# KEBIJAKAN PENANGGULANGAN TINDAK PIDANA TEKNOLOGI

*Oleh : Reny Okprianti, SH., M.Hum.*


## Abstrak

Kebijakan Pemerintrah Indonesia dengan diundangkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik (UU-ITE) merupakan payung hukum pertama yang mengatur dunia cyber (cyber law) sebab muatan dan cakupannya yang luas dalam membahas pengaturan di dunia maya seperti perluasan alat bukti elektronik sama dengan alat bukti yang sudah dikenal selama ini. Diakuinya tanda tangan elektronik sebagai alat verifikasi dan autentikasi yang sah suatu pekerjaan elektronik, serta pengaturan perbuatan-perbuatan yang dilakukan dalam cyber space sebagai suatu tindak pidana. Berkaitan dengan formulasi, kebijakan kriminalisasi dalam UU-ITE tidak hanya mengatur terhadap perbuatan-perbuatan tradisional yang terkait dengan dunia maya, tetapi juga mengkriminalisasi delik-delik tertentu di bidang cyber crime.


## A. LATAR BELAKANG

Peradaban dunia pada masa kini dicirikan dengan fenomena kemajuan teknologi informasi dan komunikasi yang berlangsung hampir di semua bidang kehidupan. Revolusi yang dihasilkan oleh teknologi informasi dan komunikasi biasanya dilihat dan sudut pandang penurunan jarak geografis, penghilangan batas-batas negara dan zona waktu serta peningkatan efisiensi dalam pengumpulan, penyebaran, analisis dan mungkin juga penggunaan data.

Revolusi tersebut tidak dapat dipungkiri menjadi ujung tombak era globalisasi yang kini melanda hampir seluruh dunia. Apa yang disebut dengan globalisasi pada dasarnya bermula dari awal abad ke-20, yakni pada saat terjadi revolusi transportasi dan elektronika yang menyebarluaskan dan mempercepat perdagangan antar bangsa, disamping pertambahan dan kecepatan lalu lintas barang dan jasa.

Teknologi informasi dan media elektronika dinilai sebagai simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial budaya, ekonomi dan keuangan. Dari sistem-sistem kecil lokal dan nasional, proses globalisasi dalam tahun-tahun terakhir bergerak cepat, bahkan terlalu cepat menuju suatu sistem global.

Sebagai mana ditulis dalam International Review of Law Computer and Technology:

> *"Global information and communication networks are now an integral part of the way in which modern governments, businesses, education and ecomomies operate. However, the increasing dependence upon the new information and communication technologies by many organizations is not without its price, they have become more exposed"*

Proses globalisasi tersebut melahirkan suatu fenomena yang mengubah model komunikasi konvensional dengan melahirkan kenyataan dalam dunia maya (virtual reality) yang dikenal sekarang ini dengan internet. Internet berkembang demikian pesat sebagai kultur masyarakat

modern, dikatakan sebagai kultur karena melalui internet berbagai aktivitas masyarakat cyber seperti berpikir, berkreasi, dan bertindak dapat diekspresikan di dalamnya, kapanpun dan dimanapun. Kehadirannya telah membentuk dunia tersendiri yang dikenal dengan dunia maya (Cyberspace) atau dunia semu yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk virtual (tidak langsung dan tidak nyata).\

Komunitas masyarakat yang ikut bergabung di dalamnya pun kian hari semakin meningkat, kecenderungan masyarakat untuk berkonsentrasi dalam cyberspace merupakan bukti bahwa internet telah membawa kemudahan-kemudahan bagi masyarakat.

Bagi sebagian orang munculnya fenomena ini telah mengubah prilaku manusia dalam berinteraksi dengan manusia lain. baik secara individual maupun secara kelompok, kemajuan teknologi tentunya akan berjalan bersamaan dengan munculnya perubahan-perubahan di bidang kemasyarakatan.

Sebagaimana dikatakan oleh Satjipto Raharjo, "banyak alasan yang dapat dikemukakan sebagai penyebab timbulnya suatu perubahan di dalam masyarakat tetapi perubahan dalam penerapan hasil-hasil teknologi modern dewasa ini banyak disebut-sebut sebagai salah satu sebab bagi terjadinya perubahan sosial". Perubahan-perubahan tersebut dapat mengenai nilai-nilai berarti mengubah atau mengganti tampilan suatu website dengan mengubah nama-nama partai yang ada dengan nama-nama buah dalam website www.kpu.go.id, yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap pemilu yang sedang berlangsung pada saat itu. Dikhawatirkan, selain nama-nama partai yang diubah bukan tidak mungkin angka-angka jumlah pemilih yang masuk di sana menjadi tidak aman dan dapat diubah, padahal dana yang dikeluarkan untuk sistem teknologi informasi yang digunakan oleh KPU sangat besar sekali. Teknik lain adalah yang memanfaatkan celah sistem keamanan server alias hole Cross Server Scripting (XXS) yang ada pada suatu situs. XXS adalah kelemahan aplikasi di server yang memungkinkan user atau pengguna menyisipkan baris-baris perintah lainnya. Biasanya perintah yang disisipkan adalah Javascript sebagai jebakan, sehingga pembuat hole bisa mendapatkan informasi data pengunjung lain yang berinteraksi di situs tersebut. Makin terkenal sebuah website yang mereka deface, makin tinggi rasa kebanggaan yang didapat. Teknik ini pulalah yang menjadi andalan saat terjadi cyber war antara hacker Indonesia dan hacker Malaysia dikarenakan pengakuan budaya reok oleh pemerintah Malaysia, sehingga terjadi perusakan website pemerintah Indonesia dan Malaysia oleh para hacker kedua negara tersebut. Dari kasus yang telah terjadi di atas dapat diketahui bahwa kejahatan ini tidak mengenal batas wilayah (borderless) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. Semua aksi itu dapat dilakukan hanya dari depan komputer yang memiliki akses Internet tanpa takut diketahui oleh orang lain/saksi mata, sehingga kejahatan ini termasuk dalam Transnational Crime/kejahatan antar negara yang pengungkapannya sering melibatkan penegak hukum lebih dari satu negara. Mencermati hal tersebut dapatlah disepakati bahwa kejahatan IT/Cybercrime memiliki karakter yang berbeda dengan tindak pidana umum baik dan segi pelaku, korban, modus operandi dan tempat kejadian perkara.

Perkembangan teknologi informasi yang demikian pesatnya haruslah diantisipasi dengan hukum yang mengaturnya. Dampak negatif tersebut harus diantisipasi dan ditanggulangi dengan hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Secara internasional hukum yang terkait kejahatan teknologi informasi

digunakan istilah hukum siber atau cyber law. Istilah lain yang juga digunakan adalah hukum teknologi informasi (law of information technology), hukum dunia maya (virtual world law), dan hukum mayantara.

Sejalan dengan istilah tersebut "tindak pidana mayantara", identik dengan "tindak pidana di ruang siber (cyber space) atau yang biasa juga dikenal dengan istilah "cybercrime". Perkembangan kejahatan di bidang teknologi informasi yang relatif baru mengakibatkan belum ada kesatuan pendapat terhadap definisi kejahatan teknologi informasi. Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar menyatakan "bahwa meskipun belum ada kesepahaman mengenai definisi kejahatan teknologi informasi, namun ada kesamaan mengenai pengertian universal mengenai kejahatan komputer".

Hal ini dapat dimengerti karena kehadiran komputer yang sudah mengelobal mendorong terjadinya universalisasi aksi dan akibat yang dirasakan dari kejahatan komputer tersebut. Istilah-istilah tindak pidana di bidang teknologi informasi tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sitem komunikasi baik dalam lingkup lokal maupul global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat virtual.

Pemerintah telah melakukan kebijakan dengan terbitnya Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diundangkan pada tanggal 21 Apri 2008.12 Undang-undang ITE merupakan payung hukum pertama yang mengatur khusus terhadap dunia maya (cyber law) di Indonesia. Substansi/materi yang diatur dalam UU ITE ialah menyangkut masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara e-comerce, azas persaingan usaha-usaha tidak sehat dan perlindungan konsurnen, azas-azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional serta azas Cybercrime. Undang-undang tersebut mengkaji cyber case dalam beberapa sudut pandang secara komprehensif dan spesifik, fokusnya adalah semua aktivitas yang dilakukan dalam cyberspace seperti perjudian, pornografi, pengancaman, penghinaan dan pencemaran nama baik melalui media internet serta akses komputer tanpa ijin oleh pihak lain (cracking,) dan menjadikan seolah dokumen otentik (phising). Berbagai komentar di media televisi, surat kabar, majalah maupun di komunitas dunia maya bermunculan terhadap keluarnya UU ITE. pasal mengenai pornografi, kesiapan aparat serta belum termuatnya aturan terhadap spamming, warm juga virus komputer di dalam undang-undang tersebut. Opini yang bersifat pro maupun kontra terhadap pemidanaan di dunia maya memang wajar dalam iklim demokrasi serta kebebasan berpendapat sekarang ini. Pemidanaan terhadap larangan-larangan di dalam UU ITE dikarenakan kegiatan di alam maya (cyber) meskipun bersifat virtual tetapi dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis untuk ruang siber sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi konvensional untuk dapat dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan cyber adalah kegiatan virtual tetapi berdampak sangat nyata meskipun alat buktinya bersifat elektronik, dengan demikian subyek pelakunya harus dikualifikasikan pula sebagai telah melakukan perbuatan hukum secara nyata. Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakekatnya, kebijakan kriminalisasi terhadap tindak pidana teknologi informasi

merupakan bagian dan kebijakan kriminal (criminal policy) dengan menggunakan sarana hukum pidana (penal), dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" (penal policy), khususnya kebijakan formulasinya. Selanjutnya menurut BNA kebijakan kriminalisasi bukan sekedar kebijakan menetapkan/ merumuskan/memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan formulasi/legislasi.

Bertolak dari pengertian di atas maka upaya atau kebijakan untuk melakukan penanggulangan tindak pidana di bidang teknologi informasi yang dilakukan dengan menggunakan sarana "penal" (hukum pidana) maka dibutuhkan kajian terhadap materi/substansi (legal subtance reform) tindak pidana teknologi informasi saat ini. Dalam penanggulangan melalui hukum pidana (penal policy) perlu diperhatikan bagaimana memformulasikan (kebijakan legislatif) suatu peraturan perundang-undangan yang tepat untuk menanggulangi tindak pidana di bidang teknologi informasi pada masa yang akan datang, serta bagaimana mengaplikasikan kebijakan legislatif (kebijakan yudikatif/yudisial atau penegakan hukum pidana in concreto) tersebut oleh aparat penegak hukum atau pengadilan.

Untuk dapat melakukan pembahasan yang mendalam mengenai masalah ini maka perlu dilakukan penelitian yang mendalam agar memberi gambaran yang jelas dalam menentukan kebijakan dalam menanggulangi tindak pidana teknologi informasi melalui hukum pidana.

Kebijakan penanggulangan hukum pidana (penal policy) tersebut pada hakekatnya bertujuan sebagai upaya perlindungan masyarakat untuk mencapai keadilan dan kesejahteraan masyarakat (social welfare).

Kumpulan hardware dan software membentuk teknologi yang digunakan sebagai penyedia layanan kebutuhan sistem informasi, seperti misalnya: electronic data intercharge, internet, intranet, extranet, data mining, workgroup, integrated Services Digital Network (ISDN) electronic commerce, dan lain sebagainya. Dengan demikian cakupan teknologi informasi menjadi cukup luas, tidak hanya komputer atau internet saja, namun termasuk juga peralatan-peralatan elektronika digital lain yang berbasis komputerisasi baik yang digunakan secara stand alone maupun terhubung ke suatu jaringan. dalam penjelasan Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Adapun permasalahan yang akan dibahas dalam makalah ini adalah:
*"Bagaimana kebijakan penanggulangan tindak pidana teknologi informasi memalui hukum pidana?"*

## A. KEBIJAKAN PENANGGULANGAN KEJAHATAN MELALUI HUKUM PIDANA

Hakekat pembangunan nasional adalah pembangunan bertujuan untuk mewujudkan manusia Indonesia seutuhnya dan masyarakat Indonesia seluruhnya untuk mencapai masyarakat adil, makmur dan sejahtera merata materiil dan sprituil berdasarkan Pancasila dan UUD 1945. Salah satu bagian pembangunan nasional adalah pembangunan di bidang hukum, yang dikenal dengan istilah pembaharuan hukum (law reform). Pembaharuan hukum nasional sebagai bagian dan rangkaian pembangunan nasional ini dilakukan secara menyeluruh dan terpadu baik hukum pidana, hukum perdata, maupun hukum administrasi, dan meliputi juga hukum formil maupun hukum materielnya.

Upaya pembaharuan hukum tidak terlepas dan kebijakan publik dalam mengendalikan dan membentuk pola sampai seberapa jauh masyarakat diatur dan diarahkan. Dengan demikian sangat penting untuk menyadarkan para perancang hukum dan kebijakan publik bahkan para pendidik, bahwa hukum dan kebijakan publik yang diterbitkan akan mempunyai implikasi yang luas di bidang sosial, ekonomi dan politik. Sayangnya spesialisasi baik dalam pekerjaan, pendidikan maupun riset yang dilandasi dua disiplin tersebut (hukum dan ilmu sosial), sehingga pelbagai informasi yang bersumber dan keduanya tidak selalu bertemu (converge) bahkan seringkali tidak sama dan sebangun (incongruent).

Secara umum kebijakan dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah dalam mengelola, mengatur atau menyelesaikan urusan-urusan publik, masalah-masalah masyarakat atau bidang-bidang penyusunan peraturan perundang-undangan dan pengaplikasian hukum/ peraturan, dengan suatu tujuan yang mengarah pada upaya mewujudkan kesejahteraan atau kemakmuran masyarakat (warga negara). Upaya perlindungan masyarakat (social defence) dan upaya mencapai kesejahteraan masyarakat (social welfare) pada hakikatnya merupakan bagian integral dan kebijakan atau upaya penanggulangan kejahatan.

Penegasan perlunya penanggulangan kejahatan diintegrasikan dengan keseluruhan kebijakan sosial, juga dikemukakan dalam kongres PBB ke-5 tahun 1975 di Geneva dalam membahas masalah criminal legislation, judicial procedures, and other form of social control in the prevention of crime, menyatakan: "The many esencies of criminal"

Tujuan penanggulanggan kejahatan yaitu perlindungan masyarakat untuk mencapai kesejahteraan masyarakat.

**A.1. Upaya Penanggulangan Kejahatan melalui Hukum Pidana**

Pertanyaan tentang perumusan tindak pidana/kriminalisasi muncul ketika kita dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakat yang hukumnya belum ada atau belum ditemukan. Berkaitan dengan kebijakan kriminalisasi menurut Sudarto perlu diperhatikan hal-hal yang intinya sebagai berikut:

a. Pengunaan hukum pidana harus memperhatikan tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil makmur yang merata materiil dan spiritual berdasarkan Pancasila: sehubungan dengan ini (penggunaan) hukum pidana bertujuan untuk menanggulangi kejahatan dan mengadakan pengugeran terhadap tindakan penanggulangan itu sendiri, demi kesejahtraan dan pengayoman masyarakat.
b. Perbuatan yang diusahakan untuk dicegah atau ditanggulanggi dengan hukum pidana harus merupakan "perbuatan yang tidak dikehendaki" yaitu perbuatan yang mendatangkan kerugian (materil dan spirituil) atas warga masyarakat.
c. Penggunaan hukum pidana harus pula memperhitungkan prinsip biaya dan hasil (cost dan benefit principle)
d. Penggunaan hukum pidana harus pula memperhatikan kapasitas atau kemampuan daya kerja dan badan-badan penegak hukum yaitu jaringan sampai ada kelampauan beban tugas (overbelasting).

Berdasarkan pertimbangan di atas, dapat disimpulkan bahwa alasan kriminalisasi pada umumnya adalah:

1. Adanya korban;
2. Kriminalisasi bukan semata-mata ditujukan untuk pembalasan;
3. Harus berdasarkan asas ratio principle; dan
4. Adanya kesepakatan sosial (public support)

Kebijakan hukum pidana berkaitan dengan masalah kriminalisasi yaitu perbuatan apa yang dijadikan tindak pidana dan penalisasi yaitu sanksi apa yang sebaiknya dikenakan pada si pelaku tindak pidana. Kriminalisasi dan penalisasi menjadi masalah seniral yang untuk penanganannya diperlukan pendekatan yang berorientasi pada kebijakan (policy oriented approach). Kriminalisasi (criminalization) mencakup ruang lingkup perbuatan melawan hukum (actus reus), pertanggungjawaban pidana (mens rea) maupun sanksi yang dapat dijatuhkan baik berupa pidana (punishment) maupun tindakan (treatment). Kriminalisasi harus dilakukan secara hati-hati, jangan sampai menimbulkan kesan refresif yang melanggar prinsip ultimum remedium (ultima ratio principle) dan menjadi bumerang dalam kehidupan sosial berupa kriminalisasi yang berlebihan (overcriminalization), yang justru mengurangi wibawa hukum. Kriminalisasi dalam hukum.

**A.2. Kebijakan Penegakan Hukum**

Penegakan hukum pidana merupakan bagian dari politik kriminal sebagai salah satu bagian dari keseluruhan kebijaksanaan penanggulangan kejahatan, memang penegakan hukum pidana bukan merupakan satu-satunya tumpuan harapan untuk dapat menyelesaikan atau menanggulangi kejahatan itu secara tuntas. Hal ini wajar karena pada hakekatnya kejahatan itu merupakan masalah kemanusiaan dan masalah sosial yang tidak dapat diatasi semata-mata dengan hukum pidana. Walaupun penegakan hukum pidana dalam rangka penanggulangan kejahatan bukan merupakan satu-satunya tumpuan harapan, namun keberhasilannya sangat diharapkan karena pada bidang penegakan hukum inilah dipertaruhkan makna dan Negara berdasarkan atas hukum.

Peran aparat penegak hukum dalam Negara berdasarkan hukum juga dinyatakan oleh Satjipto Rahardjo yang menyatakan. "hukum tidak memiliki fungsi apa-apa, bila tidak diterapkan atau ditegakkan bagi pelanggar hukum, yang menegakkan hukum di lapangan adalah aparat penegak hukum."

pidana materiil akan diikuti pula oleh langkah-langkah pragmatis dalam hukum pidana formil untuk kepentingan penyidikan dan penuntutan menjadi lebih akseptabel bersama-sama dengan peran masyarakatnya. Tanpa peran masyarakat, kebijakan penegakan hukum akan menjadi tidak optimalistis sifatnya.

Masalah pokok penegakan hukum sebenarnya terletak pada faktor-faktor yang mungkin mempengaruhinya. Menurut Soerjono Soekanto faktor-faktor yang mempengaruhi penegakan hukum tersebut mempunyai arti yang netral, sehingga dampak positif atau negatifnya terletak pada isi faktor-faktor tersebut. Faktor-faktor tersebut, adalah:

1. Faktor hukumnya sendiri (undang-undang)
2. Faktor penegak hukum yakni pihak yang membentuk maupun menerapkan hukum.
3. Faktor sarana atau fasilitas yang mendukung penegakan hukum.
4. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.

5. Faktor kebudayaan, yakni sebagai hasil karya, cipta, dan rasa yang didasarkan pada karsa manusia dalam pergaulan hidup.

Kelima faktor tersebut saling berkaitan dengan eratnya, oleh karena merupakan esensi dan penegakan hukum, juga merupakan tolak ukur daripada efektifitas penegakan hukum. Diantara semua faktor-faktor tersebut, menurut Soerjono Soekanto faktor penegak hukum menempati titik sentral sebagai tolah ukur sampai sejauh mana kontribusi bagi kesejahteraan masyarakat. Penegakan hukum sangat terikat dengan hukum acara pidana dan pembuktian. Pembuktian merupakan masalah yang memegang peranan dalam proses pemeriksaan sidang pengadilan. Melalui pembuktian ditentukan nasib terdakwa. Apabila hasil pembuktian dengan alat-alat bukti yang ditentukan undang-undang menjadi lebih akseptabel bersama-sarna dengan peran masyarakatnya. Tanpa peran masyarakat, kebijakan penegakan hukum akan menjadi tidak optimalistis sifatnya. Rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

UU ITE dalam Pasal sub-3 menegaskan pengertian teknologi informasi di Indonesia sebagai suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memperoses, mengumumkan, menganalisa, dan menyebarkan informasi.

Adanya perbedaan definisi informasi dikarenakan pada hakekatnya informasi tidak dapat diuraikan (intangible), sedangkan informasi itu dijumpai dalam kehidupan sehari-hari, yang diperoleh dari data dan observasi terhadap dunia sekitar kita serta diteruskan melalui komunikasi. Secara umum, teknologi Informasi dapat diartikan sebagai teknologi yang digunakan untuk menyimpan, menghasilkan, mengolah, serta menyebarkan informasi. Disadari betul bahwa perkembangan teknologi informasi yang berwujud internet, telah mengubah pola interaksi masyarakat, seperti interaksi bisnis, ekonomi, sosial, dan budaya. Internet telah memberikan kontribusi yang demikian besar bagi masyarakat. perusahaan / industri maupun pemerintah. Hadirnya Internet telah menunjang efektifitas dan efisiensi operasional setiap aktifitas manusia.

Perkembangan teknologi informasi yang terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara (borderless). Negara yang sudah mempunyai infrastruktur jaringan informasi yang lebih memadai tentu telah menikmati hasil pengembangan teknologi informasinya, negara yang sedang berkembang dalam pengembangannya akan merasakan kecenderungan timbulnya neo-kolonialisme. Hal tersebut menunjukan adanya pergeseran paradigma dimana jaringan informasi merupakan infrastruktur bagi perkembangan suatu negara.

Jaringan informasi melalui komputer (interconnected computer networks) dapat digolongkan dalam tiga istilah yaitu ekstranet, intranet dan internet. Perkembangan internet telah memunculkan dunia baru yang kehadirannya telah membentuk dunia tersendiri yang dikenal dengan dunia maya (Cyberspace) atau dunia semu yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk virtual (tidak langsung dan tidak nyata).

Perkembangan selanjutnya seiring dengan meluasnya penggunaan komputer istilah ini kemudian dipergunakan untuk menunjuk sebuah ruang elektronik (electronic space),

yaitu sebuah masyarakat virtual yang terbentuk melalui komunikasi yang terjalin dalam sebuah jaringan komputer (interconnected computer networks).

Dunia maya memberikan realitas, tetapi bukan realitas yang nyata sebagaimana bisa kita lihat melainkan realitas virtual (virtual reality), dunia yang tanpa batas sehingga dinyatakan borderless world, karena memang dalam cyberspace tidak mengenal batas negara, hilangnya batas dimensi ruang, waktu dan tempat. Kehidupan dalam dunia maya dapat memberikan layanan komunikasi langsung yang berbeda dari dunia realitas seperti e-mail, chat, video conference, diskusi, sumber daya informasi yang terdistribusikan, remote login, dan lalu lintas file dan aneka layanan lainnya. Diantara layanan yang diberikan internet, yang dikenal umum dilakukan antara lain:

a. *E-Commerce*
   Contoh paling umum dan kegiatan ini adalah aktifitas transaksi perdagangan umum melalui sarana internet. Umumnya transaksi melalui sarana e-commerce dilakukan melalui sarana suatu situs web yang dalam hal ini berlaku sebagai semacam etalase bagi produk yang dijajakan. Dari situs ini pembeli dapat melihat barang yang ingin dibeli, lalu bila tertarik dapat melakukan transaksi dan seterusnya.

b. *E-Banking*
   Hal ini diartikan sebagai aktivitas perbankan di dunia maya (virtual) melalui sarana internet. Layanan ini memungkinkan pihak bank dan nasabah dapat melakukan berbagai jenis transaksi perbankan melalui sarana internet, khususnya via web.

c. *E-Government*
   Hal ini bukan merupakan pemerintahan model baru yang berbasiskan dunia internet, tapi merupakan pemanfaatan teknologi internet untuk bidang pemerintahan.
   Pemerintahan dalam memberikan pelayanan kepada publik dapat menggunakan sarana ini. Dalam kerangka demokrasi dan untuk mewujudkan clean government dan good governance ini tentu sangat menarik sekali.

d. *E-Learning*
   Istilah ini didefinisikan sebagai sekolah di dunia maya (virtual). Definisi e-learning sendiri sesungguhnya sangat luas, bahkan sebuah portal informasi tentang suatu topik dapat tercakup dalam e-learning ini. Namun pada prinsipnya istilah ini ditujukan pada usaha untuk membuat transformasi proses belajar mengajar di sekolah dalam bentuk digital yang dijembatani oleh teknologi internet.

e. *E-Legislative*
   Merupakan sarana baru pemanfaatan teknologi Internet oleh lembaga legislatif atau Dewan Perwakilan Rakyat, baik di tingkat pusat maupun daerah. Hal ini dimaksudkan di samping untuk menyampaikan kepada publik tentang kegiatan dan aktifitas lembaga legislatif, juga untuk memudahkan masyarakat mengakses produk-produk yang dihasilkan oleh lembaga legislatif, mulai dan Undang-Undang, Peraturan Daerah dan Peraturan atau Keputusan Pimpinan Daerah.

Umumnya suatu masyarakat yang mengalami perubahan akibat kemajuan teknologi, banyak melahirkan masalah-masalah sosial. Hal itu terjadi karena kondisi masyarakat itu sendiri yang belum siap menerima perubahan atau dapat pula karena nilai-nilai masyarakat yang telah berubah dalam menilai kondisi yang tidak lagi dapat diterima.

Dampak negatif terjadi akibat pengaruh penggunaan media Internet dalam kehidupan

masyarakat dewasa ini. Melalui media internet beberapa jenis tindak pidana semakin mudah untuk dilakukan seperti, tindak pidana pencemaran nama baik, pornografi, perjudian, pembobolan rekening, perusakan jaringan cyber (haking), penyerangan melalui virus (virus attack) dan sebagainya.

### A.3. Tindak Pidana Teknologi Informasi

Di era global ini berbagai hal positif yang bisa dimanfaatkan oleh setiap bangsa terutama bidang teknologi, kemajuan teknologi juga menyimpan kerawanan yang tentu saja sangat membahayakan. Bukan hanya soal kejahatan konvensional yang gagal diberantas akibat terimbas oleh pola-pola modernitas yang gagal mengedepankan prinsip humanitas, tetapi juga munculnya kejahatan di alam maya yang telah menjadi realitas dunia. Memang tidak bisa diingkari oleh siapapun, bahwa teknologi itu dapat menjadi alat perubahan di tengah masyarakat. Demikian pentingnya fungsi teknologi, hingga sepertinya masyarakat dewasa ini sangat tergantung dengan teknologi, baik untuk hal-hal positif maupun negatif Pada perkembangannya internet juga membawa sisi negatif dengan membuka peluang Cybercrime pada dasarnya tindak pidana yang berkenaan dengan informasi, sistem informasi (information system) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyarnpaian/pertukaran informasi itu kepada pihak lainnya.

Cybercrime jenis ini bukan memanfaatkan komputer dan internet sebagai media atau sarana tindak pidana, melainkan menjadikannya sebagai sasaran. Contoh dari jenis jenis tindak kejahatannya antara lain pengaksesan ke suatau sistem secara illegal (hacking), perusakan situs internet dan server data (cracking), serta defacting.

## B. JURISDIKSI HUKUM PIDANA DALAM TINDAK PIDANA TEKNOLOGI INFORMASI

Jurisdiksi merupakan hal yang sangat crucial sekaligus kompleks khususnya berkenaan dengan pengungkapan kejahatan-kejahatan di dunia maya yang bersifat internasional (international cybercrime). Dengan adanya kepastian jurisdiksi maka suatu negara memperoleh terkait tindak pidana mayantara (cyberspace), Darrel Menthe, menyatakan jurisdiksi di cyberspace membutuhkan prinsip-prinsip yang jelas yang berakar dari hukum internasional.

Selanjutnya, Menthe menyatakan dengan diakuinya pninsip-pninsip jurisdiksi yang berlaku dalarn hukum internsional dalam kegiatan cyberspace oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasama dalam rangka harmonisasi ketentuan-ketentuan pidana untuk menanggulangi cybercrime.

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksaksi Elektronik (UU ITE) telah mengatur masalah jurisdiksi yang didalamnya sudah menerapkan asas universal. Hal ini dapat dilihat dan Pasal 2 dan penjelasannya:

- Pasal 2 UU ITE

Undang-Undang 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 perbutan hukum yang berlaku di Indonesia dan atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbutan hukum yang dilakukan di luar wilayah hukum (jurisdiksi) Indonesia baik oleh warga negara Indonesia maupun 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" adalah 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.

Upaya menafsirkan cybercrime ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi telah dilakukan oleh penegak hukum dalam menangani cybercrirne selama ini. Sebelum UU ITE diundangkan ada beberapa ketentuan hukum positif yang dapat diterapkan dengan keberanian untuk melakukan terobosan dengan penafsiran hukum yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan internet. Penafsiran hukum dapat dilakukan melalui penafsiran ekstensif dan analogi.

Metode penafsiran hukum yang dilakukan oleh aparat penegak hukum menjadi hal yang logis untuk menghindari kekosongan hukum terhadap tindak pidana teknologi informasi.

Penerapan ketentuan-ketentuan hukum positif sebelum adanya UU ITE tidaklah sederhana karena karateristik cybercrime yang bersifat khas dan kejahatan konvensional/ di dunia biasa. Sebelum disahkannya UU ITE terdapat beberapa peraturan perundang-undangan yang dapat digunakan untuk menanggulangi tindak pidana di dunia maya.

**Kitab Undang-Undang Hukum Pidana (KUHP)**

Badan Pembinaan Hukum Nasional, Perkembangan Pembangunan Hukum Nasional tentang Hukum

**Kriminalisasi Tindak Pidana Teknologi Informasi dalam KUHP**

Dalam upaya menangani kasus kejahatan dunia maya, terdapat beberapa pasal dalam KUHP yang mengkriminalisasi cybercrime dengan mengggunakan metode interpretasi ekstensif (perumpamaan dan persamaan) terhadap pasal-pasal yang terdapat dalam KUHP.

**Subjek, Sanksi Pidana dan Aturan Pemidanaan dalam KUHP**

Sesuatu dapat dikatakan sebagai tindak pidana apabila ada subjek (pelaku) dan tindak pidana itu sendiri. Agar dapat dipidana, dalam diri subjek atau pelaku pidana tidak terdapat dasar penghapus pidana, baik dasar pembenar maupun dasar pemaaf. Subjek tindak pidana dalam KUHP hanya "orang", sehingga semua aturan pemidanaan di dalam KUHP diorientasikan pada "orang" (natural person), sedangkan badan hukum atau rechts-persoonen tidak dianggap sebagai subjek. Meskipun demikian, pada perkembangannya terjadi perluasan terhadap subjek tindak pidana didalam undang-undang diluar KUHP, apabila undang-undang khusus memperluas subjek tindak pidana pada korporasi, seyogianya juga disertai dengan aturan pemidanaan atau pertangungjawaban khusus untuk korporasi.

Sanksi pidana pada umumnya dirumuskan dalam perumusan delik, walaupun ada juga yang dirumuskan terpisah dalam pasal (ketentuan khusus) lainnya. Jenis pidana yang pada umumnya dicantumkan dalam perumusan delik menurut pola KUHP ialah pidana pokok dengan menggunakan 9 (sembilan) bentuk perumusan, yaitu:

1. diancam dengan pidana mati atau penjara seumur hidup atau penjara tertentu;
2. diancam dengan penjara seumur hidup atau penjara tertentu;
3. diancam dengan pidana penjara (tertentu);
4. diancam dengan pidana penjara atau kurungan;
5. diancam dengan pidana penjara atau kurungan atau denda;
6. diancam dengan pidana penjara atau denda;
7. diancam dengan pidana kurungan;
8. diancam dengan pidana kurungan atau denda;
9. diancam dengan denda.

**Kualifikasi Tindak Pidana dalam KUHP**

KUHP membedakan "aturan umum" untuk tindak pidana yang berupa kejahatan dan pelanggaran. Artinya, kualifikasi delik berupa kejahatan atau pelanggaran merupakan kualifikasi juridis yang akan membawa konsekuensi juridis yang berbeda. KUHP tidak mengenal kualifikasi juridis berupa delik aduan, walaupun di dalam KUHP ada aturan umum tentang mengajukan dan menarik kembali pengaduan untuk kejahatan-kejahatan tertentu (tidak untuk pelanggaran). KUHP tidak membuat aturan umum untuk bentuk-bentuk tindak pidana ("forms of criminal offence") yang berupa permufakatan jahat, persiapan, dan pengulangan (recedive). Ketiga bentuk tindak pidana ini hanya diatur dalam aturan khusus (Buku II atau Buku III).

**Kriminalisasi Tindak Pidana Teknologi Informasi dalam UU Telekomunikasi**

Internet merupakan salah satu bentuk media komunikasi elektronik yang terdiri dari komputer dan dilengkapi dengan perlengkapan tertentu sehingga memungkinkan untuk melakukan komunikasi dengan berbagai pihak di cyberspace. Penyalahgunaan internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan undang-undang ini. Jika dikaitkan dengan kejahatan-kejahatan di internet yang marak terjadi seperti hacking (craking), carding atau bentuk-bentuk kejahatan lain yang berhubungan dengan cybercrime, maka undang-undang ini masih terlalu sumir dan tidak tegas menyebutnya. Sehingga sulit diterapkan dan dikenakan terhadap pelakunya. Kebijakan hukum yang terkait dengan masalah kriminalisasi yang terkait dengan tindak pidana teknologi informasi dalam Undang Undang Telekomunikasi.

**Sanksi Pidana dan Aturan Pemidanaan dalam UU Telekomunikasi**

Sistem perumusan sanksi pidana dalam Undang-Undang Telekomunikasi adalah secara alternatif komulatif. Perumusan sanksi secara tunggal hanya terdapat pada Pasal 53 ayat (2) yaitu penjara selama 15 tahun. Jenis sanksi pidana yang diterapkan dalarn UU ini yaitu pidana penjara, pidana denda dan pidana tambahan. Pidana tambahan dalam UU Telekomunikasi merupakan sanksi administrasi berupa peringatan tertulis dan pencabutan izin usaha (Pasal 45 dan Pasal 46). Sanksi lain yang diatur dalam Pasal 58 UU Telekomunikasi adalah perangkat telekomunikasi yang digunakan dalam tindak pidana sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 52 atau Pasal 56 dirampas untuk negara dan atau dimusnahkan sesuai dengan peraturan perundang-undangan yang berlaku. Pasal 58 tersebut menyatakan adanya jenis

Sanksi pidana pada umumnya dirumuskan dalam perumusan delik, walaupun ada juga yang dirumuskan terpisah dalam pasal (ketentuan khusus) lainnya. Jenis pidana yang pada umumnya dicantumkan dalam perumusan delik menurut pola KUHP ialah pidana pokok dengan menggunakan 9 (sembilan) bentuk perumusan, yaitu:

1. diancam dengan pidana mati atau penjara seumur hidup atau penjara tertentu;
2. diancam dengan penjara seumur hidup atau penjara tertentu;
3. diancam dengan pidana penjara (tertentu);
4. diancam dengan pidana penjara atau kurungan;
5. diancam dengan pidana penjara atau kurungan atau denda;
6. diancam dengan pidana penjara atau denda;
7. diancam dengan pidana kurungan;
8. diancam dengan pidana kurungan atau denda;
9. diancam dengan denda.

**Kualifikasi Tindak Pidana dalam KUHP**

KUHP membedakan "aturan umum" untuk tindak pidana yang berupa kejahatan dan pelanggaran. Artinya, kualifikasi delik berupa kejahatan atau pelanggaran merupakan kualifikasi juridis yang akan membawa konsekuensi juridis yang berbeda. KUHP tidak mengenal kualifikasi juridis berupa delik aduan, walaupun di dalam KUHP ada aturan umum tentang mengajukan dan menarik kembali pengaduan untuk kejahatan-kejahatan tertentu (tidak untuk pelanggaran). KUHP tidak membuat aturan umum untuk bentuk-bentuk tindak pidana ("forms of criminal offence") yang berupa permufakatan jahat, persiapan, dan pengulangan (recedive). Ketiga bentuk tindak pidana ini hanya diatur dalam aturan khusus (Buku II atau Buku III).

**Kriminalisasi Tindak Pidana Teknologi Informasi dalam UU Telekomunikasi**

Internet merupakan salah satu bentuk media komunikasi elektronik yang terdiri dari komputer dan dilengkapi dengan perlengkapan tertentu sehingga memungkinkan untuk melakukan komunikasi dengan berbagai pihak di cyberspace. Penyalahgunaan internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan undang-undang ini. Jika dikaitkan dengan kejahatan-kejahatan di internet yang marak terjadi seperti hacking (craking), carding atau bentuk-bentuk kejahatan lain yang berhubungan dengan cybercrime, maka undang-undang ini masih terlalu sumir dan tidak tegas menyebutnya. Sehingga sulit diterapkan dan dikenakan terhadap pelakunya. Kebijakan hukum yang terkait dengan masalah kriminalisasi yang terkait dengan tindak pidana teknologi informasi dalam Undang Undang Telekomunikasi.

**Sanksi Pidana dan Aturan Pemidanaan dalam UU Telekomunikasi**

Sistem perumusan sanksi pidana dalam Undang-Undang Telekomunikasi adalah secara alternatif komulatif. Perumusan sanksi secara tunggal hanya terdapat pada Pasal 53 ayat (2) yaitu penjara selama 15 tahun. Jenis sanksi pidana yang diterapkan dalarn UU ini yaitu pidana penjara, pidana denda dan pidana tambahan. Pidana tambahan dalam UU Telekomunikasi merupakan sanksi administrasi berupa peringatan tertulis dan pencabutan izin usaha (Pasal 45 dan Pasal 46). Sanksi lain yang diatur dalam Pasal 58 UU Telekomunikasi adalah perangkat telekomunikasi yang digunakan dalam tindak pidana sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 52 atau Pasal 56 dirampas untuk negara dan atau dimusnahkan sesuai dengan peraturan perundang-undangan yang berlaku. Pasal 58 tersebut menyatakan adanya jenis

pidana tambahan atau tindakan yang "khas" berupa perampasan untuk negara dan pemusnahan.

**Undang-Undang No. 19 tahun 2002 tentang Hak Cipta**

Suatu program atau data mempunyai nilai puluhan kali lipat dibandingkan nilai dari komputer atau media lainnya dimana data atau program tersebut tersimpan yang menjadikan banyak orang yang ingin mengambilnya secara tidak sah untuk disalah gunakan atau diambil manfaat tanpa izin pemiliknya.

**Kriminalisasi Tindak Pidana Teknologi Informasi dalam UU Hak Cipta**

Undang-undang Hak Cipta ditempuh dua jalur kebijakan kriminal, yaitu melalui jalur non penal terlihat dalam Bab X tentang Penyelesaian Sengketa dengan adanya Pengadilan Niaga

**Kebijakan Formulasi dalam Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik**

Negara Indonesia telah membuat kebijakan yang berhubungan dengan hukum teknologi informasi (law of information technology) setelah diundangkannya Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada tanggal 21 April 2008 oleh Menteri Hukum dan Hak Asasi Manusia. Produk hukum yang berkaitan dengan ruang siber (cyber space) atau mayantara ini dianggap oleh pemerintah perlu untuk memberikan keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal.

Kritik masyarakat baik dari akademisi, aparat penegak hukum, para bloggers terutama hackers pada saat disahkannya UU ITE adalah hal yang wajar di era demokratisasi seperti saat ini. Karena dalam merumuskan peraturan hukum dewasa ini harus mempertimbangkan secara komprehensif beragam dimensi persoalan. Di sini orang akan mempersoalkan hak-hak warga seperti kebebasan berekspresi, kebebasan media, dan masalah-masalah HAM seperti persoalan privasi, hak untuk memperoleh informasi, dan sebagainya yang saat ini sangat diperhatikan dalam legislai positif nasional. Di sinilah relevansi persoalan hak dan kewajiban menjadi penting.

Penanggulangan kejahatan di dunia maya tidak terlepas dari kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah "politik kriminal" menurut Sudarto politik kriminal merupakan suatu usaha yang rasional dan masyarakat dalam menanggulangi kejahatan. Oleh karena itu tujuan pembuatan UU ITE tidak terlepas dari tujuan politik kriminal yaitu sebagai upaya untuk kesejahteraan sosial (social welfare) dan untuk perlindungan masyarakat (social defence). Evaluasi terhadap kebijakan di dunia mayantara tetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan tersebut. Kelemahan kebijakan formulasi hukum pidana akan berpengaruh pada kebijakan penegakan hukum pliana dan kebijakan penanggulangan kejahatan. Dilihat dan persfektif hukum pidana maka kebijakan formulasi harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidanaan umum yang berlaku saat ini. Tidaklah dapat dikatakan terjadi harmonisasi/sinkronisasi apabila kebijakan formulasi berada diluar sistem hukum pidana yang berlaku saat ini. Hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Pertanyaan tentang perumusan tindak pidana/kriminalisasi muncul ketika kita dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakat yang hukumnya belum ada atau belum ditemukan.

## KEBIJAKAN PENEGAKAN HUKUM DALAM UPAYA PENANGGULANGAN TINDAK PIDANA TEKNOLOGI INFORMASI

Kebijakan penegakan hukum ini meliputi proses apa yang dinamakan sebagai kebijakan kriminal atau criminal policy. Konsepsi dan kebijakan penegakan hukum inilah yang nantinya akan diaplikasikan melalui tataran institusional melalui suatu sistem yang dinamakan Criminal Justice System (Sistem Peradilan Pidana), karenanya ada suatu keterkaitan antara Kebijakan Penegakan Hukum dengan Sistem Peradilan Pidana, yaitu sub sistem dan Sistem Peradilan Pidana inilah yang nantinya akan melaksanakan kebijakan penegakan hukum berupa pencegahan dan penanggulangan terjadinya suatu kejahatan dimana peran-peran dan sub-sistem mi akan menjadi lebih acceptable bersama-sama dengan peran masyarakatnya. Tanpa peran masyarakat, kebijakan penegakan hukum akan menjadi tidak optimalistis sifatnya.

Perkembangan teknologi informasi di era globalisasi yang semakin berkembang, dibarengi dengan pembentukan hukum teknologi informasi dewasa ini hendaknya diikuti dengan langkah-langkah antisipatif oleh aparat penegak hukum untuk mencapai keseimbangan dan tata pergaulan di tengah-tengah kehidupan kelompok, golongan, ras dan suku, serta masyarakat, didalam suatu negara maupaun dalam hubungan dengan pergaulan di kawasan regional dan internasioanal.

Masalah pokok penegakan hukurn sebenarnya terletak pada faktor-faktor yang mungkin mempengaruhinya. Menurut Soerjono Soekanto faktor-faktor yang mempengaruhi penegakan hukum tersebut mempunyai arti yang netral, sehingga dampak positif atau negatifnya terletak pada isi faktor-faktor tersebut. Faktor-faktor tersebut, adalah:

1. Faktor hukumnya sendiri (undang-undang)
2. Faktor penegak hukum yakni pihak yang membentuk maupun menerapkan hukum.
3. Faktor sarana atau fasilitas yang mendukung penegakan hukum.
4. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.
5. Faktor kebudayaan, yakni sebagai hasil karya, cipta, dan rasa yang didasarkan pada karsa manusia dalam pergaulan hidup.

Berdasarkan ke 5 (lima) faktor di atas, menurut Sutarman dalam menjamin keamanan, keadilan dan kepastian hukum dalam penegakan hukurn (law enforcement) di dunia cyber dapat terlaksana dengan baik maka harus dipenuhi 4 (empat) syarat yaitu:

1. Adanya aturan perundang-undangan khusus yang mengatur dunia cyber.
2. Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus menangani cybercrime
3. Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu.
4. Kesadaran hukum.

### A. KESIMPULAN

Kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini. Sebelum diundangkannya Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat beberapa ketentuan perundang-undangan yang berhubungan dengan pemanfaatan dan penyalahgunaan teknologi informasi yang diatur dalam KUHP dan beberapa undang-undang di luar KUHP. Kebijakan formulasi terhadap undang-undang sebelum disahkannya UU ITE baik dalam hal kriminalisasinya, jenis sanksi pidana, perumusan sanksi pidana, subjek dan kualifikasi tindak pidana berbeda-beda terutama dalam hal kebijakan

kriminalisasinya belum mengatur secara tegas dan jelas terhadap tindak pidana teknologi informasi.

Proses globalisasi dan perkembangan budaya diiringi dengan kemajuan teknologi informasi dan telekomunikasi memicu semakin berkembangnya bentuk-bentuk tindak pidana baru seperti pembajakan hak cipta secara on line, cyber money laundering, cyber terrorism, dan berbagai jenis tindak pidana baru yang dapat dilakukan melalui internet oleh individu maupun kelompok yang tidak mengenal batas wilayah (borderless) serta waktu kejadian. Kebijakan pemerintah Indonesia dengan diundangkannya Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan payung hukum pertama yang mengatur dunia siber (cyberlaw), sebab muatan dan cakupannya yang luas dalam membahas pengaturan di dunia maya seperti perluasan alat bukti elektronik sama dengan alat bukti yang sudah dikenal selama ini, diakuinya tanda tangan elektronik sebagai alat verifikasi, dan autentikasi yang sah suatu dokumen elektronik, serta pengaturan perbuatan-perbuatan yang dilakukan dalam cyberspace sebagai suatu tindak pidana. Berkaitan dengan kebijakan formulasi, Kebijakan kriminalisasi dalam UU ITE tidak hanya mengatur terhadap perbuatan-perbuatan tradisional yang terkait dengan dunia maya tetapi juga mengkriminalisasi delik-delik tertentu di bidang cybercrime, Penegasan terhadap kualifikasi yuridis sebagai kejahatan ataupun pelanggaran tidak ada dalam UU ITE. Hal ini bisa menimbulkan masalah, karena perundang-undangan pidana di luar KUHP tetap terikat pada aturan umum KUHP mengenai akibat-akibat yuridis dan pembedaan antara "kejahatan" dan "pelanggaran". Penetapan kualifikasi yuridis ini mutlak diperlukan karena sistem pemidanaan di luar KUHP merupakan sub/bagian integral dan keseluruhan sistem pemidanaan. Penerapan sanksi pidana secara kumulatif bersifat imperatif dan kaku, karena perumusan tindak pidana kedua subjek hukurn yang diatur dalam satu pasal yang sama dengan satu ancaman pidana yang sama dalam UU ITE dapat menjadi permasalahan karena pada hakikatnya subjek hukum "orang" dan "korporasi" berbeda baik dalam hal pertanggungjawaban pidana maupun terhadap ancaman pidana yang dikenakan. Aturan pemidanaan dengan adanya pemberatan terhadap pasal 37 merupakan suatu kecerobohan oleh pembuat undang-undang karena redaksi Pasal 37 tersebut tidak mengatur terhadap sanksi tindak pidana. Permasalahan lain yang menjadi rancu terhadap Pasal 52 UU ITE adalah adanya pemberatan secara kebijakan terhadap Pasal 27 sampai dengan Pasal 36, sebab Pasal 27 sampai dengan Pasal 36 tidak mengatur tindak pidana dan sanksi pidana, sementara yang mengatur adanya suatu tindak pidana dan sanksi nya terdapat dalam Pasal 45 sampai dengan Pasal 51 UU ITE. Sistem pemidanaan yang demikian akan mempersulit penegakan hukum terutama dalam operasionalisasi pidana. Pertanggungjawaban pidana terhadap korporasi diatur dalam penjelasan UU ITE yang mengatur kapan, siapa dan bagaimana korporasi dapat dipertanggungjawabkan melakukan tindak pidana. Seharusnya norma-norma tersebut tidak berada dalam "penjelasan", tetapi dirumuskan secara eksplisit dalam perumusan pasal tersendiri, yaitu dalam aturan umum mengenai pertanggungjawaban pidana korporasi.

Meningkatkan fasilitas, pengetahuan dan spesialisasi terhadap aparat penegak hukum di bidang cyber serta upaya pengamanan sistem informasi melalui kerjasama dengan Internet Service Provider (ISP) sebagai penyedia layanan Internet serta perlunya perhatian pertanggungjawaban provider, merupakan solusi dalam penanggulangan penegakan hukum tindak pidana teknologi informasi di masa yang akan datang. Pertanggunawaban pidana terhadap korporasi dalam kebijakan penanggulangan tindak pidana teknologi informasi yang akan datang seyogianya juga memberi kemungkinan menerapkan asas strict liability dan

vicarious liability atau absolute liability.

## B. SARAN

Mengingat tindak pidana dalam dunia maya akan terus berkembang sesuai dengan perkembangan teknologi dan budaya masyarakat, maka terdapat beberapa saran sehubungan dengan kebijakan penanggulangan tindak pidana teknologi informasi melalui hukurn pidana, adalah sebagai berikut:

1. Kebijakan kriminalisasi terhadap perbuatan dalam dunia maya harus terus diharmonisasikan seiring maraknya kejahatan di dunia cyber yang semakin canggih.
2. Perlu Aturan pemidanaan terhadap penyertaan, percobaan, dan pengulangan untuk menghindari terjadinya ketidakadilan hukum dan sebagai upaya untuk kesejahteraan sosial (sosial welfare) dan untuk perlindungan masyarakat (social defence).
3. Sebagai upaya penanggulangan tindak pidana teknologi informasi seyogianya diatur jenis pidana tambahan seperti pelarangan penggunaan Internet selama batas waktu yang ditentukan atau tindakan yang "khas" untuk korporasi, misalnya pencabutan izin usaha, penutupan/pembubaran korporasi dan pembatasan kegiatan terhadap
4. Mengingat yurisdiksi cybercrime bersifat transnasional crime maka agar lebih efektif dan efisiennya penanggulangan tindak pidana teknologi informasi dapat dipertimbangkan untuk memanfaatkan Internet (melalui e-mail atau messanger) dan digital signature sebagai sarana pemeriksaan sehingga dapat menghemat waktu, biaya dan jarak.

## DAFTAR PUSTAKA


Agus Rahardjo, Cybercrime pemahaman dun upaya pencegahan kejahatan berteknologi, PT. Citra Aditya Bakti, Bandung, 2002, hal.20.

Abdul Wahib dan Mohammad Labib, Kejahatan Mayantara (cybercrime). Kejahatan Mayantara.

Barda Nawawi Arief, Bunga Rampai Kebijakan Hukum Pidana, Op. Cit. hal. 165-166.

Didik J. Rachbini, "Mitos dan Implikasi Globalisasi" Catatan Untuk Bidang Ekonomi dan Keuangan.

Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar. Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi, November, 2003. hal. 25

Pengantar edisi Indonesia dalam Hirst, Paul dan Grahame Thompson. Globalisasi adalah Mitos, Jakarta, Yayasan International Review of Law Computers and Technology. 'Insider Cyber Threat: Problems and Perspectives', Volume 14, 2001, Pages 105-113.

Satjipto Raharjo, Hukum dan Masyarakat, Angkasa, Bandung, 1980, hal. 96.

Soerjono Soekanto, Faktor-faktor yang Mempengaruhi Penegakan Hukum, Op. Cit., hal. 8. Sutarman, Cybercrime Modus Operandi dan Penanggulangannya, Lakshang Pressindo, Jogjakarta, 2007, hal.108-109.