan konsumen antara, sehingga ia tidak harus terikat dalam hubungan jual beli sehingga dengan sendirinya konsumen tidak identik dengan pembeli. Menyadari lingkup perlindungan konsumen (UUPK) masih tertatih-tatih dalam merespon perkembangan telematika khsusnya transaski

di internet, maka perlu penajaman baik dalam bentuk penyempurnaan UUPK yang sudah ada (revisi) maupun membuat kebijakan yang relevan dengan hak-hak konsumen.

A .6 Hukum Telekomunikasi

Dalam kepustakaan hukum, pengsitilahan hukum telekomunikasi mungkin merupakan sesuatu yang baru. Akan tetapi, jika dirunut lebih jauh ternyata istilah tersebut bukanlah sesuatu yang baru. Pengisitlahan tata cara pengiriman pemanacaran atau penerimaan tanda-tanda sesungguhnya telah ada sejak abad ke 19. Dalam perkemabanganya hukum telekomunikasi sering berhadap-hadapan dengan hukum angkasa yang selama ini sering dianggap sebagai induk hukum telekomunikasi. Oleh karena itu beberapa ahli sepakat untuk memisahkan antara hukum telekomunikasi dan hukum angkasa.

Dalam praktik Negara-negara, ketersediaan arturan khusus di bidang telekomunikasi sangat menguntungkan bagi Negara-negara tersebut. Hal ini dikarenakan aturan-aturan tersebut (khususnya yang telah berbentuk UU) akan menjadi "tameng" dalam proses pelaksanaan tujuan kebijakan di bidang telekomunikasi. sebagaiamana tercantum dalam laporan *International Telecommunication Union* (ITU) yang dibuat pada tahun 1998 tentang reformasi telekomunikasi. Pada dasarnya suatu undang-undang dalam telekomunikasi didorong dan ditujukan untuk tiga hal, yaitu penciptaan aspek pasar yang sebelumnya belum berlaku, pemisahan regulasi dari fungsi operasional, dan liberalisasi kegiatan tertentu yang tadinya dilarang seperti kepemilikan asing, hal tersebut juga terjadi dalam undang-undang nomor 36 tahun 1999 dan contoh kompetisi dan liberalisasi dapat dilihat kasus indosat. Di indonesia perkembangan komunikasi sangatlah pesat. Hal tersebut tentunya berimplikasi pada kebutuhan untuk dibentuk aturan main tersendiri yang menagtur tentang telekomunikasi. Dalam konteks ini, pemerintah memebrikan respon berupa disahkanya Undang-Undang Nomor 36 Tahun 1999 tentang telekomunikasi. UU ini dapat dianggap sebagai momentum bagi pertelekomunikasian Indonesia.

A .7 Hak Kekayaan Intelektual

Hak Kekayaan Intelektual di atur dalam undang-undang domestik Indonesia seperti Undang-Undang Hak Cipta Diatur dalam Undang-Undang No. 19 tahun 2002, merek diatur dalam Undang-Undang No 15 Tahun 2001, paten diatur Dalam Undang-Undang No. 14

Tahun 2001, desain industri diatur dalam Undang-Undang No.31 Tahun 2000. Disamping itu, ketentuan alin dapat dilihat pada perjanjian internasional dimana Indonesia merupakan salah satu pihak perjanjian. Dalam kaitanya dengan telematika, *web site*, misalnya merupakan salah satu pilihan yang dapat digunakan untuk mendapat perlindungan merek dagang. Hak cipta atau paten. Dalam konteks merek, website tentunya, memiliki domain nama yang unik. Dengan memasukan nama sebuah *domain* dalam *web browser* akan menghubungkan pemakai dengan *web site* nama domain tersebut. Bisnis biasabya menggunakan merek daganganya sebagai nama *domain* untuk *web site* mereka.

Hal ini memudahkan bagi pelanggan yang sudah ada untuk mencari serta mengingat atau menebak nama sebuah nama *domain web site* suatu bisnis. Indonesia melindungi merek dagang berdasarkan pendaftaran pertama buka berdasarkan pemakaian pertama dengan pengecualian pada merek yang sudah terkenal. Hak cipta *web site* biasanya berisi grafis dan teks yang bersifat ekspresif yang dapat dihak ciptakan. Sementara dalam paten, sangat jarang penemuan dapat dilakukan *pada web site* kecuali seperti hak paten pada *amazon.com*, yaitu *one click shoping*. Masih banyak aktivitas hak kekayaan intelektual lainya yang dapat dilakukan dibidang telematika.

B. Undang-Undang Informasi Dan Transaksi Elektronik

Upaya untunk menghadirkan suatu perangkat hukum yang sesuai dengan perkembangan dunia informasi dan telekomunikasi menjadi sesuatu yang tidak bisa ditwar-tawar lagi. Pemerintah Indonesia melalui Kementrian Infromasi Dan Komunikasi (KOMINFO) yang bekerja dengan pihak stake holder dan universitas berupaya untuk mewujudkan asa itu. Akhirnya melalui pembahasan yang begitu “alot”, sebuah undang-undang yang secara khusus menyoal dan membahas permasalahan informasi dan transaksi elektronik diundangkan pada 21 april 2008 yang kemudian dikenal dengan Undang-Undang No. 11 Tahun 2008 Tentang Indormasi Dan Transaksi Elektronik (UU ITE) .

Komitmen pemerintah untuk melahirkan suatu produk khusus di bidang informasi dan transaksi elektronik dapat dikatakan merupakan jawaban dari keprihatinan yang timbul dalam praktik penegakan hukum di bidang telematika. Komitmen ini juga sebagai suatu bentuk pertanggungjawaban moral pemerintah terhadap masyarakat yang juga perwujudan

tugas Negara untuk melindungi warga negaranya, kedua komitmen dapat terlihat dengan jelas pada konsideran menimbang UU ITE yaitu:

a. Bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masayarakat.
b. Bahwa globalisasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya suatu pengaturan mengenai pengaturan informasi dan transaksi elektronik di tingkat nasional sehingga pembangunan teknologi informasi dapat dilakukan secara optimal. Merata dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan berbangsa.
c. Bahwa perkembangan dan kemajuan teknologi informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi bentuk-bentuk perbuatan hukum baru.
d. Bahwa penggunaan dan pemanfaatan teknologi informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan demi kepentingan nasional.
e. Bahwa pemanfaatan teknologi informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat.
f. Bahwa pemerintah perlu mendukung pengembangan teknologi informasi melalui infrastruktur hukum dan pengaturanya sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaan dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia.

Pada hakikatnya pemanfaatan teknologi informasi, media dan komunikasi telah mengubah perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia tanpa batas (*borderless*) dan telah menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi informasi kini telah menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan. Kemajuan, dan peradaban manusia. Sekaligus juga menjadi sarana efektif perbuatan melawan hukum. Lahirnya rezim hukum baru (UU ITE) yang dikenal dengan hukum telematika dapat dikatakan sebagai sebuah respon positif. Hukum telematika atau *cyber*

law, secara internasional digunakan istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*) dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi, baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang sering kali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi dan transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Adapun yang dimaksud dengan sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang di wujudkan dalam bentuk bahasa, kode, skema ataupun bentuk yang lain. apabila digabungkan dengan media yang dapat dibaca dengan Komputer akan mampu membuat komputer bekerja untukmelakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang juga merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalsis, menampilkan dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah penerapan dari perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakterisitk kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukkanya pada sisi yang lain. sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia dan subtansi informasi yang dalam pemanfaatanya mencakup fungsi

input, process, output, storage, dan *communication.* Sehubungan dengan itu, dunia hukum sudah sejak lama memeperluas penafsiran asas dan normanya keetika menghadapi persoalan kebendaan yang tidak terwujud, misalnya, dalam kasusu pencurian listrik sebagai perbuatan pidana. Dalam kenyataanya kegiatan siber tidak lagi sederhana karena kegiatanya tidak lagi diabatsi oleh batas wilayah (teritorial) suatu Negara, yang mudah di akses kapanpun dan dari manapun.

Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian pada kartu kredit melalui pembelanjaan di internet. Disamping itu, pembuktian meruapakn faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum Indonesia secara komprihensif. Melainkan juga sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit. Permasalahan yang lebih luas terjadi pula di bidang keperdataan karena kegiatan transaksi elektronik untuk bidang perdagangan melalui sistem elektronik *(electronic commerce)* telah menjadi bagian perdagangan nasional dan internasional.

Kenyataan ini menunjukan bahwa konvergensi di bidang teknologi informasi media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seirirng ditemukannya perkembangan baru di bidang teknologi informasi, media, dan komunikasi. Kegiatan melalui sistem media elektronik, yang disebut juga ruang siber (*cyber space),* meskipun bersifat virtual dapat diakategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan banyak hal yang lolos dari pemberlakuan hukum.

Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* antara lain dikenal dengan adanya dokumen elektronik yang kedudukanya disetarakan dengan dokumen yang dibuat diatas kertas. Berkaitan dengan hal

itu, pelu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media dan komunikasi.

Agar dapat berkembang secara optimal. oleh karena itu, terdapat tiga pendekataan untuk menjaga keamanan di *cyber space*. Yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan system secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal. Keseluruhan uraian di atas dapat dilihat pada sistematika UU ITE sebagai berikut.

I. BAB I Bersifat Ketentuan Umum
II. BAB II Berisi Asas Dan Tujuan
III. BAB III Berisi Informasi, Dokumen Dan Tanda Tangan Elektronik
IV. BAB IV Berisi Penyelenggaraan Sertifikasi Elektronik Dan Sistem Elektronik
V. BAB V Berisi Transaksi Elektronik
VI. BAB VI Berisi Nama Domain, Hak Kekayaan Intelektual Dan Perlindungan Hak Pribadi
VII. BAB VII Berisi Perbuatan Yang Dilarang
VIII. BAB VIII Berisi Penyelesaian Sengketa
IX. BAB IX Berisi Peran Pemerintah Dan Masyarakat
X. BAB X Berisi Penyidikan
XI. BAB XI Berisi Ketentuan Pidana (Sanksi)
XII. BAB XII Berisi Ketentuan Peralihan
XIII. BAB XIII Berisi Ketentuan Penutup

Oleh karena itu, dengan diberlakukanya UU ITE, diharapkan segala perdebatan tentang apa dan bagaimana untuk penyelesaian hukum apabila ditemukanya kasus-kasus yang berhubungan dengan informasi dan transaksi elektronik dapat terjawab, meskipun demikian walaupun sebagai produk perundang-undangan yang baru tentunya tantangan dimasa datang sangat banyak. Apalagi UU ini belum teruji keahlianya karena usia yang masih balita.

B. 1 Perbuatan Yang Dilarang Menurut UU ITE

Klasifikasi perbuatan yang dilarang dalam UU ITE dijelaskan dalam pasal 27 hingga pasal 37. Konstruksi pasal-pasal tersebut mengatur lebih detail tentang pengembangan modus-modus kejahatan tradisional sebagaimana yang tercantum dalam Kitab Undang-Undang Hukum Pidana (KUHP). Pasal 27 misalnya, mengatur masalah pelanggaran kesusilaan, perjudian, pencemaran nama baik dan tindakan pemerasan dan pengancaman. Adapun pasal-pasal yang mencantumkan mengenai perbauatn apa saja yang dilarang pada undang-undang ITE bisa dilihat pada lampiran pasal 27 sampai pasal 37. setiap ayat pada Sepuluh pasal tersebut sudah dengan jelas menetapkan perbuatan apa saja yang dilarang.

Walaupaun pemerintah sudah membuat Undang-Undang ITE No 11 Tahun 2008 tingkat kejahatan mayantara atau *cyber crime* di Indonesia justru semakin lama semakin meningkat di Indonesia. Berdasarkan data *Norton Report* tahun 2013, tingkat potensi dan resiko tindak kejahatan *cyber* di Indonesia sudah memasuki status darurat. Diungkapkan terdapat sekitar 400 juta korban kejahatan *cyber* di Indonesia tiap tahunya dengan kerugian finanasial mencapai USD 113 Miliar,

sementara menurut hasil riset yang dirilis oleh Indonesia *Security Response Team*, di tahun 2011 lalu saja tercatat kurang lebih 1 juta serangan *cyber* yang ditujukan para pengguna internet di Indonesia tiap harinya. Mayoritas serangan tersebut hadir dalam bentuk *malware* ataupun *phising* dan lebih menyasar pada institusi perbankan dan pemerintah.

B. 2 Yurisdiksi

Sebelum menyoal masalah yurisdiksi *cyber space* lebih spesifik, terlebih akan dijelaskan bahasan yurisdiksi secara umum dalam konteks hukum internasional. Yurisdiksi diartikan sebagai kekuasaan atau kompetensi hukum Negara terhadap orang, benda atau peristiwa hukum. Yurisdiksi ini dipandang sebagai refleksi dari prinsip dasar kedaulatan Negara, kesamaan derajat Negara, dan prinsip tidak campur tangan. Dalam pandangan. Shaw[12],

[12] M.N Shaw 1986

yurisdiksi dipnadang sebagai suatu kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum. Meskipun disadari makna yurisdiksi selalu berkasit dengan persoalan wilayah, namun dalam praktik tidaklah mutlak sifatnya. Negara-negara lain pun dapat mempunyai yurisdiksi untuk mengadili suatu tindak pidana meskipun tindak pidana itu dilakukan diluar negerinya.[13] Hukum internasional dalam teori dan praktik sesungguhnya telah meletakan prinsip-prinsip yang berkaitan dengan yurisdiksi suatu Negara. Prinsip-prinsip tersebut adalah.

C. Prinsip Territorial

Menururt prinsip ini, setiap Negara memiliki yurisdiksi terhadap kejahatan-kejahatan yang dilakukan didalam wilayahnya. Prinsip ini dipandang sebagai prinsip yang fundamental dalam hukum internasional ketika menyoal masalah yurisdiksi.[14] Dalam hal ini, penting untuk menyimak apa yang dikemukakan oleh loed macmillan bahwa, *It is essential attribute of the sovereignty of this realm, as of all sovereign independent states, that is should posses jurisdiction over all person and things within its territorial limits and in all causes civil and criminal arising within this limits*.[15]

Dalam praktik sering ditemui bahwa prinsip territorial ini sering diklaisfikasikan ke dalam prinsip territorial subjektif dan prinsip teritorial objektif. Lebih jelasnya dapat dilihat pada contoh dimana seseorang yang berdiri dekat perbatasan dua Negara dan menembak orang lain yang telah berada dalam yuridiksi Negara lain yang mengakibatkan orang tersebut terluka pertanyaan yang kemudian timbul adalah Negara mana yang memiliki yurisdiksi atas kasus penembakan tersebut?

Jawaban dapat keduanya. Hal ini dapat diartikan bahwa Negara dimana si penembak menembakan senjata berada di bawah prinsip territorial subjektif, sedangkan Negara dimana si korban tertembak tunduk pada prinsip teritorial objektif. Dalam konteks sebagaimana kasus diatas, Hyde memberikan pengertian prisnsip teritorial sebagai berikut *"The setting in motion outside of states which produce as a direct consequences an*

[13] Huala Adolf 1991
[14] D.J .Harris, 1998
[15] Huala Adolf

injuries effect therein justifies territorial sovereign in prosecuting the actor when he enters its domain".

Merujuk pada pendapat Hyde, Glanville Williams mengatakan bahwa sangat erat kaitanya antara suatu Negara dengan kompetensi yurisdiksinya. Keeratan hubungan tersebut tertuang dalam bentuk:[16]

a. Negara dimana suatu perbuatan tindak piadana/kejahatan dilakukan biasanya mempunyai kepentingan yang paling kuat untuk menghukumnya:
b. Biasanya pelaku kejahatan ditemukan ditempat Negara ia melakukan tindak pidana/kejahatan
c. Biasanya *local court* (pengadilan setempat) dimana tindak pidana/kejahatan terjadi adalah yang paling tepat, karena saksi-saksi termasuk di dalamnya barang buktinya dapat ditemukan di Negara tersebut
d. Adanya fakta bahwa adanya sistem–sistem hukum yang berbeda, dan karenanya akan janggallah, misalnya seorang amerika yang datang ke London harus tunduk pada dua sistem hukum, yaitu sistem hukum amerika dan/atau sistem hukum London.

Oleh karena itu, dalam perkembanganya prinsip teritorial ini bukan hanya berlaku terhadap hak lintas di laut teritorial terhadap kapal berbendera asing di laut territorial, pelabuhan terhadap orang asing dan/atau terhadap tindak pelaku pidana akan tetapi, dapat mengalami perluasan makna yang meliputi tindak pidana yang dilakukan dengan media komputer/internet (dunia maya) yang bersifat *untouchable*

C. 1 Prinsip Nasionalitas

Menurut prinsip ini, suatu Negara dapat mengadili warga negaranya terhadap kejahatan-kejahatan yang dilakukan di manapun juga. Dalam hal ini prinsip nasionalitas dibedakan atas

a. **Prinsip nasionalitas akfif**. Menurut prinsip ini, suatu Negara memiliki yurisdiksi terhadap warga negaranya yang melakukan tindak pidana di luar

[16] Ibid

negeri. Dalam hal mengadili, tentunya orang terebut harus diekstardisikan terlebih dahulu.[17]

b. **Prinsip nasionalitas pasif**. Menurut prinsip ini, suatu Negara memiliki yurisdiksi untuk mengadili orang asing yang melakukan tindak pidana terhadap warga negaranya di luar negeri.

C. 2 Prinsip Perlindungan

Menururt prinsip ini, suatu Negara dapat melaksanakan suatu yurisdiksinya terhadap warga Negara asing yang melakukan kejahatan di luar negeri yang diduga dapat mengancam kepentingan keamanan., integritas dan kemerdekaan, misalnya komplotan yang bermaksud menggulingkan pemerintahan yang sah suatu Negara, dapat pula kegiatan yang menyelundupkan mata uang asing, kegiatan spionase atau kegiatan yang melanggar perundang-undangan integrasi suatu bangsa. Prinsip yang dipandang sebagai prinsip yang berupaya untuk melindungi kepentingan vital suatu Negara.

Dalam hal ini dapat saja ditemukan seseorang yang dapat melakukan suatu kegiatan (dapat dikategorikan sebagai tindakan pidana) yang didalam negerinya bukanlah suatu tindak pidana, akan tetapi dalam lingkup internasional hal-hal tersebut dapat di kategorikan sebagai tindak pidana. Dalam praktiknya hampir seluruh Negara menerapkan prinsip ini, namun tidak demikian halnya dengan Amerika Serikat dan Inggris yang tidak lazim yang menggunakan prinsip ini[18] beberapa contoh dimana prinsip ini diterapakan dapat dilihat pada beberapa kasus kejahatan politik dan pelaksanaan doktrin zona tambahan (*contiguous zone*),[19]

dalam hal ini Negara-negara pantai menetapkan jalur *contiugous zone* dengan tujuan untuk melindungi kepentingan tertentu Negara-negara pantai terhadap kejahatan-kejahatan orang asing diluar wilayah kedaulatanya. Dalam kaitanya dengan kejahatan siber, maka seyogyanya prinsip ini dapat diterapakan dengan melihat aktivitas-aktivitas yang dilakukan dengan memanfaatkan teknologi yang dapat berakibat timbulnya kecemasan dan kehawatiran terhadap persolan keamanan, integritas dan kemerdekaan.

---

[17] Ibid
[18] DJ Harris
[19] Ibid

C. 3 Prinsip Universal

Menururt prinsip ini, setiap Negara memiliki yurisdiksi untuk mengadili tindak kejahatan tertentu. Prinsip ini diterima secara umum karena tindakan kejahatan tersebut dianggap sebagai tindak kejahatan yang mengancam masyarakat internasional secara keseluruhan. N.A Maryan Green berpendapat bahwa terhadap kejahatan-kejahatan seperti obat-obatan terlarang, pembajakan, aphertaid dan kejahatan terhadap diplomat, selain Negara memiliki yurisdiksi, Negara-negarapun memiliki hak dan bahkan kewajiban untuk menghukumnya.[20]

Dalam praktik Negara-negara, kegiatan pembajakan *(piracy*) dan kejahatan perang telah mendapat pengakuan oleh masyarakat internasional dengan menerapkan prinsip universal dalam menghukum pelakunya. Sebagai buktinya dapat dilihat pada eksistensi kedua kejahatan di atas yang dapat ditemukan dalam konvensi hukum laut III (UNCLOS III) 1982 dan *International Criminal Court* (ICC). Uraian tentang prinsip-prinsip yurisdiksi yang dimiliki oleh suatu Negara akan menjadi rujukan dalam *cyber space.*

C. 4 Kebijakan NonPenal Untuk Memerangi *Cyber Crime*

Dalam kaitanya dengan upaya memerangi *cyber crime* melalui sarana nonpenal, muladi berpendapat sebagai berikut.

1. Perlu dirumuskan dahulu model undang-undang paying (*umberella act*) yang mengatur ttentang kebijakan tentang komunikasi massa baik yang berbentuk cetak, penyiaran maupun *cyber*.
2. Perlu dirumuskan secara professional penyususnan kode etik, *Code Of Conduct And Code Of Practice* tentang penggunaan teknologi informatika.
3. Perlu kerjasama antar semua pihak yang terkait termasuk kalangan industri untuk mengembangkan *preventive technology* menghadapi *cyber crime*, sebagai contoh adalah pengembangan *cyber patrol software* yang dapat digunakan oleh *internet service provider* (ISP) atau *Internet Content Provider* (ICP) untuk menyaring atau mem-blok akses ke situs tertentu secara otomatis apabila situs tersebut telah masuk

[20] N.A Maryan Green 1978 *International Law Peace*

dalam *balcklist*. Hal ini didasarkan fakta bahwa internet memang bukan jaringan yang aman[21].

Dalam kontek kebijakan non-penal, Muladi menyatakan bahwa perlu juga dilakukan upaya berikut

A. Kerjasama Internasional

Sifat *cyber crime* adalah transnasional, karena itu diperlukan kerjasama internasional yang intensif baik dalam penegakan hukum pidana maupun dalam bidang teknologi berupa pembentukan jaringan informasi yang kuat, misalnya program "*24 Hours Point Of Contact*" untuk menghadapi kejahatan *cyber crime*. Pelatihan personil penegak hukum yang memadai, harmonisasi hukum dan penyebarluasan kesepakatan-kesepakatan internasional. Dalam meningkatkan kemampyan polisi dalam menagngani *cyber crime*, tahun 2013 divisi *cyber crime* polda metro jaya bersama *Australia Federal Police* (AFP) meresmikan kantor *Cybercrime Investigation Satellite Office* (CCISO), kerjasama tersebut dilakukan agar dapat terus memerangi *cyber crime* yang dampaknya semakin menghawatirkan. Rencananya, selain ada di poda metro jaya CCISO juga aka nada di mabes polri, polda suamtra utara, polda bali, dan polda nusa tenggara barat. Bahkan pada masa mendatang CCISO akan diadakan di semua polda. Polda metro jaya menerima sekitar 800 kasus *cyber crime* pertahun.Sebelum ada kerjasaama dengan AFP tersebut pengungkapan kasus *cyber crime* relatif sedikit namun, setelah ada kerjasama dengan AFP mulai juni 2012 penelesaian kasus mencapai 40% kasus yang masuk ke kepolisisan bahkan, dengan sudah beroperasinya CCISO yang lengkap dengan semua peralatanya, polisis menargetkan penyelesaian kasus *cyber crime* sebesar 60% pertahun.

B. Rencana Aksi Nasional (*National Action Plan*)

Dalam ruang lingkup nasional perlu disusun suatu aksi rencana nasional (*National Plan For Action)* untuk menaggulangi *cyber crime*, karena proses viktimasi kejahatan tersebut sangat luas dan sifatnya transnasional. Pemerintah dan beberapa komunitas teknologi informasi nasional perlu menggalang kerjasama guna

[21] Muladi, demokratisasi , hak asasi manusia dan reformasi hokum di indonesia Jakarta 2002.

menanggulangi kejahatan di dunia maya (c*ybercrime*).[22] Kegiatan tersebut misalnya melalui pendirian *Indonesia On Forum Information For Infocom Incident Response And Security Team* (ID-FIRST) yang diharapkan menciptakan sinergi antara pemerintah, kepolisian, dan industry teknologi informasi dalam mencegah dan memeberantas kejahatan dunia maya melalui internet.[23]

C. 5 Yurisdiksi di Ruang Maya

Pemikiran-pemikiran tradisional atas yurisdiksi didasarkan pada geografi dan kontak fisik yang dimiliki terdakwa dengan forum (baik secara langsung atau dengan jalan mengirimkan produk). Tetapi internet memungkinkan adanya peluang untuk kontak visual. Mengingat sifat kontak di internet kontak seorang terdakwa dengan forum mungkin seluruhnya bersifat *online*, dan kontak fisiknya dengan forum tidak ada. Maka yursidiksi diri atas seseorang pengguna internet yang hanya memiliki kontak *online* dengan forum akan didasarkan pada sifat kontak tersebut.

Berdasarkan uji kontak minimum tradisional, perolehan keuangan menunjukan bahwa seorang terdakwa telah mendapatkan manfaat dari forum. Jika seorang pengguna internet menghasilkan uang di forum. Ini mungkin merupakan indikasi bahwa pengguna hendaknya dikenal tuntutan di forum tersebut. Tapi perbuatan di internet sering kali tidak terarah ke forum. Terutama jika produk di *download* langsung (misalnya perangkat lunak atau musik) si penjual tidak mengetahui lokasi fisik pembeli. Jasa-jasa informasi lainya dapat ditawarkan sepenuhnya *online* (misalnya pemantauan sistem pendidikan, pengolahan data dan konsultasi). Pembayaran lewat kartu kredit dapat menggunakan identitas seseorang pelanggan tetapi bukan lokasinya. Dan pembayaran dengan uang tunai digital bahkan lebih sulit dilacak. Demikian pula, perbuatan lain yang tidak diarahkan untuk menghasilakn uang dapat dikenai gugatan,sebagai contoh komunikasi pribadi dan kelompok diskusi dapat memunculkan gugatan kerugian (misalnya pencemaran nama baik atau fitnah).

Sulit pula bagaimana pemakaian tertentu internet dipandang sebagai "pemanfaatan keuntungan dari forum" sebagai contoh meskipun seorang pemakai mungkin meminta

[22] ibid
[23] *Indonesia Bentuk ID FIRST,* Harian Sinar Harapan 21 Maret 2003

sebuah informasi dari komputer induk di forum. Sipemakain biasanya tidak tahu (dan tidak peduli) dimana komputer induk terebut berada. Demikian pula bila suatu usaha, internet tidak mengetahui lokasi pembeli *downloadnya* sulit menyimpulkan bahwa bisnis itu hendaknya mengantisipasi diseret ke pengedilan di forum pembeli.Jadi yursdiksi diri di dunia maya adalah memebingungkan mengingat masih begitu barunya pertumbuhan perdagangan di internet, pengadilan belum cukup memahami masalah-masalahnya untuk dapat menetapkan standar yang terperinci.

Berdasarkan uraian tentang yurisdiksi *cyber crime* tersebut, baik pidana maupun perdata sebagimana dijelaskan diatas, menunjukkan bahwa yurisdiksi universal menjadi pilihan yang paling baik untuk sementara ini dalam menyelesaikan persoalan yurisdiksi *cyber crime.*[24] Namun bagi indonesia yang nota benenya terhitung Negara yang masih baru dalam mengesahkan peraturan perundang-undangan dalam hal ini UU ITE 2008, dapat dikatakan hingga saat ini indonesia masih belum bisa mengikuti konsep yurisdiksi universal tersebut.

D. Sindikat *Cyber Crime* Internasional Cina (Tiongkok) di Indonesia

Sebagai bahan pengamatan kasus sindikat yang ada di indonesia adalah kasus sindikat *cyber crime* asal Negara tiongkok yang berhasil diungkap oleh mabes polri, sindikat ini merupakan motif penipuan dan pemerasan terhadap korban yang merupakan warga Negara tiongkok juga. Informasi yang didapatkan oleh Mabes Polri merupakan informasi dari pihak ototritas tiongkok yang memberikan laporan mengenai adanya sindikat tersebut. Walaupun pelaku sindikat *cyber crime* tiongkok berhasil diamankan dan diungkap oleh polri tetapi para pelaku tidak dapat diadili oleh penegak hukum di indonesia dan hanya dideportasi atas pelanggaran keimigrasian di Indonesia dikarenakan pelaku kejahatan *cyber* dan korban bukan merupakan warga Negara Indonesia. Tentunya hal ini akan menjadi kerugian bagi penegak hukum indonesia walaupun pelaku dan korban bukan warga Negara Indonesia namun tempat beroperasinya berada di wilayah kedaulatan hukum Indonesia.

Di sisi lain ketika penggerbekan dilakukan oleh tim Mabes Polri. Pihak Satuan Direktorat Reserse Kriminal Umum polri mengamankan pelaku yang berjumlah puluhan orang dalam satu rumah yang terdiri dari wanita dan pria, ketika diperiksa dari dokumen

[24] Kenny Wiston 2002 the *Internet Issuses Of Jurisdicto And Controversies Sorounding Domain Names*

paspor para tersangka mereka berasal dari Cina, Taiwan Dan Hongkong. Selain itu pihak kepolisisan juga telah menyita barang bukti berupa pulihan alat komunikasi berupa puluhan unit telpon genggam/handphone, laptop/computer dan peralatan elektronik lainya.

Modus yang digunakan adalah dengan motif penipuan dan pemerasan, para pelaku menyamar sebagai penegak hukum spserti kepolisian, kejaksaan dan petugas pajak pemerintah tiongkok. Para korban adalah warga Negara tiongkok yang terkena kasus hukum seperti kasus korupsi, penggelapan pajak dan kasus criminal lainya. Para tersangka mengancam para korban agar memudahkan proses penyelesaian kasus hokum para korban dapat diselesaikan dengan cepat, jika tidak mengikuti perintah para tersangka maka akan diancam berupa hukuman yang yang akan diterima oleh korban

Gambar 3.1 Barang Bukti Sindikat Cyber Tiongkok

Sumber (liputan6.com)

Gambar 3.2 Barang Bukti Sindikat Cyber Tiongkok

Sumber (CNN Indonesia)

Gambar 3.3 Tersangka Sindikat Cyber Tiongkok

Sumber (detik.com)

Dengan adanya peristiwa ini diharapkan pemerintah bisa secepatnya menerapkan dan mengikuti prinsip hukum universal sehingga pelaku bisa di adili dengan hukum Indonesia. Dilihat dari peralatan elektronik dan komunikasi yang digunakan oleh tersangka, bisa dilihat bahwa pengawasan terhadap pemakaian fasilitas internet dan komunikasi masih sangat minim. Bayangkan saja dalam penggerbekan dirumah kontrakan para tersangka

petugas reserse criminal umum telah menyita puluhan alat komunikasi telpon dan laptop. Mudahnya mendapatkan izin untuk pemasangan fasilitas internet juga disinyalir sebagai penyebab para tersangka dengan leluasa menipu para korban. Jika peristiwa ini terus terjadi maka bukan tidak mungkin dunia internasional akan memasukan indonesia ke dalam *blacklist* dalam kasus dunia maya sehingga akan merugikan masyarakat indonesia dimasa-masa yang akan datang.